Issn: 2612-4491

# Diritto di INTERNET

## Intelligenza artificiale, Digital Copyright e Data Protection

RIVISTA TRIMESTRALE

2024
3



Pacini Giuridica

# SOMMARIO

## SAGGI



## GIURISPRUDENZA

### EUROPEA



### CIVILE

# Il diritto del nuovo millennio tra giurisdizionalizzazione ed algoritmo

**di Nicolò Lipari**

Muovendo dalla constatazione dell'avvenuta costituzionalizzazione del diritto privato, il saggio ripropone la necessità di superare la logica del formalismo giuridico ed invece prendere atto del processo di giurisdizionalizzazione del diritto, nell'ambito del quale assume rilievo il principio di ragionevolezza come idoneo a saldare le attese di giustizia con gli indici di valore dei consociati.

*Starting from the observation of the constitutionalization of private law, the essay re-proposes the need to overcome the logic of legal formalism and instead take note of the process of 'giuridizionalizzazione' of law, in the context of which the principle of reasonableness assumes importance as suitable for welding the expectations of justice with the value indices of the associates.*

Considero estremamente significativa l'iniziativa assunta dal Centro fiorentino di studi giuridici di organizzare una serie di incontri sulla "giurisdizione del futuro". Affrontare oggi una tematica di questo tipo con chi fa professione del diritto – e segnatamente con magistrati ed avvocati – appare opera altamente meritoria, per la semplice ma decisiva ragione che (come io vado ripetendo da tempo) il diritto ha subíto, nell'ultimo mezzo secolo, una trasformazione epocale della quale pochi sembrano essersi resi conto, anche a causa di un sistema universitario che continua ad essere modellato sugli schemi del passato. Accade così che la riflessione teorica sembra svolgersi su di un piano del tutto parallelo rispetto ai paradigmi culturali correnti, spesso banalmente moltiplicati dai *talk-show* televisivi, laddove sembra risultare che l'esercizio della giurisdizione si risolva, nella maggior parte dei casi, in un abuso. Per limitarmi ad un esempio soltanto citerò il volume recente di uno dei nostri massimi filosofi del diritto Giuseppe Zaccaria, intitolato "*Postdiritto*", nel quale significativamente si riassume la trasformazione di cui dicevo, volume peraltro rimasto del tutto estraneo al panorama culturale dei nostri professionisti del giure. Al di là della provocatorietà del titolo, il sottotitolo specifica che si tratta di coniugare "nuove fonti e nuove categorie"; il che è proprio l'opposto di ciò che viene insegnato alle matricole delle nostre Facoltà giuridiche, alle quali si continua a ripetere che le fonti del diritto sono quelle di cui all'art. 1 delle preleggi (magari interpretativamente integrato dal riferimento alla costituzione e alle norme comunitarie) e le categorie quelle consolidate dalla solida tradizione della dogmatica. Da un lato la Corte costituzionale continua insistentemente a ripetere che il procedimento interpretativo impone di essere svolto ponendo in rapporto dialettico testi e contesti, dall'altro, sfogliando un qualsiasi repertorio di giurisprudenza, si constata come la pratica faccia ancora pervicacemente riferimento all'art. 12 delle Preleggi, non a caso definito da Paolo Grossi un "reperto archeologico". Nelle nostre Università si continua ad insegnare ai nostri studenti ad interpretare testi; nessuno insegna loro ad analizzare contesti, che è invece il compito precipuo che ci tocca affrontare quando svolgiamo la funzione di magistrati od avvocati (del resto secondo un paradigma martellantemente richiamato dalla Corte costituzionale). Non è temerario dunque affermare che chi esercita oggi la professione del diritto si trova ad operare all'interno di un quadro che non esiterei a definire schizofrenico. Spesso, sfogliando un manuale universitario di diritto, si ha una sensazione analoga a quella di chi pretenda di insegnare la fisica quantistica con le tecniche di analisi della fisica newtoniana. Il che si riflette nel diffuso discredito che oggi accompagna, nei modelli correnti, l'esercizio della giurisdizione, alla quale ci si affida non con fiducia ma con diffidenza. Ognuno di noi è responsabile di questo esito, se è vero quel che diceva Capograssi: "Ciascuno, con la propria azione, modifica la vita del mondo e della storia e quindi ne porta tutta la responsabilità".

Quando io mi sono iscritto all'Università, intorno alla metà degli anni Cinquanta, il diritto era pacificamente riconducibile ad una scienza teoretica, una scienza cioè che ha un proprio oggetto definito, previamente individuabile nel sistema legislativo dettato dall'autorità legittimamente costituita, secondo paradigmi riconducibili ad un criterio di validità formale. Da questa premessa

(*) Il testo riproduce la relazione svolta a Firenze il 1 marzo 2024 nel quadro di una serie di incontri organizzati dal Centro fiorentino di Studi giuridici sul tema "La giurisdizione del futuro".

consegue che la conoscenza del diritto è conoscenza di norme, dovendo rigorosamente evitarsi ogni commistione tra diritto e fatti (sociali, psicologi, antropologici, biologici). La norma sfugge all'alternativa vero o falso, buono o cattivo: è soltanto se stessa nella capacità di ottenere obbedienza. Il suo "valore" sta nel "farsi valere". Su questi presupposti – ancorché si continuasse a parlare di "amministrazione della giustizia" – a me è stato insegnato che la coincidenza tra diritto e giustizia è del tutto accidentale, dipendendo esclusivamente da quanto sia illuminato l'atteggiamento di chi detta le norme. Francesco Santoro Passarelli – uno dei miei Maestri, sulle cui "*Dottrine generali del diritto civile*" si sono formate generazioni di magistrati ed avvocati – così testualmente ammoniva: "Il giurista può mettere a frutto la sua esperienza giuridica per contribuire alla realizzazione della giustizia o di un assetto più razionale e conveniente, ma con la chiara consapevolezza che va oltre il suo compito di giurista, cioè di interprete". In sostanza, la maggior parte di coloro che oggi hanno a che fare con l'esercizio della giurisdizione, quale che sia la funzione che svolgono, sono stati educati secondo i canoni di un rigido e abbastanza ottuso positivismo e continuano ad attendersi dall'intervento palingenetico del legislatore soluzioni che questo – nella ormai cronica crisi del nostro sistema politico – è sempre meno in grado di rendere. Senza dire che, con la progressiva crescente riduzione del numero dei votanti, il Parlamento, ammesso che si possa ancora continuare a fare riferimento al paradigma della rappresentatività, oggi finisce con il rappresentare meno della metà del contesto sociale. Ancor meno rappresentativa ovviamente risulta quella che si suole definire come maggioranza.

Il processo di costituzionalizzazione del diritto – al quale ha certamente concorso quel gruppo che Enrico Scoditti ha designato come "i giovani civilisti degli anni Sessanta", cui mi onoro di avere appartenuto – ha radicalmente sovvertito questa prospettiva. La scienza giuridica è oggi pacificamente intesa come scienza pratica; il suo sapere non è un sapere veritativo e descrittivo, ma un sapere costruttivo, valutativo, ipotetico, dubitativo, in linea con il metodo di quelle scienze che assumono a loro oggetto la fluidità di una prassi, la realtà di un'esperienza vissuta. Persino un'opera ciclopica come l'"*Enciclopedia del diritto*", senza che nel frattempo il nostro ordinamento avesse subíto radicali modifiche di struttura, ha ritenuto necessario far seguire alla voce "Legalità", affidata negli anni Settanta a Sergio Fois, in cui il principio veniva ricondotto, secondo l'impostazione tradizionale, ad una rispondenza ad indici formali dettati, una analoga voce, affidata negli anni Duemila a Massimo Vogliotti, in cui la legalità viene definita come "*eupraxia*", cioè prassi indirizzata ad un risultato di giustizia. Quel traguardo che un tempo poteva ritenersi, senza sostanziali conflitti, consegnato ad un testo, oggi va ricercato, indagato, esplorato. Paolo Grossi ha parlato di "invenzione" del diritto, dove al sostantivo va assegnato il significato discendente dall'*invenire* latino, che significa cercare per trovare. Io ho, in altro luogo, parlato di un epocale passaggio da uno *ius positum* a uno *ius in fieri*. In sintesi, noi che facciamo professione del diritto dobbiamo imparare a misurare il passaggio da una legalità sostanziale (incardinata appunto nella sostanza legislativa) ad una legalità procedurale (che non può che commisurarsi ad una valorizzazione dell'azione secondo giustizia). Per dirla con una formula di recente entrata nell'uso, noi dobbiamo abituarci – vincendo le resistenze di una cultura ancora schiava di vecchi modelli – a passare da una legalità-legittimità ad una legalità-giustizia. dobbiamo passare dalla logica degli atti di posizione alla logica degli atti di riconoscimento.

Non ho qui evidentemente né il tempo né il modo di approfondire questa evoluzione (che tuttora incontra vigorose resistenze dalle posizioni che si riconducono al c.d. nichilismo giuridico). L'ho fatto in un piccolo libretto che ho intenzionalmente intitolato "*Elogio della giustizia*". Sono convinto tuttavia – ma constato di essere, in questa convinzione, in buona ed autorevole compagnia – che noi dobbiamo liberarci, una volta per tutte, dal condizionamento culturale che assume il diritto non come un'azione che deve tendere ad un risultato di giustizia, ma come un dato esterno che deve essere descritto nella sua oggettività. Dobbiamo cioè uscire dallo schema valutativo di quelle che Aristotele chiamava le scienze teoretiche e abbandonare la convinzione che il diritto sia una sostanza oggettivamente definibile, radicalmente separata dal soggetto conoscente, che deve quindi limitarsi a descriverlo nella sua consistenza.

Tutto ciò evidentemente implica un radicale sovvertimento nell'uso degli strumenti ricostruttivi ai quali siamo stati educati. Da un lato ci dobbiamo liberare dal paradigma della fattispecie, che implica il necessario riferimento ad uno schema astratto disegnato dalle norme. Nella sua prima parte la Costituzione non detta norme, non definisce fattispecie; si limita ad indicare fini da attuare, valori da perseguire, beni da realizzare; prospetta cioè principi dei quali da un lato riconosce la implementabilità storica, dall'altro – come ha più volte ribadito la Corte costituzionale – implicitamente afferma la non modificabilità, neppure attraverso il procedimento di revisione costituzionale. Tutto ciò implica la necessità di liberarci di quella sovrastruttura concettuale che ha fin qui ritenuto il mondo dei fatti privo di incidenza sulla configurazione del diritto. Non a caso Francesco Viola, un altro autorevole nostro filosofo del diritto, ha parlato di "legalità del caso". Noi dobbiamo abituarci a comprendere che il fatto non è un fattore esterno alla vita del diritto, ma un suo ingrediente essenziale. Solo

alla luce del fatto il principio assume il suo autentico significato, spesso all'esito di un delicato processo di bilanciamento con altri principi, fermo restando che fra i principi non è pensabile una gerarchia (come invece è sempre stato ritenuto possibile per le norme). E l'accertamento del fatto, la sua definizione, non appartiene al legislatore, ma a chi combatte nelle trincee dei conflitti giudiziali.

Diventa in quest'ottica decisivo il riferimento all'art. 3 cpv. cost., che (impegnando "la Repubblica" e quindi tutti i suoi assetti istituzionali, ivi compresa la giurisdizione) implica il capovolgimento del rapporto tra norma e fatto istituito per via di sussunzione ed esige che l'applicazione della regola venga modulata in relazione alle peculiarità del destinatario. Per riprendere una formula utilizzata molti anni fa da Luigi Ferrajoli, nella nuova prospettiva non è più la norma ma il fatto "ad essere assunto ad oggetto primario e privilegiato di conoscenza, non più in segmenti frazionati ed avulsi dal contesto come il formalismo postula e impone attraverso il filtro della rilevanza giuridica, bensì nella totalità dei suoi nessi e delle sue complesse e singolari determinazioni economico-materiali". Attuare in concreto l'eguaglianza significa uscire dalla logica deformante del formalismo e dell'astrattismo giuridico. L'espediente con il quale la nuova cultura giuridica ha segnato questo passaggio è stato il costante riferimento al principio di ragionevolezza (assunto ormai dalla Corte costituzionale a criterio direttivo di fondo per la maggior parte delle sue pronunce), che sposta il punto focale per il giudizio sulla legittimità della legge dal momento della posizione di una regola in conseguenza dell'esercizio di un potere al momento del riconoscimento da parte di una comunità di riferimento in base ad indici di valore condivisi ed attuati. Mi limito qui ad osservare, tra parentesi, che, come è stato già autorevolmente dimostrato, vi era potenzialmente maggiore possibilità di abuso quando si trattava semplicemente di assegnare significato a parole, che non quando si operi nell'intento di far emergere un valore, che è attuato praticato vissuto e quindi ricavabile da una serie molteplice di indici rivelatori.

Secondo l'impostazione di Esser – che ha ricevuto di recente significative rivisitazioni – nella prospettiva ermeneutica non si conosce propriamente il senso di un enunciato normativo secondo il metodo veritativo, descrittivo e oggettivante delle scienze teoretiche, ma lo si progetta, muovendo dalla precomprensione del caso e in vista di una sua soluzione ragionevole e giusta, tale cioè da essere ritenuta adeguata alle peculiarità del fatto e conforme alla tavola costituzionale dei valori dai soggetti ragionevoli della comunità interpretativa alla quale si rivolge il giudice. Il fine da raggiungere viene prima della regola e la rende possibile.

Tutto ciò – a differenza di quanto potesse pensare l'autorità di Santoro Passarelli – implica che un criterio di giustizia entri necessariamente all'interno del processo applicativo del diritto, perché, come ha giustamente ammonito Cacciari, la ragione non può avere un fondamento né naturalistico né positivistico in quanto trova il fondamento ultimo in se stessa. Quando la Corte costituzionale fa richiamo al principio di ragionevolezza – e non va, fra parentesi, dimenticato che la Corte ha ripetute volte invitato il giudice ordinario a fare diretta applicazione del principio, nell'ottica di una interpretazione costituzionalmente orientata, senza necessità di un inutile e insistito ricorso alla questione di costituzionalità – ribadisce che non è possibile limitarsi a porre il fondamento della regola nella legittimità formale della sua posizione e nell'autorità di chi è autorizzato a dettarla, senza avvertire l'esigenza di una sua comprensibilità da parte dei destinatari. Oggi si ritiene necessario che la regola, non più assunta in astratto ma riferita alle peculiarità del caso, appaia supportata da motivazioni e argomentazioni tali da renderla accettabile alla comunità di riferimento proprio a cagione della sua ragionevolezza, intesa questa come capacità di rispondere agli orizzonti di attesa della collettività. Se cioè ci si colloca nell'ottica non di una regola desunta da atti di posizione, ma determinata da atti di riconoscimento, non è più sufficiente accontentarsi di una correttezza procedurale, ma è necessario riferirsi appunto ad un fondamento di ragione, che è doveroso individuare nel rapporto di congruenza tra le esigenze del caso ed il quadro dei principi costituzionali, peraltro assunti nella consapevolezza di una loro duttilità storica non cristallizzabile nella fissità di enunciati. Il fine da raggiungere viene prima della regola e la rende possibile.

Se tutto ciò è vero, è ovvio che ne discende un mutamento radicale del ruolo che siamo soliti assegnare alle tradizionali professioni legali, e segnatamente a quella del giudice. Secondo il modello classico – purtroppo rispondente al paradigma culturale corrente, passivamente recepito e moltiplicato da trasmissioni televisive come quella di Bruno Vespa o radiofoniche come quella di Emanuela Falcetti, spesso supportate da pseudogiuristi – il giudice dovrebbe essere chiamato a svolgere una funzione prevalentemente meccanica assimilabile a quella del farmacista: egli sarebbe chiamato semplicemente a trarre dagli scaffali delle norme quella adatta al caso che gli viene sottoposto e, quando dovesse sbagliare scaffale, la verifica sarebbe sempre rigorosamente possibile in funzione di un riscontro con il contenuto oggettivo della norma. È chiaro che un'affermazione di questo tipo si risolve in una tipica petizione di principio perché il contenuto (*scilicet:* il significato) di un precetto non è necessariamente ricavabile dal suo enunciato, ma discende dall'esito di un procedimento interpretativo, inevitabil-

mente soggetto a condizionamenti di tempo e di luogo. Ritornano qui ammonitrici le pagine che, sulla scia di Crisafulli, Franco Modugno ha di recente dedicato al classico problema della distinzione tra disposizione e norma, con il primo termine designandosi il semplice enunciato lessicale, con il secondo il significato precettivo che al medesimo viene attribuito all'esito di un procedimento interpretativo. Si tratta di un'affermazione che non può essere oggi seriamente contestata, ma che ancora continua invece ad essere autorevolmente contraddetta, se è vero che il vicepresidente del Consiglio superiore della magistratura, svolgendo di recente il suo intervento nel convegno organizzato dalla Cassazione per i cento anni della sua unificazione, ha perentoriamente affermato che il limite del procedimento interpretativo sta "nel significante del testo normativo" (che è affermazione che qualunque filosofo del diritto sanzionerebbe con matita blu).

È chiaro che, nel momento in cui il giudice è chiamato a ricercare principi che non risultano talora nemmeno letteralmente formulati e che pure sono fondativi di norme, principi che esigono un reciproco bilanciamento in funzione delle peculiarità del fatto, non svolge più una funzione passiva, di mero enunciatore di un dato assunto in una asserita oggettività (appunto il significante), ma concorre alla formazione del precetto; non svolge la semplice funzione passiva del farmacista, ma è dentro il processo che conduce alla formazione della medicina.

Tutto ciò si riflette anche – com'è evidente – sul ruolo dell'avvocato, il quale non può, di riflesso, limitarsi, in maniera miope, a farsi esclusivamente carico degli interessi di una parte, perché, se i principi, non essendo regole, determinano regole all'insorgenza del fatto, diventa anch'egli soggetto attivo del processo formativo del diritto e non può che farlo in chiave di solidarietà, cioè rappresentandosi anche gli interessi della controparte. Che è proprio quanto la Cassazione ha insistentemente ribadito (bisogna riconoscerlo: con qualche diffidenza da parte della comune degli avvocati) quando ha affermato che il principio di solidarietà connota necessariamente il contenuto di qualsiasi contratto, indipendentemente da una esplicita pattuizione. Non a caso Calamadrei qualificava il ruolo dell'avvocato come quello di un "primo giudice".

È chiaro che, nel momento in cui si riconosce al giudice – ma con la collaborazione decisiva di chi concorre allo svolgimento della vicenda processuale e quindi in primo luogo dell'avvocato – un ruolo determinante nell'individuazione del precetto, proprio perché l'impianto costituzionale ha fatto emergere un diritto non già definito nei suoi indici qualificanti, ma da perseguire in fini da attuare, in prospettive da realizzare, si rompe il vecchio postulato della c.d. certezza del diritto e si apre il panorama di quel processo che oggi viene definito di giurisdizionalizzazione del diritto e che continua ad incontrare diffuse resistenze, a partire – se mi consentite un'impertinenza – dalle posizioni espresse dal nostro stesso Ministro della giustizia.

È diffusa oggi, sulla spinta dei *mass-media*, una singolare diffidenza sul ruolo della magistratura che, al di là dei casi patologici che sono propri di qualunque esercizio di una funzione pubblica, risulta essere sintomo di una grave insufficienza culturale. Dobbiamo una buona volta convincerci che, al di là di episodi del tutto particolari e marginali, la vita di una comunità giuridica si esprime e si risolve in una costante ed instancabile prassi interpretativa della quale il giudice che eserciti correttamente la sua funzione è mero riflesso o portavoce. Il comando non esiste nell'immutabile astrattezza del suo enunciato, ma vive nello spazio e nel tempo in un inevitabile attrito con l'esperienza, all'interno della quale i consociati attuano varie modalità di comportamento, accettando e riconoscendo precetti, ai quali attribuiscono significato in funzione di ben individuate contingenze storiche. Negare questa realtà, delegittimando il ruolo della giurisprudenza, significa anteporre astratti postulati ideologici al vero modo d'essere dell'esperienza giuridica, che oggi si misura appunto attraverso il ruolo decisivo della giurisdizione.

Personalmente – e proprio da avvocato – mi meraviglio quando gli avvocati (ma normalmente accade ad opera dei meno provveduti) attaccano pesantemente il processo di giurisdizionalizzazione del diritto. Non si rendono evidentemente conto che, riesumando il vecchio postulato della certezza del diritto in funzione della rilevanza oggettiva di norme poste, si finisce tendenzialmente per annullare proprio la decisiva mediazione dell'avvocato. Se il diritto non è un fatto, ma viene fatto, chi ne fa esercizio professionale non può limitarsi ad analizzare un edificio da altri costruito, ma deve concorrere ad edificarlo. Nella stagione, sempre più assorbente, delle intelligenze artificiali sarebbe agevole coltivare la tentazione di affidare al computer la totalità del panorama legislativo e un numero sempre maggiore di decisioni giurisprudenziali per far decidere poi all'algoritmo l'esito della causa. All'avvocato e al giudice non resterebbe altro ruolo che quello di registrare un'operazione puramente meccanica.

A ben vedere, la cultura del positivismo, nell'utopia di conseguire un risultato certo, ha da sempre alimentato la tentazione che si possano stemperare le dispute giuridiche nella perentorietà di un calcolo. Oggi la mai sopita dialettica tra chi coltiva una autonomia dogmatica riferita ad indici tutti individuabili e presupposti e chi guarda invece ad un tessuto di valori sottoposti a variabili storiche ed ambientali corre il rischio di risolversi in un esito meramente meccanico di fronte ad un contesto esperienziale che tende a perdere la stessa abitudine al

dialogo. Noi, professori della vecchia guardia, dobbiamo renderci conto che i nostri interlocutori appartengono ad una generazione che non si misura più, rispetto alla precedente, con un semplice metro culturale, ma che utilizza paradigmi radicalmente diversi dai nostri: una generazione la cui dimensione centrale dell'esistenza è la connessione *on line*, una generazione che tende a sostituire i legami virtuali ai legami sociali, il *web* allo Stato, il "chattare" al parlare. Per essere compresi, dobbiamo innanzitutto capire che è necessario adattare il nostro linguaggio a chi ci ascolta. Non dobbiamo mai dimenticare che noi viviamo in una difficile stagione in cui – come è stato lucidamente evidenziato da chi si è occupato di questi temi – al ragionamento si sostituisce il sillogismo, al sillogismo il sillogismo formalizzato, al sillogismo formalizzato il calcolo logico, al calcolo logico il computer, al computer il robot 'intelligente', al robot 'intelligente' il robot 'esperto', che sa imparare dall'esperienza. Non credo ci voglia molto acume per capire che un simile procedimento applicato all'esercizio della giurisdizione comporterebbe inevitabilmente la fine di quelle professioni liberali che la caratterizzano e che, al di là dei loro limiti, ne hanno negli anni segnato la legittimazione e il ruolo. Forse gli stessi cultori del positivismo, del mito della legge fine a se stessa, non se ne rendono conto, ma la loro prospettiva culturale apre al baratro della c.d. giustizia predittiva affidata alle macchine.

È purtroppo doloroso dover constatare che la delicatezza del problema non è neppure lontanamente avvertita dalla nostra classe politica, che continua a coltivare l'apriorismo della sua onnipotenza, senza alcuna attenzione o sensibilità per ciò che accade nell'esperienza. Un esempio soltanto. Quando la Corte di Cassazione rese la famosa sentenza sul caso Englaro, il Parlamento (nonostante il disperato tentativo del sottoscritto e di pochi altri coraggiosi di paralizzare l'iniziativa) sollevò un conflitto di attribuzioni innanzi alla Corte costituzionale, nell'assurdo presupposto che la giurisdizione si fosse arrogato il compito che spettava al legislatore, senza rendersi conto che, in un ordinamento che si assume privo di lacune, il giudice deve parlare anche quando il legislatore è silente. E si tratta di una situazione che – come la Corte costituzionale ha, di recente, più volte rilevato – tende oggi a verificarsi sempre più di frequente. Noi dobbiamo, una buona volta, renderci conto che, nel momento in cui contestiamo la giurisdizionalizzazione del diritto, non facciamo che portare acqua al mulino di chi, in forme più o meno esplicite, auspica di affidare l'esito del giudizio alla macchina, dimenticando che la macchina cataloga utilizzando un arbitrio classificatorio; calcola mediante misurazione aritmetica; commisura – o pretende di commisurare – anche le stesse qualità secondo una cadenza geometrica o topologica, con criteri di pura quantificazione, in una sorta di ossessiva ripetizione che cancella ogni valore e ogni interiorità. Il risultato è la perdita del 'buon senso', inteso come perdita di ciò che articola e caratterizza la nostra umanità e la nostra ragione. Così la macchina, protesi dell'umano, tende a trasformare l'essere umano in una sua protesi.

È necessario riflettere su quale straordinario impatto la rivoluzione digitale abbia avuto sulla società, sull'economia e sull'etica, prima ancora che sul diritto, ma dobbiamo altresì essere consapevoli che l'ottica del positivismo formalistico condurrà inesorabilmente a valorizzare gli schematismi dell'intelligenza artificiale, con tutti i rischi che ciò comporta. Mi limito qui a ricordare, tra parentesi, che lo Zingarelli 2023 segnala, fra le parole di nuovo conio, "algocrazia", ossia il rischio di divenire prigionieri e di sottometterci al dominio dell'algoritmo. Questo pericolo è tanto più alto nelle professioni forensi perché nel ragionamento giudiziale è insita la possibilità dell'innovazione e del rinnovamento (anche nei gradi successivi del giudizio), che è invece preclusa dallo schematismo ripetitivo dell'algoritmo e dalla logica cristallizzante del digitale. Segnalo che la legislazione francese (con la legge n. 222 del 2019) ha vietato la piattaforma *Predictice*, che forniva gli orientamenti dei singoli giudici, ritenendola lesiva della loro indipendenza.

Proprio nel momento in cui acquisiamo consapevolezza che il diritto si colora e acquista significato in funzione della specificità del fatto, non possiamo ancorarci a strumenti operativi che ne negano l'intrinseca storicità. È stato già ampiamente dimostrato che l'elaborazione digitale ha l'effetto di disarticolare il rapporto di correlazione tra *quaestio facti* e *quaestio iuris*, che solo l'interpretazione è in grado di svolgere. Senza dire che, nell'accesso infinito di dati, l'individuo, come unità che esprime la razionalità e come titolare di diritti fondamentali, sprofonda e scompare. I dati inseriti nell'algoritmo sono insensibili al contesto, tanto a quello generale del momento storico, quanto a quello specifico dei casi concreti.

Si tratta dunque di educare il giurista ad un serio rapporto con le macchine che non lo espropri dei suoi poteri di decisione e di scelta. Il diritto, le cui forme sono radicalmente poste in discussione dalla giustizia digitale, deve rivendicare i grandi principi e i valori non negoziabili su cui tali forme si basano, primo fra tutti quello della libertà di scegliere. Io credo che, per conseguire un risultato di questo tipo, sia decisivo il riferimento al principio di ragionevolezza, che salda le ragioni della scelta ad un criterio di condivisione socialmente rilevante e quindi non meccanico né arbitrario.

Oggi valorizzare il profilo della ragionevolezza nell'esercizio della giurisdizione, pur con tutti i rischi che ciò possa in ipotesi comportare, significa superare il pericolo della società digitale, che mette tra parentesi la propria storicità perché non conferisce adeguato rilievo

al fatto che la potenza degli algoritmi è la forza in cui oggi si manifesta l'azione poietica dell'uomo. Pur rendendomi perfettamente conto che l'esperienza giuridica non può non misurarsi con l'intelligenza artificiale, così come la recente prassi del processo telematico sta dimostrando, mi domando quale input dovrebbe assegnarsi alle macchine perché la soluzione appaia ragionevole e in quanto tale pacificamente accettata dai consociati. Se ragioniamo in chiave di ragionevolezza, assume un profilo determinante l'argomentazione (con conseguente decisiva connessione del ruolo dell'avvocato a quello del giudice), che è difficilmente riconducibile alla radicalità dell'algoritmo. Come è possibile ridurre alla binarietà di questo meccanismo quella manifestazione dialogica che è intrinseca all'argomentare e che si realizza quando ci si pone nei panni degli altri attraverso un processo psicologico di sdoppiamento e di reintegrazione? Nel richiamo al principio di ragionevolezza, pur non facilmente definibile nei suoi connotati individuanti, ma certamente riconducibile ad una convinzione diffusa, a un consenso sociale, si saldano le attese di giustizia con le capacità di comprensione e gli indici di valore dei consociati. Superando i rigidi confini della logica apodittica si configura una sorta di "logica dell'umano" (per riprendere qui una felice formula coniata da Modugno), che trova la sua bussola nel riferimento ad un panorama di giustizia. Con il richiamo alla ragionevolezza, quale indice giustificativo di una soluzione di rilevanza giuridica, si individua un criterio di raccordo tra il sistema istituzionale e la società civile che, senza bisogno di particolari motivazioni, rende la decisione accettabile dai più, sul presupposto che qualsiasi diversa soluzione risulterebbe palesemente inadeguata. In questa chiave, proprio nell'ottica di un diritto inteso come prassi storicamente vissuta, il riferimento ad un principio di ragione condiviso finisce per diventare quasi un connotato intrinseco dell'ordinamento giuridico, che, per essere riconosciuto, non ha bisogno di alcuna connotazione formale. Non dobbiamo allora spaventarci di questo processo di giurisdizionalizzazione del diritto, ancorché non corrisponda ai nostri modelli scolastici, perché da esso discende un maggiore raccordo con l'esperienza sociale e soprattutto un recupero della giustizia quale necessario momento costitutivo del processo applicativo del diritto, di contro all'impostazione cara ai nostri maestri. Come è stato da più parti lucidamente ribadito, alla crisi della legge come unica dimensione della giuridicità ha fatto riscontro una nuova centralità del giudice e del momento giurisdizionale, tanto negli ordinamenti nazionali quanto in quello internazionale. Egli infatti non è più chiamato semplicemente ad applicare le norme preesistenti al giudizio, ma è chiamato a coniugare la dimensione prescrittiva a quella autoritativa, mantenendo una comunicazione stretta e dinamica con le basi sociali ed etiche del diritto. Applicando principi e operando un bilanciamento tra beni giuridici diversi in funzione delle peculiarità del caso, il giudice oggi concorre a svincolare l'idea del diritto da quel radicamento nel potere costituito che il positivismo aveva assunto a criterio cardine del modo d'intendere la giuridicità e la fonda in un tessuto di valori condivisi a consolidare i quali ciascuno di noi, come persona, come cittadino, come avvocato porta la sua misura di responsabilità. Zagrebelsky ha giustamente riconosciuto che "la causa dell'incertezza nei processi di applicazione del diritto non è in una cattiva disposizione mentale dei giuristi, ma nel deperimento di un quadro di principi di senso e di valore generalmente condiviso". Le valutazioni in termini di giustizia, che il giudice inevitabilmente compie, pur non essendo assolutamente verificabili come vere o false secondo metodi di controllo scientifici in senso specifico, hanno tuttavia una loro oggettività storico-relativa, suscettibile di essere di volta in volta giustificata con particolari procedimenti interpretativi. Noi avvocati conosciamo molte sentenze che giudichiamo – non a torto – ingiuste, ma nessun indirizzo consolidato della Cassazione che non corrisponda ad un quadro di valori condiviso. In una stagione, come quella del postmoderno, che vive di contraddizioni, sarebbe assurdo pensare che le tensioni sociali non si riflettano anche nell'esercizio della giurisdizione.

Non si tratta quindi di assumere una esigenza assoluta della giustizia (in quanto tale inconoscibile e inesprimibile), ma visioni particolari della giustizia, capaci di riflettere la peculiarità di un determinato ambiente storico, visioni che sono suscettibili di giustificazioni relative alle singole situazioni e alle strutture storiche dalle quali emergono. Quale che sia il profilo che si voglia di volta in volta accentuare nel richiamo alla giustizia, la si riconduca ad un profilo di eguaglianza, di ordine, di integrazione di interessi o di finalità emergenti dalla realtà sociale nelle sue variazioni strutturali e congiunturali, certo è che, in un determinato momento storico, la parola giustizia è, nel suo stesso uso comune, evocatrice di un significato costante. Laddove ciò non accada, significa che ci troviamo in uno di quei territori di confine, nei quali non si è ancora formata una convergenza in chiave di valore e che quindi non sono riconducibili ad una prospettiva condivisa in termini di giustizia.

L'esercizio della giurisdizione si trova oggi, per così dire, al centro del crogiolo. Nella stagione in cui viviamo la stessa parola giustizia, proprio perché rievoca un pensiero trascendente, metafisico, assolutista, è divenuta parola scandalosa, impronunciabile. Nell'epoca del pensiero debole ogni concetto che sembri tendere all'assoluto, diviene foriero di ideologia, di esclusione. Non va tuttavia mai dimenticato che per intendere il significato di giustizia è indispensabile muovere dalla storicità della

vita sociale e dagli ordini normativi che essa esprime. Ed è proprio questo il compito che oggi è rimesso in modo peculiare all'attività giurisdizionale. Da qui l'artificio di un dibattito politico che, mentre imputa alla magistratura di non essere capace di fornire soluzioni uniformi, non è in grado di creare le basi per un dialogo comune su problemi fondamentali, con un atteggiamento del tutto alternativo rispetto a quello esemplare dei nostri padri costituenti che realizzarono punti significativi di convergenza (pur in una stagione ad altissima conflittualità ideologica e politica) nella visione di un interesse comune superiore a qualsiasi prospettiva parziale.

Non dobbiamo mai dimenticare che il diritto (come la filosofia) include il ricercante nella ricerca. Non spaventiamoci dunque se, dopo aver constatato che il diritto è storia, dobbiamo, anche prendere atto che esso non può essere incapsulato in schemi rigidi: deve tornare ad incarnarsi nell'esperienza. Vincendo le rigidità delle nostre opzioni politiche e gli schematismi dei nostri modelli concettuali dobbiamo renderci avvertiti che il momento giudiziale, nonostante i suoi rischi, esprime e sublima la positività del diritto. La giustizia come traguardo esige di passare attraverso le difficili vie della storia, ma sarebbe pretesa assurda quella di ingabbiare la storia entro il cemento del legalismo e del formalismo.

# Note minime sul D.D.L. in materia di Intelligenza Artificiale

**di Giuseppe Cassano**



L'innovazione è un motore di progresso economico, inclusione sociale e salvaguardia ambientale essenziale per assicurare all'Italia prosperità e competitività nel contesto europeo e globale. La transizione digitale costituisce, insieme alla transizione ecologica, una delle due direttrici fondamentali per lo sviluppo socioeconomico e la sostenibilità dei Paesi membri dell'U.E.. Tra le sfide innovative più importanti c'è sicuramente lo sviluppo dell'intelligenza artificiale (IA). L'utilizzo dell'intelligenza artificiale nel nostro Paese si pone come opportunità chiave per superare le attuali problematiche economiche e sociali.

*Innovation is a driver of economic progress, social inclusion and environmental protection essential to ensuring Italy's prosperity and competitiveness in the European and global context. The digital transition constitutes, together with the ecological transition, one of the two fundamental directions for the socio-economic development and sustainability of the EU member countries. Among the most important innovative challenges there is certainly the development of artificial intelligence (AI). The use of artificial intelligence in our country presents itself as a key opportunity to overcome current economic and social problems.*

## 1. Premessa

Con la seduta n. 78 del 23 aprile 2024, all'esito della quale il Consiglio dei Ministri ha approvato il disegno di legge "Recante disposizioni e delega al governo in materia di intelligenza artificiale", l'Italia si accinge ad avere la propria fonte interna di regolamentazione organica di un settore che tanti dibattiti sta alimentando in questi ultimi tempi (1).

Il tema dell'intelligenza artificiale (IA) diventa di dominio pubblico – e tutti se ne occupano – all'indomani dell'avvento (era il novembre del 2022) della nota Chat GPT (*Generative Pre-Trained Transformer*) e, oggi, può dirsi che il suo uso sia ormai ricorrente in molti settori.

Ci si avvale dell'IA, invero, nell'*automotive*, nell'arte e nella musica, nell'elaborazione dati, nella medicina, nella programmazione di software ed ancora per il riconoscimento vocale, nei mercati azionari e finanziari, per operazioni di marketing mirato (profilazione dell'utente), per i sistemi di erogazione dell'energia elettrica, per il funzionamento degli smartphone di ultima generazione, etc..

L'IA già vanta diversi suoi riconoscimenti e regolamentazioni a livello legislativo (2) e, se pensiamo al cinema,

(1) Ci si limita in questa sede a citare quanto pubblicato, in ideale rapporto di continuità, sulle pagine di questa ***Rivista***. Cfr. Ferrari, *La seducente perfezione di algoritmi e intelligenza artificiale nelle procedure amministrative alla luce dei modelli di responsabilità civile*, in questa ***Rivista***, 2020, 178 ss.; Gallone, *Il Consiglio di Stato marca la distinzione tra algoritmo, automazione ed intelligenza artificiale*, in questa ***Rivista***, 2022, 161 ss.; Giuliani, *Dalla nozione di "algoritmo di trattamento" e di intelligenza artificiale ai riflessi della tecnologia* blockchain *sul rapporto di lavoro dei* riders, in questa ***Rivista***, 2022, 426 ss.; Moro Visconti, *Le società* medtech *e biotech: piattaforme digitali, intelligenza artificiale e valutazione economica*, in questa ***Rivista***, 2023, 180 ss.; Tassone, *Riflessioni su intelligenza artificiale e soggettività giuridica*, in questa ***Rivista***, 2023, 213 ss.; La Rosa, *La tutelabilità dell'opera creata col supporto di sistemi di intelligenza artificiale*, in questa ***Rivista***, 2023, 483 ss.; Rossi, *Opere in cerca d'autore: creatività,* copyright *e sistemi di intelligenza artificiale generativa di immagini*, in questa ***Rivista***, 2023, 617 ss.; D'Antonio, Ruocco, *L'intelligenza artificiale "pronuncia" sentenze? Un* leading *case peruviano*, in questa ***Rivista***, 2023, 661 ss.; Moro-Visconti - Frank, Chatbot *e intelligenza artificiale generativa: valutazione economica*, in questa ***Rivista***, 2023, 821 ss.; Arnone, *L'uso dei servizi di intelligenza artificiale da parte dei minori: solo una questione di* "age verification"?, in questa ***Rivista***, 2024, 13 ss.; Capaccioli, Vaciago, Criticità del trattamento automatizzato e dell'intelligenza artificiale nel sistema tributario, in questa ***Rivista***, 2024, 157 ss.; Moro Visconti, *La valutazione delle startup nell'intelligenza artificiale*, in questa ***Rivista***, 2024, 167 ss.; Cassano - Di Ciommo, Atti digitali di <Gli stati generali del diritto di internet e della intelligenza artificiale>, LUISS 14, 15, 16 dicembre 2023, in questa ***Rivista***, 2024, 187 ss.

(2) Il D.L. 7 maggio 2024, n. 60 ("Ulteriori disposizioni urgenti in materia di politiche di coesione") all'art. 26 ("Funzionamento del sistema informativo per l'inclusione sociale e lavorativa - SIISL") espressamente prevede che "Al fine di favorire l'incontro tra domanda e offerta di lavoro, il Sistema Informativo per l'inclusione sociale e lavorativa utilizza, nei limiti consentiti dalle disposizioni vigenti, gli strumenti di intelligenza ar-

il Maestro *Stanley Kubrick* nel 1968 anticipava, nel suo capolavoro "2001: Odissea nello spazio", il nocciolo del dibattito di questi giorni, se l'uomo sarà sostituito dalla macchina.

## 2. Crescita economica del Paese

Filo conduttore dello schema di DDL in esame è la volontà di intercettare le opportunità di crescita economica e sociale che le nuove tecnologie offrono al contempo governando un fenomeno di cambiamento epocale che potrebbe, altrimenti, prestarsi ad usi impropri e dannosi, fermo restando la centralità dell'essere umano che non dovrà essere scalzato dall'intelligenza artificiale.

Una prima questione che l'interprete è chiamato a risolvere è data dal rapporto tra il Regolamento europeo sull'AI (approvato il 13 marzo 2024 dal Parlamento Europeo e ormai prossimo ad essere emanato) e il DDL nazionale: quest'ultimo, nelle intenzioni e nelle dichiarazioni del Governo, non si "sovrappone" al primo "ma ne accompagna il quadro regolatorio in quegli spazi propri del diritto interno" tanto è che al comma 2 dell'art. 1 si prevede espressamente, quanto forse ovviamente, che "le disposizioni della presente legge si interpretano e si applicano conformemente al diritto dell'Unione Europea" (3).

Alcune note critiche, riportate nelle pagine che seguono, hanno solo lo scopo di mettere in luce punti della normativa che possono essere migliorati giacché si tratta di un testo destinato ad essere oggetto dei lavori parlamentari e, di conseguenza, di modifiche ed emendamenti.

## 3. La nuova normativa, principi e finalità

Il Capo I della futura Legge nazionale sull'IA detta principi e finalità dell'intervento normativo in esame.

L'art. 1 (Finalità e ambito di applicazione) prevede che la legge reca principi in materia di "ricerca, sperimentazione, sviluppo, adozione e applicazione di sistemi e modelli di intelligenza artificiale" promuovendone un utilizzo "corretto, trasparente e responsabile", in una dimensione – come detto – antropocentrica, per coglierne le opportunità e ferma restando la vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali della stessa IA.

Quanto alle definizioni l'art. 2 indica cosa si intende per: a) sistema di intelligenza artificiale; b) dato; c) modelli di intelligenza artificiale.

Precisamente:

a) un sistema di intelligenza artificiale è "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali";
b) dato è "qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva";
c) i modelli di intelligenza artificiale sono "modelli che identificano strutture ricorrenti attraverso l'uso di collezioni di dati, che hanno la capacità di svolgere un'ampia gamma di compiti distinti e che possono essere integrati in una varietà di sistemi o applicazioni".

Il Legislatore nazionale ha qui attinto all'AI ACT (si veda la definizione di "sistema di intelligenza artificiale" di fatto sovrapponibile nei due testi) per cui si dovranno ben coordinare le due fonti in modo che alle modifiche della normativa europea corrispondano anche le medesime modifiche al testo nazionale.

## 4. Uno sguardo ai principi generali

Quanto ai principi generali l'art. 3 prescrive che tutto ciò che attiene all'IA debba avvenire nel rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione, del diritto dell'U.E. e dei principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità.

Inoltre sistemi e modelli di intelligenza artificiale dovranno essere sviluppati ed applicati nel rispetto dell'autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità e della spiegabilità. Né l'IA potrà pregiudicare lo svolgimento con metodo democratico della vita istituzionale e politica.

tificiale per l'abbinamento ottimale delle offerte e delle domande di lavoro ivi inserite". Il D.Lgs. 25 marzo 2024, n. 41 ("Disposizioni in materia di riordino del settore dei giochi, a partire da quelli a distanza") all'art. 14 ("Tutela della salute del giocatore") prevede che per perseguire la piena e affidabile protezione della salute del giocatore attraverso misure idonee a prevenire ogni modalità di gioco che possa generare disturbi patologici del comportamento o forme di gioco d'azzardo patologico "l'offerta di gioco e le relative modalità di svolgimento dovranno essere supportate da idonei strumenti di tecnologia avanzata, con particolare riguardo anche agli strumenti dell'intelligenza artificiale". Il Nuovo Codice degli Appalti Pubblici (D.Lgs. 31 marzo 2023, n. 36), all'art. 30 ("Uso di procedure automatizzate nel ciclo di vita dei contratti pubblici") espressamente prevede che per migliorare l'efficienza "le stazioni appaltanti e gli enti concedenti provvedono, ove possibile, ad automatizzare le proprie attività ricorrendo a soluzioni tecnologiche, ivi incluse l'intelligenza artificiale (...)". Nella "Delega al Governo per la riforma fiscale" (D.Lgs. 9 agosto 2023, n. 111) si prevede all'art. 17, I, lett. f, che "per la revisione dell'attività di accertamento" si potenzi l'utilizzo di tecnologie digitali, "anche con l'impiego di sistemi di intelligenza artificiale".

(3) Tale inciso normativo comporta che, a qualsiasi livello si pongano in essere, le operazioni di interpretazione ed applicazione delle disposizioni nazionali dovranno essere conformi al diritto euro-unionale (sia già esistente, che avvenire) così evitandosi la frammentarietà in un settore tanto strategico per l'economia quale è quello della IA.

Per garantire il rispetto di tali diritti e principi deve essere assicurata "la cybersicurezza lungo tutto il ciclo di vita dei sistemi e dei modelli di intelligenza artificiale, secondo un approccio proporzionale e basato sul rischio, nonché l'adozione di specifici controlli di sicurezza, anche al fine di assicurarne la resilienza contro tentativi di alterarne l'utilizzo, il comportamento previsto, le prestazioni o le impostazioni di sicurezza".
Infine, ancora all'art. 3 è garantita alle persone con disabilità il pieno accesso ai sistemi di IA e alle relative funzionalità o estensioni, su base di uguaglianza e senza alcuna forma di discriminazione e di pregiudizio.

## 5. Sul rapporto tra IA e informazione e riservatezza dei dati personali

L'art. 4, richiamando alcuni fondamentali principi del GDPR, prescrive che l'utilizzo di sistemi di intelligenza artificiale nell'informazione avvenga senza pregiudizio alla libertà e al pluralismo dei mezzi di comunicazione, alla libertà di espressione, all'obiettività, completezza, imparzialità e lealtà dell'informazione (4).
Tale utilizzo deve altresì garantire il trattamento lecito, corretto e trasparente dei dati personali e la compatibilità con le finalità per le quali sono stati raccolti, in conformità con il diritto euro-unionale in materia di dati personali e di tutela della riservatezza.
Il Legislatore si è preoccupato poi di disciplinare espressamente l'accesso alle tecnologie di IA da parte dei minori.
L'accesso a tali tecnologie, da parte dei minori degli anni 14, richiede il consenso di chi esercita la responsabilità genitoriale.
Il minore degli anni diciotto, che abbia compiuto quattordici anni, può invece esprimere il proprio consenso per il trattamento dei dati personali connessi all'utilizzo di sistemi di IA, purché le informazioni e le comunicazioni siano facilmente accessibili e comprensibili.

## 6. IA e sviluppo economico

Capitolo centrale – quello delle opportunità economiche sottese all'utilizzo dell'IA – che si declina (art. 5) in quattro punti fondamentali e precisamente nell'impegno programmatico per lo Stato, e le altre autorità pubbliche, di:

a) promuovere l'utilizzo dell'IA come strumento per migliorare l'interazione uomo-macchina nei settori produttivi e migliorare la produttività in tutte le catene del valore e le funzioni organizzative, nonché quale strumento utile all'avvio di nuove attività economiche;
b) favorire un nuovo mercato dell'IA, che dovrà essere oltre che innovativo anche "equo, aperto e concorrenziale", e di ecosistemi innovativi;
c) facilitare la disponibilità e l'accesso a dati di alta qualità per le imprese che sviluppano o utilizzano sistemi di IA e per la comunità scientifica e dell'innovazione;
d) indirizzare le piattaforme di *e-procurement* delle PPAA (di cui all'art. 1, II, D.Lgs. 30 marzo 2001, n. 165) in modo che, nella scelta dei fornitori di sistemi e modelli di intelligenza artificiale, vengano privilegiate quelle soluzioni che garantiscono la localizzazione ed elaborazione dei dati critici presso data center posti sul territorio nazionale, nonché modelli in grado di assicurare elevati standard in termini di trasparenza nelle modalità di addestramento e di sviluppo di applicazioni basate su IA generativa.

## 7. Disposizioni in materia di sicurezza e difesa nazionale

Un limite all'applicazione della normativa in esame è rappresentato dalla materia della sicurezza e della difesa nazionale (art. 6).
Precisamente vengono escluse dall'ambito di applicazione del DDL in esame quelle attività svolte per scopi di sicurezza nazionale, per la cybersicurezza nazionale (5) e, ancora, per scopi di difesa dalle forze armate e dalle forze di polizia.

## 8. Utilizzo dell'IA in ambito sanitario e di disabilità

Procediamo ora ad una prima lettura delle disposizioni di settore (Capo II) soffermandoci su sanità (6) e disabilità.
L'art. 7 muove dall'affermazione di principio per cui l'utilizzo di sistemi di IA deve contribuire al miglioramento del sistema sanitario e alla prevenzione e alla cura delle malattie, nel rispetto dei diritti, delle libertà e degli interessi della persona, anche in materia di protezione dei dati personali.
L'IA non può selezionare e condizionare l'accesso alle prestazioni sanitarie con criteri discriminatori e al paziente è riconosciuto il diritto ad essere informato circa l'utilizzo di tecnologie di intelligenza artificiale e sui vantaggi, in termini diagnostici e terapeutici, derivanti dall'utilizzo delle nuove tecnologie, nonché di ricevere informazioni sulla logica decisionale utilizzata.

(4) Cfr. Capparelli, *Disinformazione online, intelligenza artificiale e ruolo dell'autoregolamentazione*, in *Giurisprudenza italiana*, 2024, 2, 480 ss.

(5) Si consideri che il DDL espressamente prevede, all'art. 16, l'utilizzo dell'IA per il rafforzamento della cybersicurezza nazionale.

(6) Cfr. Faccioli, *Intelligenza artificiale e responsabilità sanitaria*, in *La nuova giurisprudenza civile commentata*, 2023, 3, II, 732 ss.

I sistemi di intelligenza artificiale nell'ambito sanitario costituiscono un supporto nei processi di prevenzione, diagnosi, cura e scelta terapeutica, lasciando impregiudicata la decisione, che è sempre rimessa alla professione medica.
Si prescrive, ancora, la periodica verifica e l'aggiornamento dei sistemi di IA al fine di minimizzare il rischio di errori così da garantirne la piena affidabilità.
I sistemi di intelligenza artificiale sono altresì chiamati a migliorare le condizioni di vita delle persone con disabilità e ad agevolare l'accessibilità, l'autonomia, la sicurezza e i processi di inclusione sociale delle medesime persone anche ai fini dell'elaborazione del progetto di vita di cui all'art. 2, II, lett. a) n. 1), L. 22 dicembre 2021, n. 227.
Per il supporto alle finalità di cura, e in particolare per l'assistenza territoriale, è prevista l'istituzione di una piattaforma di IA la cui progettazione, realizzazione, messa in servizio e titolarità sono attribuite all'Agenzia nazionale per i servizi sanitari regionali (AGENAS) in qualità di Agenzia nazionale per la sanità digitale.
Tale piattaforma avrà il compito di erogare servizi di supporto:

a) ai professionisti sanitari per la presa in carico della popolazione assistita;
b) ai medici nella pratica clinica quotidiana con suggerimenti non vincolanti;
c) agli utenti per l'accesso ai servizi sanitari delle case di comunità.

## 9. IA, dati sanitari e ricerca scientifica

Sono dichiarati di rilevante interesse pubblico (art. 8, I) i trattamenti di dati, anche personali, eseguiti da soggetti pubblici e privati senza scopo di lucro (no profit) per la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di IA per finalità di prevenzione, diagnosi e cura di malattie, sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicali, incluse protesi e interfacce fra il corpo e strumenti di sostegno alle condizioni del paziente, di salute pubblica, incolumità della persona, salute e sicurezza sanitaria, in quanto necessari ai fini della realizzazione e dell'utilizzazione di banche dati e modelli di base.
Al comma II si prevede espressamente che "ai medesimi fini, fermo restando l'obbligo di informativa dell'interessato che può essere assolto anche mediante messa a disposizione di un'informativa generale sul sito web del titolare del trattamento e senza ulteriore consenso dell'interessato ove inizialmente previsto dalla legge, è sempre autorizzato l'uso secondario di dati personali privi degli elementi identificativi diretti, anche appartenenti alle categorie indicate all'articolo 9 del regolamento UE n. 679/2016, da parte dei soggetti di cui al comma 1".
Orbene detti trattamenti (cioè quelli dei commi 1 e 2 appena riportati) devono essere oggetto di approvazione da parte dei comitati etici interessati e devono essere comunicati all'Autorità garante per la protezione dei dati personali e possono essere iniziati decorsi trenta giorni dalla predetta comunicazione se non oggetto di blocco disposto dalla medesima Autorità Garante.
La norma merita una riflessione critica: da un lato, presenta un "vuoto" quanto all'ipotesi della ricerca da parte di soggetti con scopo di lucro e, dall'altro lato, deve altresì essere necessariamente coordinata con quanto prevede il "nuovo" art. 110 (Ricerca medica, biomedica ed epidemiologica), Codice della Privacy (D.Lgs. n. 196/2003) nel testo in vigore dallo scorso primo maggio.
E tale operazione di coordinamento non è affatto scontata.
Il regime autorizzatorio previsto dal DDL (per l'uso secondario dei dati medici) contrasta invero con il diritto dell'U.E. e con il richiamato (nuovo) art. 110 che non solo esclude l'approvazione del Garante (a fronte di un trattamento necessario per un interesse pubblico ovvero quando sia una legge ad attribuirgli finalità pubblica) ma anche la consultazione preventiva del Garante (in riferimento all'uso secondario dei dati medici sempre per ricerca medica), spettando al Garante individuare le garanzie da osservare.
Chiudono il cerchio dell'IA nella sanità le disposizioni in materia di fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità digitale.

## 10. Utilizzo dell'IA in materia di lavoro

Con riferimento al mondo del lavoro il DDL in esame detta il principio generale dell'antropocentrico (art. 10): l'uomo dunque non è destinato ad essere sostituito dalle macchine e all'IA è affidato il compito di migliorare le condizioni di lavoro, di tutelare l'integrità psico-fisica dei lavoratori, di accrescere la qualità delle prestazioni lavorative e la produttività delle persone in conformità al diritto dell'Unione Europea.
Il Legislatore vuole un utilizzo dell'intelligenza artificiale in ambito lavorativo sicuro, affidabile, trasparente e che non si ponga in contrasto con la dignità umana né violi la riservatezza dei dati personali.
È così garantito non solo il diritto del lavoratore ad essere informato dell'utilizzo dell'IA ma anche l'osservanza dei diritti inviolabili del lavoratore senza discriminazioni in funzione del sesso, dell'età, delle origini etniche, del credo religioso, dell'orientamento sessuale, delle opinioni politiche e delle condizioni personali, sociali ed economiche, ancora una volta in conformità con il diritto dell'U.E.

Al tempo stesso è istituito presso il Ministero del Lavoro e delle Politiche Sociali l'osservatorio sull'adozione di sistemi di intelligenza artificiale nel mondo del lavoro (art. 11) – presieduto dal Ministro del Lavoro e delle Politiche Sociali o da un suo rappresentante – per massimizzare i benefici e contenere i rischi derivanti dall'impiego dei sistemi di intelligenza artificiale in ambito lavorativo.
L'Osservatorio avrà il compito di:
- definire una strategia sull'utilizzo dell'IA in ambito lavorativo,
- monitorare l'impatto sul mercato del lavoro,
- identificare i settori lavorativi maggiormente interessati dall'avvento dell'IA,
- promuovere la formazione dei lavoratori e dei datori di lavoro in materia di IA.

## 11. IA e professioni intellettuali

Per le professioni intellettuali, l'art. 12, nei due commi che lo compongono, stabilisce che le decisioni finale sia assunta dal professionista che potrà avvalersi dell'utilizzo di sistemi di IA solo per esercitare attività strumentali e di supporto alla sua attività.
Si prevede, per assicurare il rapporto fiduciario tra professionista e cliente, che le informazioni relative ai sistemi di intelligenza artificiale utilizzati dal professionista siano comunicate al soggetto destinatario della prestazione intellettuale con linguaggio chiaro, semplice ed esaustivo.

## 12. Principi in materia di Pubblica Amministrazione

Si disciplina l'utilizzo dell'IA da parte della P.A. (art. 12) per
- incrementare l'efficienza degli uffici pubblici,
- ridurre i tempi di definizione dei procedimenti amministrativi,
- aumentare qualità e quantità dei servizi erogati ai cittadini e alle imprese.

Il tutto fermo restando che è assicurata agli interessati la conoscibilità del funzionamento e la tracciabilità dell'utilizzo dell'IA che avviene in funzione strumentale e di supporto all'attività provvedimentale in modo che sia garantito il rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale.

## 13. L'utilizzo dell'intelligenza artificiale nell'attività giudiziaria

L'art. 14, nei suoi "soli" e "brevi" due commi che lo compongono, nelle intenzioni del Legislatore disciplina l'impatto della IA sull'amministrazione della giustizia ma, a ben vedere, riporta solo mere petizioni di principio.
La previsione (I comma) secondo cui "i sistemi di intelligenza artificiale sono utilizzati esclusivamente per l'organizzazione e la semplificazione del lavoro giudiziario nonché per la ricerca giurisprudenziale e dottrinale" è non solo eccessivamente generica ma anche priva di disposizioni cogenti che ci si aspettava di trovare nell'economia di un testo di riforma così importante.
E così il Legislatore non affronta, quanto alla giustizia penale (7), i temi oggi più dibattuti in riferimento alle indagini preliminari (si pensi alla "polizia predittiva" (8)) e, in riferimento al dibattimento, all'assunzione delle prove a mezzo dell'IA.
Il Legislatore si limita a porre il principio per cui è sempre riservata al Magistrato la decisione sulla interpretazione della legge, sulla valutazione dei fatti e delle prove e sulla adozione di ogni provvedimento.
Certamente è il Magistrato a decidere ma oggi il codice di rito per il processo penale già prevede le prove atipiche (art. 189 c.p.p.) che spetta al Giudice assumere se idonee ad assicurare l'accertamento dei fatti e non pregiudicano la libertà morale della persona.
E non vi è ragione di ritenere che le prove atipiche generate a mezzo di IA non si possano utilizzare al fine si assumere la decisione finale di un processo penale.
Quanto poi alla giustizia civile l'unico cenno è dato dalla previsione per cui tra le materie di competenza esclusiva del Tribunale civile si aggiungono le cause che hanno ad oggetto il funzionamento di un sistema di intelligenza artificiale (art. 15).
È doveroso a questo punto uno sguardo all'AI ACT che, al considerando 61, riconosce che i sistemi di IA destinati all'amministrazione della giustizia dovrebbero essere classificati come sistemi ad alto rischio, in considerazione del loro impatto potenzialmente significativo sulla democrazia, sullo Stato di diritto, sulle libertà individuali e sul diritto a un ricorso effettivo e a un giudice imparziale.

---

(7) Cfr. Picotti, *Intelligenza artificiale e diritto penale: le sfide ad alcune categorie tradizionali*, in *Diritto penale e processo*, 2024, 3, 293 ss.; Ubertis, *Processo penale telematico, intelligenza artificiale e Costituzione*, in *Cassazione penale*, 2024, 2, 439 ss.

(8) Cfr. Ongaro - Simonini, *Software italiano Giove per la polizia predittiva: pro e contro*, secondo cui "oggi in Italia stiamo assistendo ad un dibattito sulle sorti di Giove, il software di polizia predittiva che sfrutta la tecnologia di *KeyCrime*. *KeyCrime* – sviluppato già nel 2004 per la predizione di rapine commerciali – è utilizzabile per entrambi i settori di pubblica sicurezza e giudiziario. Si tratta di un'IA ibrida tra *person-based* e *place-based predictive policing* con miglioramenti rispetto ai sistemi statunitensi ed europei più noti, quali *PredPol, Palantir, HunchLab e Precob*" reperibile al link <https://www.agendadigitale.eu/documenti/giustizia-digitale/ia-in-polizia-e-giustizia-predittiva-opportunita-e-rischi-del-software-italiano-giove/>.

Sottolinea altresì l'opportunità, al fine di far fronte ai rischi di potenziali distorsioni, errori e opacità, di classificare come ad alto rischio i sistemi di IA destinati a essere utilizzati da un'autorità giudiziaria o per suo conto per assistere le autorità giudiziarie nelle attività di ricerca e interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti.
Anche i sistemi di IA destinati a essere utilizzati dagli organismi di risoluzione alternativa delle controversie a tali fini dovrebbero essere considerati ad alto rischio quando gli esiti dei procedimenti di risoluzione alternativa delle controversie producono effetti giuridici per le parti.
L'utilizzo di strumenti di IA può fornire sostegno al potere decisionale dei Giudici o all'indipendenza del potere giudiziario, ma non dovrebbe sostituirlo: il processo decisionale finale deve rimanere un'attività a guida umana.
Non è tuttavia opportuno estendere la classificazione dei sistemi di IA come ad alto rischio ai sistemi di IA destinati ad attività amministrative puramente accessorie, che non incidono sull'effettiva amministrazione della giustizia nei singoli casi, quali l'anonimizzazione o la pseudonimizzazione di decisioni, documenti o dati giudiziari, la comunicazione tra il personale, i compiti amministrativi.

## 14. Strategia nazionale, autorità competenti, risorse

Con le disposizioni del Capo III il Legislatore intende disciplinare la strategia nazionale per l'IA, le autorità nazionali competenti e il delicato tema delle risorse da investire (9).
All'art. 17 si introduce la strategia nazionale per l'IA, predisposta e aggiornata dalla struttura della Presidenza del Consiglio dei ministri competente in materia di innovazione tecnologica e transizione digitale, d'intesa con le Autorità nazionali di intelligenza artificiale di cui a breve parleremo e sentito il Ministro delle imprese e del *made in Italy* per i profili di politica industriale e di incentivazione e il Ministro della difesa per gli aspetti relativi ai sistemi di intelligenza artificiale impiegabili in chiave duale, ed è approvata con cadenza almeno biennale dal Comitato interministeriale per la transizione digitale (CITD).
Si vuol così favorire la collaborazione tra le PP.AA. e i soggetti privati quanto allo sviluppo e all'adozione di sistemi di IA, il coordinamento dell'attività della P.A. in materia, la promozione della ricerca e della diffusione della conoscenza in materia di IA, anche indirizzando le misure e gli incentivi finalizzati allo sviluppo imprenditoriale e industriale dell'intelligenza artificiale.
Quanto alle cennate autorità nazionali per l'intelligenza artificiale (art. 18) esse sono l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN) con il compito di garantire l'applicazione e l'attuazione della normativa nazionale ed euro-unionale in materia di IA (10).
Ciascuna per quanto di rispettiva competenza, assicurano – tra l'altro – l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di IA conformi alla normativa nazionale e dell'Unione europea, sentito il Ministero della difesa per gli aspetti relativi ai sistemi di intelligenza artificiale impiegabili in chiave duale.
Resta da chiedersi quale sia il ruolo del Garante per la privacy che non viene interessato da questa riforma che si limita a prevedere all'ultimo comma dell'art. 18 che "Restano ferme le competenze, i compiti e i poteri del Garante per la protezione dei dati personali".

## 15. Misure di sostegno ai giovani e allo sport

Il DDL in commento (art. 20) prevede che per poter beneficiare del regime agevolativo a favore dei lavoratori rimpatriati si terrà contro dell'aver svolto un'attività di ricerca nell'ambito delle tecnologie di intelligenza artificiale.
Ed altresì si favorisce l'accessibilità ai sistemi di intelligenza artificiale per il miglioramento del benessere psicofisico attraverso l'attività sportiva, anche ai fini dello sviluppo di soluzioni innovative finalizzate a una maggiore inclusione in ambito sportivo delle persone con disabilità.
Con la precisazione che i sistemi di intelligenza artificiale possono essere utilizzati anche per l'organizzazione delle attività sportive.

## 16. Investimenti nei settori dell'IA

L'art. 21 è la norma dettata in tema di investimenti: in linea con la strategia nazionale e al fine di supportare lo sviluppo di imprese operanti nei settori dell'IA, della cybersicurezza, del calcolo quantistico, delle telecomunicazioni e delle tecnologie per questa abilitanti, è stanziata la somma di un miliardo di euro per l'assunzione di partecipazioni nel capitale di rischio direttamente o indirettamente, di:

a) PMI con elevato potenziale di sviluppo ed innovative, aventi sede operativa in Italia, che operano nelle tecnologie dell'intelligenza artificiale, della cybersicurezza e del calcolo quantistico e delle tecnologie

(9) È autorizzata all'art. 19 la spesa di euro 300.000 annui per ciascuno degli anni 2025 e 2026 per la realizzazione di progetti sperimentali volti all'applicazione dell'IA ai servizi forniti dal Ministero degli affari esteri e della cooperazione internazionale a cittadini e a imprese.

(10) Si affida dunque un compito così delicato ad Autorità strettamente collegate al Governo e non già ad Autorità Amministrative indipendenti.

per queste abilitanti, nonché nel settore delle telecomunicazioni con particolare riferimento al 5G e alle sue evoluzioni, al *mobile edge computing*, alle architetture aperte basate su soluzioni *software*, al Web 3, all'elaborazione del segnale, anche in relazione ai profili di sicurezza e integrità delle reti di comunicazione elettroniche, e che si trovano in fase di sperimentazione (*seed financing*), di costituzione (*start up financing*), di avvio dell'attività (*early-stage financing*) o di sviluppo del prodotto (*expansion, scale up financing*);

b) imprese, anche diverse da quelle innanzi indicate ma comunque finalizzate alla creazione e allo sviluppo di campioni nazionali nei settori e nelle tecnologie di cui si è appena detto.

Tali investimenti saranno effettuati mediante utilizzo delle risorse del Fondo di sostegno al venture capital di cui all'art. 1, comma 209, L. 30 dicembre 2018, n. 145.

## 17. Delega al Governo in materia di IA

Alla centralità dell'uomo, nell'economia dello schema in esame, corrisponde a ben vedere anche la centralità della delega al Governo (art. 22) chiamato così a svolgere un ruolo chiave nel guidare il Paese nella svolta verso l'IA.

In via di estrema sintesi è da rilevare come il Governo sia chiamato: a designare come autorità nazionali competenti ai fini dell'attuazione del regolamento, un'autorità di vigilanza del mercato, un'autorità di notifica, nonché del punto di contatto con le istituzioni dell'U.E.; a percorsi di alfabetizzazione e formazione in materia di IA (in particolare per i professionisti); al potenziamento dell'IA nelle scuole nelle università e nei centri di ricerca.

Il Governo è, altresì, delegato ad adottare uno o più decreti legislativi per definire organicamente la disciplina nei casi di uso di sistemi di intelligenza artificiale per finalità illecite.

## 18. Tutela degli utenti e del diritto d'autore

Il Capo IV si compone degli articoli 23 e 24 così tutelando, da un lato, gli utenti e, dall'altro lato, il diritto d'autore delle opere generate con l'ausilio dell'IA.

Si prevedono, in particolare, nell'ambito del T.U. per la fornitura di servizi di media audiovisivi (11), le misure volte a favorire l'identificazione e il riconoscimento dei sistemi di IA nella creazione di contenuti testuali, fotografici, audiovisivi e radiofonici.

E cioè a dire, quando un contenuto sia stato completamente, o solo parzialmente, generato, ovvero modificato o alterato dai sistemi di IA, in modo tale da presentare come reali dati, fatti e informazioni che non lo sono, dovrà presentare (a cura dell'autore o del titolare dei diritti di sfruttamento economico, se diverso dall'autore) un elemento o segno identificativo, anche in filigrana o marcatura incorporata con l'acronimo "IA" (nel caso di "audio" tale adempimento avverrà attraverso annunci audio ovvero con tecnologie adatte a consentire il riconoscimento).

Si tratta quindi di una marchiatura cui fanno eccezione l'opera o un programma manifestamente creativo, satirico, artistico o fittizio, fatte salve le tutele per i diritti e le libertà dei terzi.

Si rimette poi ad uno specifico regolamento dell'AGCOM il compito di dettare e definire le misure attuative.

Quanto alla tutela del diritto d'autore delle opere generate con l'ausilio di IA si incide nell'ambito della legge sul diritto d'autore (L. 22 aprile 1941, n. 633) prevedendo una disciplina specifica per le opere create con l'ausilio di sistemi di IA, assicurando l'identificazione delle opere e degli altri materiali il cui utilizzo non sia espressamente riservato dai titolari del diritto d'autore.

Ma si ha una vera "tutela del diritto d'autore delle opere generate con l'ausilio dell'intelligenza artificiale"?

A ben vedere il Legislatore della riforma esclude la tutela autoriale in riferimento a quelle opere generate con l'IA (in tal senso già si sono espressi anche altri Paesi U.E. e gli USA): ciò emerge dalle modifiche che si intendono apportare all'art. 1 L. n. 633/1941.

Il primo comma oggi prevede: "Sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione".

Se non vi saranno modifiche al DDL si avrà il seguente nuovo testo: "Sono protette ai sensi di questa legge le opere dell'ingegno «umano» di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione «anche laddove create con l'ausilio di strumenti di intelligenza artificiale, purché costituenti risultato del lavoro intellettuale»" (le parti aggiunte sono riportate tra le virgolette caporali) (12).

Quindi saranno tutelate le opere dell'ingegno umano – e tali saranno anche quelle create con l'ausilio di strumenti di IA purché purché costituenti risultato del lavo-

(11) D.Lgs. 8 novembre 2021, n. 208.

(12) Nella stesura del DDL in esame, antecedente alla bollinatura della Ragioneria Generale dello Stato, si prevedeva – a chiusura della norma – l'aggiunta dell'inciso «", anche laddove create con l'ausilio di strumenti di intelligenza artificiale, purché il contributo umano sia creativo, rilevante e dimostrabile"» formula che aveva, da subito, sollevato più di una perplessità.

ro intellettuale – ma non le opere create esclusivamente con l'IA.
Il tutto senza dimenticare che la L. 27 dicembre 2023, n. 206 (Disposizioni organiche per la valorizzazione, la promozione e la tutela del made in Italy) ha previsto la nuova figura dei "Creatori digitali" (art. 27, I) ovvero "gli artisti che sviluppano opere originali ad alto contenuto digitale".
Con la precisazione che "per tutelare i diritti sulle opere dei creatori digitali, con decreto del Ministro della cultura, da adottare entro novanta giorni dalla data di entrata in vigore della presente legge, è istituito un repertorio delle opere dei creatori digitali nel registro pubblico generale delle opere protette, di cui all'articolo 103 della legge 22 aprile 1941, n. 633" (art. 27, II).
Se vi è dunque un apposito repertorio è ben possibile la richiesta di registrazione di opere frutto integrale dell'IA.
Infine nel DDL in esame si prevede ancora l'introduzione del nuovo art. 70-*septies* (sempre nel contesto della L. n. 633/1941) secondo cui "La riproduzione e l'estrazione di opere o altri materiali attraverso modelli e sistemi di intelligenza artificiale anche generativa, sono consentite in conformità con gli articoli 70-*ter* e 70-*quater*".
In tal modo si consente l'uso di opere protette da parte dei sistemi di IA in uso da parte degli organismi di ricerca e degli istituti di tutela del patrimonio culturale per scopi di ricerca scientifica.

## 19. IA e disposizioni penali

Al quinto ed ultimo capo del DDL troviamo le disposizioni penali, e non poche sono le novità in arrivo. Filo conduttore è il contrasto dell'abuso dell'IA.
Si registra (art. 25) in primis una nuova aggravante (art. 61, I, n. 11-*decies*) consistente nell'avere "commesso il fatto mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato".
Poi ancora si prevede:
b) in tema di sostituzione di persona (art. 494 c.p.) che "La pena è della reclusione da uno a tre anni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale";
c) in tema di rialzo e ribasso fraudolento di prezzi sul pubblico mercato o nelle borse di commercio all'articolo all'art. 501, III, il nuovo n. 2-*bis* secondo cui le pene sono raddoppiate "se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale»;
d) il nuovo art. 612-*quater* che punisce la condotta di "illecita diffusione di contenuti generati o manipolati con sistemi di intelligenza artificiale".
Ancora l'impiego di sistemi di IA sarà punito nei reati di truffa (art. 640 c.p.), di frode informatica (art. 648-*bis* c.p.), di impiego di denaro, beni o utilità di provenienza illecita (artt. 648-*ter* c.p.) e, ancora, nell'aggiotaggio (art. 2637, I, c.c.).
La Legge sul diritto di autore (n. 633/1941) punirà, all'art. 171, I, chi "riproduce o estrae testo o dati da opere o altri materiali disponibili in rete o in banche di dati in violazione degli articoli 70-*ter* e 70-*quater*, anche attraverso sistemi di intelligenza artificiale" e, infine, per l'ipotesi della "Manipolazione del mercato" nel Testo unico delle disposizioni in materia di intermediazione finanziaria (D.Lgs. 24 febbrsaio 1998, n. 58) all'art. 185, I, (secondo cui "chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari, è punito con la reclusione da uno a sei anni e con la multa da euro ventimila a euro cinque milioni"), è aggiunto il seguente periodo: "Se i fatti sono commessi mediante l'impiego di sistemi di intelligenza artificiale, la pena è aumentata".

## 20. IA e disposizioni finanziarie

L'art. 26, ultima norma del DDL qui in esame, ricorre all'ormai nota e diffusa formula di chiusura secondo cui "Dall'attuazione della presente legge non devono derivare nuovi o maggiori oneri a carico della finanza pubblica.
Le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni della presente legge con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente".
Stessa formula si trova adoperata all'ultimo comma dell'art. 11 cit. riferito all'assenza di costi per l'istituzione e il funzionamento dell'Osservatorio sull'adozione di sistemi di IA nel mondo del lavoro.
È un bene, da un lato, l'assenza di nuovi costi per i contribuenti ma occorre, dall'altro lato, riflettere e chiedersi se una riforma a costi zero non sia destinata a rimanere solo una riforma sulla carta.
Riusciranno autorità e ministeri a dare concretezza ad una riforma che necessita sicuramente dell'apporto degli esperti senza intaccare le finanze pubbliche (di là del miliardo di euro già stanziato per le imprese *ex* art. 21 e dalla spesa di euro 300.000 annui per ciascuno degli anni 2025 e 2026 *ex* art. 19)?
Il tempo darà risposta al quesito; certa è, ad oggi, l'esiguità dell'impegno economico pubblico su cui comunque è lecito attendersi l'innesto di forti investimenti privati con innegabili effettivi positivi per il sistema.

# Ammissibilità del modello "pay or consent": tra rivoluzione economica digitale e modernizzazione della protezione dei dati

**di Luca Bolognini, Lorenzo Covello e Giuseppe Fiordalisi**



Il modello 'pay or consent' – con gli opportuni aggiustamenti e rispettando criteri di equivalenza e fungibilità dei servizi a prezzi ragionevoli – potrebbe rappresentare, a parere degli Autori, un approccio valido e legittimo nell'ecosistema digitale, coerente con il quadro legislativo dell'Unione Europea. Tale approccio costituirebbe un bilanciamento dei diritti alla privacy e alla protezione dei dati personali con la libertà di iniziativa economica, nel rispetto dei principi di proporzionalità e ragionevolezza. Effettivamente, il modello in esame introduce un elemento di scelta per gli utenti, offrendo loro la possibilità di decidere attivamente come interagire con i servizi online. Il modello, cioè, consentirebbe di rendere sostenibili – sia dal lato della domanda, sia dal lato dell'offerta – un'ampia gamma di servizi digitali, traducendosi in un meccanismo in grado di bilanciare, da una parte, le esigenze commerciali delle aziende che forniscono i servizi e, dall'altra, la scelta dell'utente di usufruirne concedendo il consenso o, in alternativa, pagando il corrispettivo richiesto che, a meno che non si tratti di un cosiddetto servizio pubblico essenziale (valutazione che dovrebbe essere rimandata al legislatore), potrebbe essere determinato autonomamente dal fornitore nell'esercizio del suo diritto alla libertà di impresa.

*The 'pay or consent' model – with appropriate adjustments and respecting criteria of equivalence and fungibility of services at reasonable prices – may represent, in the Authors' opinion, a valid and legitimate approach in the digital ecosystem, consistent with the current legal framework of the European Union. It would constitute a way to balance the rights to privacy and personal data protection with the freedom to conduct a business, while respecting the constitutional principles of proportionality and reasonableness. Actually, the model under consideration introduces an element of choice for users. The model would make it possible to sustain – both on the demand side and on the supply side – a wide range of online services. A mechanism capable of balancing, on the one hand, the business needs of the companies providing the services and, on the other, the user's choice to make use of them by granting consent or, alternatively, by paying the required fee which, unless it is a so-called essential public service (an assessment that should be referred to the legislator), could be determined autonomously by the provider in the exercise of its right to freedom of enterprise.*

## 1. "Visione di mondo" - Brevi osservazioni sull'evoluzione dei modelli di business, sui principi di bilanciamento tra diritti e libertà fondamentali, e sulla valorizzazione economica del trattamento dei dati personali

L'evoluzione dei modelli di business nell'era digitale rappresenta un argomento vasto e complesso, che si intreccia strettamente con la questione della valorizzazione economica del trattamento dei dati personali. Il tema tocca molti aspetti: dall'economia digitale e dall'innovazione tecnologica alla regolamentazione dei dati personali, che non può non tenere conto dei continui progressi dei sistemi tecnologici e sociali e 'modernizzarsi' di conseguenza.

Come è noto, l'avvento di Internet e la rapida diffusione delle tecnologie digitali hanno trasformato profondamente i modelli di business tradizionali. A partire dagli anni '90 e con l'ascesa del Web 2.0 nei primi anni 2000, si è manifestata una progressiva digitalizzazione delle attività economiche con l'emergere di nuovi modelli di business basati sulla raccolta, l'analisi e la valorizzazione economica del trattamento dei dati, anche personali.

Uno dei cambiamenti più significativi è stato il passaggio da modelli basati sulla produzione e fornitura fisica di beni e servizi a modelli incentrati su contenuti digitali, servizi e piattaforme online. Aziende come Amazon, Google e Facebook (oggi Meta) hanno ridefinito il concetto stesso di business, dimostrando come sia possibile generare valore non solo vendendo prodotti fisici, ma anche scambiando e intermediando beni, servizi, contenuti e informazioni attraverso piattaforme digitali. Parallelamente, si è sviluppata un'economia guidata dai dati (*data-driven*), in cui il potenziale economico è sempre più legato alla capacità di raccogliere, analizzare e creare valore dai dati. I dati sono dunque diventati una risorsa chiave per le aziende, utilizzati per personalizzare i servizi, migliorare l'efficienza operativa, guidare le de-

cisioni strategiche e creare nuovi modelli di business (1). Pertanto, i dati oggi svolgono un ruolo significativo per la competitività e l'innovazione.

In questo quadro di galoppante sviluppo, si inserisce il fattore della regolazione, che non è mai neutrale. Vale, in effetti, la pena di sottolineare che ogni normativa, anche la più tecnica o settoriale, porta con sé e valorizza una particolare "visione del mondo" e ne esclude, o almeno penalizza, altre e diverse. Il Regolamento Generale sulla Protezione dei Dati (Reg. UE 2016/679, "GDPR") non sfugge a questa regola e si pone, da un lato, come strumento per innalzare i livelli di protezione e valorizzazione dei diritti, delle libertà e degli interessi delle persone meritevoli di tutela nell'ordinamento europeo e, dall'altro, come elemento che limita l'estensione di altri diritti, libertà e interessi. Tra questi, sia in positivo (soggetti a potenziamento) sia in negativo (soggetti a limitazione), troviamo senza dubbio le libertà.

L'articolo 16 della Carta dei Diritti Fondamentali dell'Unione Europea, intitolato 'Libertà d'impresa', recita: *È riconosciuta la libertà d'impresa, conformemente al diritto dell'Unione e alle legislazioni e prassi nazionali*. Anche l'articolo 41 della Costituzione italiana sancisce la libertà di iniziativa economica come pilastro fondamentale, sebbene nei limiti stabiliti dall'ordinamento giuridico e dal necessario bilanciamento con altri diritti, libertà e interessi: *L'iniziativa economica privata è libera. Non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla salute, all'ambiente, alla sicurezza, alla libertà, alla dignità umana. La legge determina i programmi e i controlli opportuni perché l'attività economica pubblica e privata possa essere indirizzata e coordinata a fini sociali e ambientali*.

La libertà d'impresa è un diritto fondamentale delle persone fisiche e giuridiche e, in quanto tale, deve essere salvaguardata e non può essere annientata, né dai poteri privati, né dal legislatore, né dalle autorità pubbliche chiamate a far rispettare la legge. È opinione comune che il bilanciamento tra diritti, libertà e interessi non possa essere operato in generale e in astratto, né tanto meno in termini assoluti, ma debba essere condotto caso per caso.

Nell'esercizio di bilanciamento tra diritti e libertà fondamentali e interessi pubblici, gli interpreti devono essere guidati dai principi di proporzionalità e ragionevolezza. Ragionevolezza che, stando alle parole della sentenza della Corte Costituzionale n. 1130 del 1988, «*lungi dal comportare il ricorso a criteri di valutazione assoluti e astrattamente prefissati, si svolge attraverso ponderazioni relative alla proporzionalità dei mezzi prescelti*»; per poi lievitare, questo impasto misto e bilanciato tra proporzionalità e ragionevolezza, nella formula della cosiddetta "*razionalità pratica*", adottata dalla Corte costituzionale con sentenza n. 172 del 1996. Sempre attraverso le parole della Corte Costituzionale, nella sentenza n. 85 del 2013 sul caso ILVA, si acclara che «*tutti i diritti fondamentali tutelati dalla Costituzione si trovano in rapporto di integrazione reciproca e non è possibile, pertanto, individuare uno di essi che abbia la prevalenza assoluta sugli altri. La tutela deve essere sempre "sistemica e non frazionata in una serie di norme non coordinate ed in potenziale conflitto tra loro*" (sentenza n. 264 del 2012). *Se così non fosse, si verificherebbe l'illimitata espansione di uno dei diritti, che diverrebbe "tiranno" nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette, che costituiscono, nel loro insieme, espressione della dignità della persona*».

E qui veniamo all'oggetto di questo breve studio, che intende considerare il bilanciamento tra diritti e libertà fondamentali in relazione a nuovi modelli di relazione socioeconomica. Il concetto di "valorizzazione del trattamento dei dati personali" non si riferisce ai dati personali in sé come merce (questo significato sarebbe incompatibile con la tutela dei dati personali come diritto fondamentale): si riferisce invece all'elaborazione dei dati personali – "concessi in licenza" dagli interessati – come un bene economico a cui può essere attribuito un valore commerciale. Un modello d'avanguardia che certamente presenta sia opportunità sia sfide. Da un lato, lo sfruttamento economico del trattamento dei dati può portare a innovazioni e servizi personalizzati che migliorano l'esperienza dell'utente, dall'altro c'è il rischio che tali pratiche – se mal eseguite o utilizzate con intenzioni non etiche e illegali – possano violare i diritti e le libertà delle persone e creare disuguaglianze.

Un esempio concreto di nuovo "schema di gioco dell'era digitale", in cui le aziende cercano di bilanciare la valorizzazione economica del trattamento dei dati personali, in conformità con l'articolo 16 della Carta dei Diritti Fondamentali dell'UE, con la protezione dei dati personali degli interessati, in particolare nel contesto europeo alla base del GDPR, sono i modelli *'pay or consent'* ("paga o acconsenti"). Questi modelli sono l'oggetto del presente *paper*. In pratica, essi offrono agli utenti, da un lato, la possibilità di pagare un corrispettivo in denaro per accedere a contenuti o servizi online senza che i loro dati personali vengano elaborati per scopi di marketing e/o di *targeting* e, dall'altro, la possibilità di accedere 'gratuitamente' agli stessi contenuti o servizi in cambio della visualizzazione di pubblicità mirata, richiedendo il consenso degli utenti per l'elaborazione dei loro dati personali a fini pubblicitari. Va peraltro sottolineato, a scanso di equivoci, che nei modelli *'pay or consent'* og-

(1) Sui nuovi modelli di monetizzazione dei dati personali e sulle loro basi giuridiche, si veda anche il saggio di Bolognini, *Valorizzazione economica dei dati personali e basi giuridi*che in *Commerciabilità dei dati personali - Profili economici, giuridici, etici della monetizzazione*, a cura di G. Cerrina Feroni, Bologna, 2024, 37.

getto del presente studio non rientrano le profilazioni necessarie a rendere servizi personalizzati richiesti dagli utenti e come tali contrattualizzati, le quali ricadono evidentemente in tutt'altra casistica e base giuridica (es. *ex* art. 6 par. 1.b) GDPR).

Anche in quest'ottica, la Direttiva 2019/770/CE, al Considerando 24, precisa quanto segue: "*La fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico. Tali modelli commerciali sono utilizzati in diverse forme in una parte considerevole del mercato. Oltre a riconoscere appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce, la presente direttiva dovrebbe garantire che i consumatori abbiano diritto a rimedi contrattuali, nell'ambito di tali modelli commerciali. La presente direttiva dovrebbe pertanto applicarsi ai contratti in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o servizi digitali al consumatore e in cui il consumatore fornisce, o si impegna a fornire, dati personali. [...]*".

La scelta per gli utenti tra il pagamento di un servizio o l'ottenimento dello stesso servizio 'gratuito' pagato dagli inserzionisti dalle aziende fornitrici – se acconsentono all'utilizzo dei propri dati personali per scopi di marketing e/o di *targeting* – sta sollevando domande sull'effettività della libertà di scelta e sull'autonomia degli utenti. Per esempio, la protezione dei dati personali può spingersi fino a 'obbligare' le aziende a fornire servizi online gratuiti o, in alcuni casi, a determinare l'equità o l'adeguatezza del prezzo se questo è legato alla concessione del consenso al marketing e/o al targeting come alternativa? Un approccio così assolutizzante alla privacy è adeguato? Un'altra domanda riguarda il tipo di servizi online, che si vorrebbe fossero gratuiti o 'a prezzo equo': potrebbero i *social media* essere considerati servizi pubblici essenziali? L'utente, in definitiva, avrebbe un diritto 'assoluto' di utilizzare servizi come i *social network* o la fruizione di notizie online offerte da professionisti, tra gli altri, gratuitamente o ad un 'prezzo equo'? E, in tal caso, chi sarebbe responsabile della determinazione del 'prezzo equo' o della classificazione dell'importanza pubblica del servizio?

## 2. La validità del consenso come alternativa al pagamento alla luce della legge europea sulla protezione dei consumatori e dei dati

In generale, come accennato nella prima parte del presente *paper*, va ribadito che il diritto alla protezione dei dati personali non è un diritto assoluto. La protezione dei dati deve essere conciliata con altri diritti e libertà fondamentali, sia delle persone fisiche sia di altre persone giuridiche, come riconosciuto dalle Costituzioni e, se vogliamo rimanere eurocentrici, dalla Carta dei Diritti Fondamentali dell'Unione Europea. La semplice lettura del Considerando 4 del GDPR fornisce una conferma inequivocabile di questo assunto: "*Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica*".

Se combiniamo il Considerando 4 del GDPR con l'articolo 52 par. 1 della Carta dei Diritti Fondamentali dell'Unione Europea, in merito al principio di proporzionalità, a cui i legislatori e le istituzioni (e quindi anche le Autorità) sono tenuti in primo luogo, il quadro si completa: "*Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui*".

Va notato che ciò che attiene sia alla protezione dei dati personali, sia, viceversa, alla salvaguardia dei diritti e delle libertà altrui, non può essere soffocato da interpretazione tiranniche e massimaliste.

Inoltre, con riferimento al tema specifico di cui qui ci occupiamo, il legislatore, prima a livello europeo e poi a livello nazionale, ha già più o meno esplicitamente riconosciuto la legittimità delle pratiche commerciali attuate attraverso modelli come quello del '*pay or consent*' in esame, non prescrivendo *ex ante* la nullità o annullabilità di tali rapporti contrattuali in quanto tali, ma sottoponendoli, oltre alle norme ordinarie che regolano la materia contrattuale e a quelle vigenti in materia di protezione dei dati personali, alla legislazione sulla tutela dei consumatori (2).

(2) D'altronde, non è la prima volta che i giuristi prima, e il legislatore poi, nell'inevitabile rincorsa del diritto al progresso della società, si servono dello strumento dell'interpretazione per valutare la legittimità delle prassi e degli usi posti in essere dai consociati. Basti pensare alla cd. *lex mercatoria*, definita da uno dei più illustri giuristi che il nostro ordinamento abbia conosciuto come "*un diritto creato dal ceto imprenditoriale, senza la mediazione del potere legislativo degli Stati, e formato da regole destinate a disciplinare in modo uniforme, al di là delle unità politiche degli Stati, i rapporti commerciali che si instaurano entro l'unità economica dei mercati*", GALGANO, *Diritto civile e commerciale*, I, Padova, 1999, 89 ss. Ancora, come osservato *illo tempore* da determinata dottrina, "*L'applicazione della lex mercatoria al commercio elettronico è dunque un fenomeno già in atto, le cui manifestazioni*

La citata Direttiva UE 2019/770 e, di conseguenza, il Decreto Legislativo italiano modificato n. 206 del 6 settembre 2005 (il 'Codice del Consumo' italiano), hanno il pregio di prevedere il sinallagma "dati personali vs. servizio" come un accordo contrattuale legittimo, quindi riconosciuto e meritevole di tutela da parte dell'ordinamento giuridico. Inoltre, la Direttiva Omnibus 2019/2161 sui diritti dei consumatori menziona espressamente che un servizio può essere fornito in considerazione della fornitura e dell'utilizzo di dati personali.
Il riconoscimento della legittimità, realizzato dalla Direttiva 2019/770/CE e dal Codice del Consumo, del rapporto di sinallagmaticità "dati personali contro servizio digitale", qui inteso come l'assetto contrattuale dove l'interessato fornisce i propri dati personali affinché siano utilizzati per finalità di marketing per finanziare un servizio erogato dal titolare del trattamento, permette di affermare che "*questi dati – ed i metadati ad essi associati – costituiscono un bene oggetto di relazioni economiche e giuridiche*" (3). La legittimità del contratto avente come oggetto tale relazione sinallagmatica è riconosciuta anche, come dettagliato nei paragrafi seguenti, nelle disposizioni e nelle Linee Guida di più di un'Autorità per la protezione dei dati in UE.
La pubblicità personalizzata è stata, poi, considerata un modello di business legittimo dalle corti e dai regolatori dell'UE, nonostante siano stati imposti dei requisiti. Vale la pena di citare la sentenza della CGUE (C-252/21) 147, in cui si afferma che *"[...] la circostanza che l'operatore di un social network online, in quanto titolare del trattamento, occupi una posizione dominante sul mercato dei social network non osta, di per sé, a che gli utenti di tale social network possano validamente acconsentire, ai sensi dell'articolo 4, punto 11, del RGPD, al trattamento dei loro dati personali effettuato da tale operatore* [...]" e che "[...] *gli utenti* [di Facebook] *devono disporre della libertà di rifiutare individualmente, nell'ambito della procedura contrattuale, di prestare il loro consenso a operazioni particolari di trattamento di dati non necessarie all'esecuzione del contratto, senza essere per questo tenuti a rinunciare integralmente alla fruizione del servizio offerto dall'operatore del social network online, il che implica che a detti utenti venga proposta, se del caso a fronte di un adeguato corrispettivo, un'alternativa equivalente non accompagnata da simili operazioni di trattamento di dati* [...]".
Ecco che, volendo prendere in considerazione i profili di legittimità del fenomeno della valorizzazione economica del trattamento dei dati personali nel contesto dello schema negoziale del modello '*pay or consent*', diviene cruciale esaminare e interpretare le disposizioni pertinenti del GDPR. La questione si sposta verso una necessaria indagine sulla legittimità della transazione che coinvolge i dati personali in cambio di servizi, e questa indagine, alla luce delle disposizioni del GDPR, deve concentrarsi principalmente sulla problematica della libertà del consenso al trattamento dei dati.
La questione in Europa riguarda il concetto di consenso liberamente prestato (Art. 7.4 GDPR) al trattamento dei dati personali. In sostanza, il consenso dovrebbe essere un'espressione libera, specifica e informata della volontà dell'individuo, ma il modello *'pay or consent'* potrebbe introdurre una dinamica coercitiva? In altre parole, il libero accesso ai servizi online, condizionato al consenso, potrebbe implicitamente spingere gli utenti/interessati ad accettare l'uso dei loro dati personali anche quando preferirebbero non farlo? Quali fattori devono essere considerati per valutare se il consenso è 'liberamente prestato, specifico, informato e inequivocabile'?

## 3. Le posizioni europee: una strada a più corsie

È necessario analizzare il consenso prestato nell'ambito del modello "paga o acconsenti" alla luce della disciplina europea sulla protezione dei dati, al fine di valutare la legittimità dello "schema negoziale" in questione. La Corte di Giustizia dell'Unione Europea, con la menzionata decisione CJEU (C-252/21) 147 su "Meta Platforms and Others (General terms of use of a social network)" (4), e più di un'Autorità nazionale per la protezione dei dati coinvolta sul tema, hanno contribuito a elaborare una serie di criteri e requisiti il cui soddisfacimento garantirebbe al titolare del trattamento di agire in conformità con le normative vigenti. Questi criteri – come la somiglianza o l'equivalenza dei servizi a cui l'utente avrebbe accesso scegliendo di dare il proprio consenso o, piuttosto, di pagare il corrispettivo richiesto per il servizio, o l'infungibilità dei servizi e la ragionevolezza del prezzo – sebbene espressi in quasi tutte le decisioni pubblicate

*fondamentali sembrano costituite dall'estrema oggettivazione dello scambio, attraverso pratiche contrattuali uniformi, che veicolano il diritto anche attraverso le scelte tecnologiche*" Finocchiaro, in *Diritto di Internet*, Terza edizione, Bologna, 2020, 19 ss.

(3) Resta, Zeno Zencovich, in *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile*, 2018, 416.

(4) Sul tema cfr, Cassano, *Pubblicità personalizzata e formalismo degli interpreti*, nota a Corte di Giustizia dell'Unione Europea; grande sezione; sentenza 4 luglio 2023, n. 252/21, in questa ***Rivista***, 2024, 445. Sulla questione si ricorda altresì, a titolo esemplificativo e non esaustivo, il Provvedimento dell'Autorità Garante austriaca del 20 agosto 2019 nonché le successive FAQ prodotte in materia dalla medesima Autorità nel 2022 (cfr. FAQ zum Thema Cookies und Datenschutz); i criteri di valutazione pubblicati il 16 maggio 2022 dall'Autorità Garante francese, il CNIL (cfr. Cookie walls : la CNIL publie des premiers critères d'évaluation); il Provvedimento del 23 marzo 2023 dell'Autorità Garante tedesca (cfr. DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf) (<datenschutzkonferenz-online.de>) e, ancora, il Provvedimento dell'Autorità Garante danese del 8 febbraio 2023 (cfr. Gul og Gratis' brug af cookie walls (datatilsynet.dk).

finora sul tema, possono essere interpretati e applicati in modo diverso.
Da ultimo, il Parere 08/2024 "on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms", pubblicato dal Comitato Europeo per la Protezione dei Dati (EDPB) in data 17 aprile 2024, ha ulteriormente frammentato il quadro normativo, producendo una serie di riflessioni e di criteri apparentemente applicabili alle sole cd. Piattaforme online di grandi dimensioni.

### *3.1. I criteri di equivalenza e infungibilità dei servizi*

In primo luogo, è necessario enucleare cosa si intende con i concetti di equivalenza e infungibilità dei servizi, delineati nel contesto italiano da fonti giurisprudenziali e decisioni dell'Autorità italiana, Garante per la protezione dei dati personali (di seguito, anche "Autorità Garante"). L'equivalenza dei servizi si riferisce alla possibilità offerta agli utenti di accedere a contenuti o servizi con caratteristiche identiche o molto simili attraverso diverse opzioni di accesso, senza richiedere necessariamente il loro consenso per finalità di marketing e/o profilazione all'uso di cookie (o altri *tracker*) per poter accedere a tali servizi. In altre parole, la libertà di scelta dell'utente tra dare o meno il consenso è considerata valida quando esiste un'alternativa che consente di utilizzare un servizio o un contenuto sostanzialmente analogo, indipendentemente dalla modalità di accesso scelta. Il concetto è rinvenibile nel Provvedimento n. 231 del 10 giugno 2021, pubblicato sulla Gazzeta Ufficiale n. 163 del 9 luglio 2021, emanato dall'Autorità Garante e recante le "Linee Guida sull'utilizzo dei cookie" (5). Nella suddetta decisione, l'Autorità Garante ha specificato che l'uso del 'cookie wall', che richiede agli utenti di accettare i cookie per accedere ai contenuti, è generalmente inammissibile. Un'eccezione può essere presa in considerazione solo in circostanze specifiche e comunque valutate caso per caso, laddove l'editore del sito permetta l'accesso a contenuti o servizi equivalenti/simili senza richiedere il consenso per l'utilizzo di cookie o altri meccanismi di tracciamento. In sostanza, le suddette Linee Guida non considerano illegittimo il modello *'pay or consent'*, nel senso che non si pronunciano sul merito di esso, limitandosi a suggerire un orientamento interpretativo "condizionante".
Per quanto riguarda il principio della 'fungibilità della prestazione', espresso nella sentenza della Corte di Cassazione n. 17278 del 2 luglio 2018 (6), esso implica che il servizio stesso può essere considerato fungibile se l'utente può rinunciare al servizio senza subire un "gravoso sacrificio". Nella pratica, in virtù del suddetto principio, gli operatori di siti web sarebbero autorizzati a richiedere il consenso al trattamento dei dati personali per scopi pubblicitari come condizione per accedere a determinati servizi, a condizione che il consenso sia dato in modo libero, specifico, informato e inequivocabile per tali scopi, e la fungibilità si basi sulla possibilità di sostituire il servizio con altri simili disponibili, senza che ciò comporti un onere troppo pesante per l'utente. In altre parole, la Sentenza *de qua* stabilisce che, quanto più il servizio offerto è essenziale e indispensabile per l'utente, quindi infungibile e non disponibile attraverso altre fonti, tanto meno è legittimo assoggettarlo alla condizione del rilascio del consenso.

### *3.2. Il criterio della ragionevolezza del prezzo*

Più di un'Autorità nazionale per la protezione dei dati (7), nonché l'EDPB con il suddetto Parere 08/2024, pronunciandosi sulla liceità del modello *'pay or consent'*, ha affermato che, per considerare il consenso eventualmente dato dall'interessato come libero e conforme alle disposizioni del GDPR, l'alternativa a pagamento proposta dal titolare del trattamento deve poter essere considerata "ragionevole", nel senso di non essere sproporzionata, completamente irrealistica, irragionevolmente alta o così alta che la persona registrata non abbia realmente una scelta (cioè tale che il compenso non crei una situazione di "significativa costrizione economica").

(5) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876#english>.

(6) Corte di Cassazione n. 17278 del 2 luglio 2018: "[...] *Ritiene la Corte, nel quadro di applicazione del citato art. 23, che la risposta al quesito non possa essere univoca e, cioè, che il condizionamento non possa sempre e comunque essere dato per scontato e debba invece essere tanto più ritenuto sussistente, quanto più la prestazione offerta dal gestore del sito Internet sia ad un tempo infungibile ed irrinunciabile per l'interessato, il che non può certo dirsi accada nell'ipotesi di offerta di un generico servizio informativo del tipo di quello in discorso, giacché all'evidenza si tratta di informazioni agevolmente acquisibili per altra via, eventualmente attraverso siti a pagamento, se non attraverso il ricorso all'editoria cartacea, con la conseguenza che ben può rinunciarsi a detto servizio senza gravoso sacrificio. Non può allora essere condiviso l'argomento svolto dal giudice di merito secondo cui, dando credito alla tesi sostenuta dal Garante, si finirebbe per "delineare una sorta di obbligo tout court, per il gestore del portale, di offrire comunque le proprie prestazioni, a prescindere dalla prestazione del consenso al trattamento dei dati personali da parte dell'utente": e, in buona sostanza, per obbligare così il gestore del portale a rinunciare al tornaconto economico dell'operazione che egli compie, proveniente dall'attività pubblicitaria realizzata tramite l'impiego dei dati personali acquisiti. Nulla, infatti, impedisce al gestore del sito - beninteso, si ripete, in un caso come quello in questione, concernente un servizio né infungibile, né irrinunciabile -, di negare il servizio offerto a chi non si presti a ricevere messaggi promozionali, mentre ciò che gli è interdetto è utilizzare i dati personali per somministrare o far somministrare informazioni pubblicitarie a colui che non abbia effettivamente manifestato la volontà di riceverli. Insomma, l'ordinamento non vieta lo scambio di dati personali, ma esige tuttavia che tale scambio sia frutto di un consenso pieno ed in nessun modo coartato. [...]*".

(7) Vedere nota 5.

Mentre la conduzione di un'indagine teleologica facilita l'individuazione della logica sottostante al criterio in esame, un'accurata interpretazione letterale pone più di un problema critico.
Argomentando in questo modo, è chiaro che le Autorità per la protezione dei dati desiderano evitare una situazione in cui l'interessato, dovendo decidere se dare il consenso o pagare un prezzo esagerato, sia *de facto* costretto a limitare il suo diritto alla protezione dei dati personali per poter usufruire di un determinato servizio (8). Tuttavia, il criterio della ragionevolezza del prezzo, e in particolare l'uso dell'aggettivo "ragionevole", sebbene apprezzabile nella sua logica, solleva più di una riflessione sulla sua applicazione.
Volendo procedere in ordine logico-giuridico, si dovrebbero per esempio approfondire due questioni. Da un lato, infatti, è necessario individuare le caratteristiche che, se presenti, rendono 'ragionevole' un determinato prezzo. Dall'altro lato, è inevitabile un'indagine su chi sia il soggetto deputato a verificare l'eventuale irragionevolezza del prezzo richiesto in alternativa al consenso in relazione al modello *'pay or consent'*. In riferimento alla prima domanda, è sufficiente rappresentare come, in una società liberal-capitalista come quella europea di oggi, il prezzo sia ragionevole in quanto percepito come equo dal consumatore, e possa essere considerato non sproporzionato in riferimento al valore del particolare servizio per i consumatori, nonché confrontando il prezzo con i prodotti e servizi concorrenti sul mercato. Quindi, si potrebbe dire che il mercato si regola da solo, attraverso le varie interazioni tra domanda e offerta, per un determinato bene o servizio. Per fare un esempio banale, i prodotti di moda dei marchi di lusso hanno un valore intrinseco percepito dal consumatore molte volte superiore al loro costo di produzione.
In relazione alla seconda domanda, invece, dato che il controllo della ragionevolezza del prezzo non può rientrare completamente nell'ambito dei poteri delle Autorità Nazionali per la Protezione dei Dati (9) (che avranno una capacità limitata di valutare l'adeguatezza del prezzo, ad esempio limitata a confermare che il prezzo non sia sproporzionato o crei una situazione di "significativa costrizione economica"), è essenziale identificare gli eventuali altri soggetti, quali Autorità indipendenti competenti per altri settori, a cui affidare questo controllo.
In conclusione, il titolare del trattamento dei dati intenzionato a utilizzare il modello *'pay or consent'*, in un misto sbilanciato di rischio d'impresa e principio di responsabilità, dovrà determinare autonomamente il prezzo ragionevole per l'utilizzo del suo servizio.

### *3.3. Applicabilità degli stessi criteri alle discipline e-privacy e DMA*

Come riflessione finale, ci si potrebbe chiedere se il ragionamento sopra esposto – con i suoi criteri e condizionamenti, ancora incerti ma già visibili in filigrana nel quadro giuridico europeo – sia applicabile anche alle discipline dell'e-privacy e del Digital Markets Act.
La Direttiva 2002/58/CE (direttiva relativa alla vita privata e alle comunicazioni elettroniche, cd. e-privacy) chiarisce al Considerando 17: "*Ai fini della presente direttiva il consenso dell'utente o dell'abbonato, senza considerare se quest'ultimo sia una persona fisica o giuridica, dovrebbe avere lo stesso significato del consenso della persona interessata come definito ed ulteriormente determinato nella direttiva 95/46/CE. Il consenso può essere fornito secondo qualsiasi modalità appropriata che consenta all'utente di esprimere liberamente e in conoscenza di causa i suoi desideri specifici, compresa la selezione di un'apposita casella nel caso di un sito Internet.*"
Anche l'art. 5 par. 2 del Digital Markets Act (DMA, Reg. (UE) 2022/1925) introduce l'obbligo per cui "*il gatekeeper: a) non tratta, ai fini della fornitura di servizi pubblicitari online, i dati personali degli utenti finali che utilizzano servizi di terzi che si avvalgono di servizi di piattaforma di base del gatekeeper; b) non combina dati personali provenienti dal pertinente servizio di piattaforma di base con dati personali provenienti da altri servizi di piattaforma di base o da eventuali ulteriori servizi forniti dal gatekeeper o con dati personali provenienti da servizi di terzi; c) non utilizza in modo incrociato dati personali provenienti dal pertinente servizio di piattaforma di base in altri servizi forniti separatamente dal gatekeeper, compresi altri servizi di piattaforma di base, e viceversa; e d) non fa accedere con registrazione gli utenti finali ad altri servizi del gatekeeper al fine di combinare dati personali, a meno che sia stata presentata all'utente finale la scelta specifica e quest'ultimo abbia dato il proprio consenso ai sensi dell'articolo 4, punto 11), e dell'articolo 7 del regolamento (UE) 2016/679*".
In entrambi gli scenari, sia e-privacy sia DMA, sono richiesti consensi specifici per trattamenti di dati che ricadono nelle rispettive discipline. Ci si può domandare, dunque, se il modello '*pay or consent*', nei limiti e alle condizioni che sembrano emergere come percorribili con riferimento al "consenso GDPR", siano applicabili anche nel caso dei consensi aggiuntivi impo-

(8) Sul possibile squilibrio e sull'adeguatezza del prezzo, si veda anche Mikołaj Barczentewicz, 'Pay or consent': Personalized ads, the rules and what's next, IAPP Portal, 20 November 2023 <https://iapp.org/news/a/pay-or-consent-personalized-ads-the-rules-and- whats-next/>.

(9) Al riguardo, si rappresenta come, in primo luogo, non sia rinvenibile un tale potere e responsabilità nella normativa che regola l'operato di siffatte Autorità. In secondo luogo, l'attribuzione della valutazione in esame in capo alle Autorità Garanti nazionali potrebbe condurre a decisioni diverse in merito alla ragionevolezza dello stesso prezzo, applicato per il medesimo servizio ma in Paesi europei differenti, con conseguente potenziale violazione dei principi europei di libera concorrenza nonché, se del caso, danno al mercato unico europeo.

sti da queste ulteriori norme. In tale ottica, la risposta sembra venire direttamente dal testo di tali strumenti legislativi: sia nella direttiva e-privacy, sia nel DMA, si sottolinea espressamente che il consenso va inteso come definito nel GDPR: dunque, a parere degli Autori, gli stessi possibili criteri condizionanti di ammissibilità dell'alternativa tra pagamento e consenso validi per il GDPR dovrebbero poter applicarsi anche alle casistiche di consensi e-privacy e/o DMA.

## 4. Conclusioni

In conclusione, si nota che il modello *'pay or consent'* – con gli opportuni aggiustamenti e rispettando criteri di equivalenza e fungibilità dei servizi a prezzi ragionevoli – potrebbe rappresentare, a parere degli Autori, un approccio valido e legittimo nell'ecosistema digitale, coerente con il quadro legislativo dell'Unione Europea. Dopotutto, il modello in esame introduce un elemento di scelta per gli utenti, offrendo loro la possibilità di decidere attivamente come interagire con i servizi online. Il modello, cioè, consentirebbe di rendere sostenibili – sia dal lato della domanda, sia dal lato dell'offerta – un'ampia gamma di servizi digitali, traducendosi in un meccanismo in grado di bilanciare, da una parte, le esigenze commerciali delle aziende che forniscono i servizi e, dall'altra, la scelta dell'utente di usufruirne concedendo il consenso o, in alternativa, pagando il corrispettivo richiesto che, a meno che non si tratti di un cosiddetto servizio pubblico essenziale (valutazione che dovrebbe essere rimandata al legislatore), potrebbe essere determinato autonomamente dal fornitore nell'esercizio del suo diritto alla libertà di impresa.

# La Corte di Giustizia dell'Unione europea fa il punto sui danni da violazione dei dati personali

**di Caterina Brignolo**



Il saggio approfondisce il tema della responsabilità di cui all'art. 82 del Regolamento 2016/679/Ue a seguito della sentenza della Corte di Giustizia UE del 14 dicembre 2023, nella causa C-340/2021, che, pronunciandosi sul fondamento dell'inversione dell'onere della prova sull'adeguatezza dei trattamenti e sul contenuto dell'esimente di cui al paragrafo 3 dell'art. 82, permette una riflessione sulla natura giuridica della fattispecie. Sulla scorta della pronuncia, il lavoro si sofferma, infine, sulla risarcibilità a titolo di danno immateriale del solo timore di un potenziale utilizzo abusivo dei dati personali da parte di terzi, conseguente a una violazione del Regolamento.

*The essay analyzes the issue of the liability in Article 82 of the GDPR following the judgment of the Court of Justice of the European Union on December 14, 2023, in the case C-340/21, that, ruling on the base of the reversal of the burden of proof on adequacy of treatment and the meaning of the exemption from liability in Article 82 (3) of the GDPR, allows a reconsideration on the legal nature of the case. On the basis of the judgment, the article examines the compensation even of the mere fear experienced by a data subject with regard to a possible misuse of his or her personal data by third parties as a result of an infringement of that regulation.*

## 1. Premessa

La Corte di Giustizia dell'Unione Europea, con la sentenza del 14 dicembre 2023, nella causa C-340/2021, a quasi trent'anni dall'emanazione della Direttiva 95/46/Ce, pone dei punti fermi circa la natura e la portata della responsabilità civile per la violazione dei dati personali, contemplata oggi dall'art. 82 del Regolamento 2016/679/Ue (GDPR).

La sentenza si pone in continuità con gli approdi della giurisprudenza europea laddove ribadisce che l'art. 82 GDPR, in quanto disposizione di carattere comunitario, deve essere interpretato secondo i canoni ermeneutici e giurisprudenziali propri del diritto dell'Unione e che l'obbligo risarcitorio scaturisce in capo al titolare del trattamento in presenza di tre presupposti: la violazione di una regola di condotta posta dal Regolamento, la presenza di un danno e del nesso causale tra la violazione e il danno.

La pronuncia pone, invece, un inedito tassello in merito al tema, ancora aperto, dell'imputabilità della responsabilità *ex* art. 82 GDPR, allorché afferma che la violazione dei dati personali non è di per sé prova dell'inadeguatezza delle misure tecniche e organizzative adottate dal titolare, che dovrà essere valutata di volta in volta con riferimento al caso concreto.

Chiarisce altresì che, nell'ambito di un giudizio sulla responsabilità del titolare per la violazione dei dati personali, l'onere della prova dell'adeguatezza delle misure, anche di sicurezza, grava in capo al titolare e che l'inversione dell'onere della prova si fonda sul principio di *accountability ex* artt. 5 e 24, in combinato disposto con i paragrafi 1 e 2 dell'art. 82 GDPR. L'esimente di cui al paragrafo 3 dell'art. 82 riguarda, invece, l'esclusione del nesso causale, pur in presenza di un'accertata violazione dell'obbligo di protezione.

Con riferimento al perimetro del danno immateriale risarcibile, la sentenza conferma i propri precedenti, secondo cui una normativa o una prassi di diritto interno volta a stabilire una soglia di gravità al danno immateriale risarcibile sarebbe in contrasto con la disciplina comunitaria. Afferma infine che il solo timore di un potenziale utilizzo abusivo dei dati personali, da parte

di terzi, può di per sé costituire un danno immateriale risarcibile, se concreto e fondato.

## 2. La continuità della disciplina contenuta nell'art. 82 del GDPR rispetto all'art. 23 della Direttiva 95/46/Ce

L'art. 23 della Direttiva 95/46/Ce contemplava già il diritto di ottenere il risarcimento dei danni, conseguenti a un «*trattamento illecito*», dal «*responsabile del trattamento*» (figura che corrisponde al «*titolare del trattamento*» secondo le definizioni del GDPR (1)), salva la prova che l'evento dannoso non fosse a quest'ultimo imputabile.
Al considerando 55, la Direttiva esemplificava i casi di esclusione della responsabilità, prevedendo che l'evento dannoso non fosse imputabile al responsabile se questi provava «*l'esistenza di un errore della persona interessata o un caso di forza maggiore*».
L'ordinamento italiano dava attuazione alla Direttiva 95/46/Ce, in un primo tempo, con la l. 31 dicembre 1996, n. 675 prevedendo all'art. 18 che «*Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile*».
L'art. 29 della citata legge prevedeva anche esplicitamente la risarcibilità del danno non patrimoniale, senza tuttavia richiamare né l'art. 18 della medesima legge né l'art. 2050 c.c.: era quindi sorto il dubbio che l'onere probatorio gravante sul danneggiato che chiedeva i danni non patrimoniali fosse assoggettato alla regola ordinaria, più gravosa di quella prevista dall'art. 18 mediante il richiamo all'art. 2050 c.c. (2).
Successivamente il Codice della *Privacy*, introdotto con il d.lgs. 30 giugno 2003, n. 196, regolava il diritto al risarcimento del danno all'art. 15, che al comma 1 riproponeva, sostanzialmente invariato, il testo dell'art. 18 della l. n. 675 del 1996 e al comma 2 prevedeva esplicitamente la risarcibilità del danno non patrimoniale, superando definitivamente i dubbi circa la diversificazione del regime probatorio (3).
Con riguardo al criterio di imputazione della responsabilità e al susseguente tema della prova liberatoria, autorevole dottrina (4) ha sostenuto che l'art. 82 GDPR non ribalta il criterio di imputazione né la *ratio* dell'illecito che aveva caratterizzato la legislazione precedente (5) e che la lettura più corretta della nuova disposizione è quella che la pone in assoluta continuità con il regime previgente (6).
La Corte di Cassazione pronunciandosi su un'ipotesi di trattamento illecito dei dati personali ancora regolato dal d.lgs. n. 196 del 2003 ha affermato, in un *obiter dictum*, che il GDPR conferma lo schema della responsabilità oggettiva delineato dall'art. 15 Codice della *Privacy*, in quanto la prova liberatoria di cui all'art. 82, par. 3, GDPR coincide con quella del sistema interno previgente: il titolare del trattamento deve fornire «*la prova positiva di aver valutato autonomamente il rischio di impresa, purché tipico, cioè prevedibile, e attuato le misure organizzative e di sicurezza tali da eliminare o ridurre il rischio connesso alla sua attività*» (7).
Bisogna tuttavia considerare che l'art. 15 Codice della *Privacy*, sebbene sia una norma di attuazione di una fonte comunitaria, ha origine nell'ordinamento giuridico italiano, mentre l'art. 82 GDPR è una norma regolamentare direttamente applicabile senza intermediazione della legge nazionale (8). Anche nel linguaggio, l'art. 82 GDPR si pone in continuità più con l'art. 23 della Direttiva 95/46/Ce (9), che con l'art. 15 Codice della *Privacy*, peraltro oggi espressamente abrogato dall'art. 27 del d.lgs. 10 agosto 2018, n. 101 (10).

## 3. La tesi che sostiene la natura oggettiva della responsabilità *ex* art. 82 GDPR

Parte della dottrina (11) accoglie la qualificazione della responsabilità civile per il trattamento dei dati personali

(1) Ai sensi dell'art. 4, n. 7, GDPR «*ai fini del presente regolamento s'intende per «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*».

(2) Palmerini, *Responsabilità da trattamento illecito dei dati personali*, in Navarretta (a cura di), *Codice della responsabilità civile*, Milano, 2021, 2475.

(3) Palmerini, *ibidem*.

(4) Riccio, *Art. 82. Diritto al risarcimento e responsabilità*, in Riccio - Scorza - Belisario (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2018, 596 ss.; S. Sica, *Art. 82. Diritto al risarcimento e responsabilità*, in D'Orazio - Finocchiaro - Pollicino - Resta (a cura di), *Codice della privacy e data protection*, Milano, 2021, 891 ss.

(5) Riccio, *Art. 82*, cit., 597.

(6) Sica, *Art. 82*, cit., 891.

(7) Cass. 17 settembre 2020, n. 19328, in *Nuova giur. civ. comm.*, 2021, 142 ss., con nota di Solinas, *Danno non patrimoniale e violazione del diritto alla protezione dei dati personali*.

(8) Navone, *Ieri, oggi e domani della responsabilità civile da illecito trattamento dei dati personali*, in *Nuove leggi civ. comm.*, 2022, 139.

(9) Salanitro, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di Giustizia*, in *Riv. dir. civ.*, 2023, 430.

(10) Navone, *Ieri*, cit., 138.

(11) Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Milano, 2019, 49 ss.; Camardi, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in *Juscivile*, 2020, 786 ss.; Bilotta, *La responsabilità civile nel trattamento dei dati personali*, in Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del*

in termini di responsabilità oggettiva per rischio d'impresa (12).
Secondo questo orientamento le disposizioni che regolano il potere del titolare sui dati e le modalità del suo esercizio non sono meramente regole di condotta, ma costituiscono delle vere e proprie obbligazioni di risultato, che impongono al titolare di impedire il verificarsi di violazioni dei dati (13).
L'art. 82 GDPR sarebbe una declinazione settoriale della categoria della responsabilità oggettiva per rischio d'impresa (14), tesi avvalorata dalle disposizioni del Regolamento che sottolineano il carattere pericoloso dell'attività di trattamento dei dati e istituiscono un conseguente approccio basato "sul rischio" (15).
La dottrina che si occupa della responsabilità oggettiva per rischio tipico afferma che la responsabilità si estende a tutto il maggior rischio creato, superiore alla normale tollerabilità, salvi i limiti derivanti da una particolare descrizione legislativa (16). Un esempio di tali limiti è rappresentato dall'obbligo di adottare misure adeguate (17), che emerge in via generale dall'art. 5, par. 1, lett. f, GDPR, in forza del quale per ogni trattamento devono essere adottate le misure tecniche e organizzative adeguate a garantire la sicurezza e la protezione dei dati (18).
Si parla, in proposito, di responsabilità oggettiva per rischio evitabile (19), in quanto tale responsabilità risulta limitata in ragione del fatto oggettivo che siano state, o meno, adottate le misure offerte dalla tecnica, idonee a evitare il danno, tenendo conto dei fattori espressamente menzionati all'art. 32 GDPR, tra i quali lo stato dell'arte e i costi di attuazione (20).
La responsabilità è esclusa, inoltre, per gli eventi eccezionali di gravità sproporzionata al rischio creato (21), che risulterebbe irragionevole e sproporzionato attribuire al soggetto (22), come gli eventi che presentano i caratteri del caso fortuito (23).
La non imputabilità «*in alcun modo*» prevista dall'art. 82, par. 3, GDPR comporterebbe, dunque, la responsabilità del titolare per il rischio evitabile, anche raro, restando escluso quello atipico e imprevedibile (24).

## 4. La tesi dell'imputazione a titolo di colpa della responsabilità *ex* art. 82 GDPR

Altra dottrina (25) configura la responsabilità del titolare del trattamento ai sensi dell'art. 82 GDPR quale responsabilità soggettiva per colpa.
Il Regolamento detta una disciplina dell'attività di trattamento dei dati personali fondata sulla prevenzione e la valutazione del rischio (26) e fissa i principi e le regole del trattamento, anche attraverso la previsione di puntuali obblighi di condotta per il titolare (27).
Si afferma, dunque, che la violazione del Regolamento che fa scaturire la responsabilità in questione è, di norma, una violazione di regole di condotta (28).
In particolare, l'art. 24 GDPR prevede che il titolare del trattamento debba attuare misure tecniche e organizzative adeguate a garantire ed essere in grado di dimostrare che il trattamento è conforme al Regolamento: il titolare viene lasciato libero di adottare le misure adeguate, salvo poi essere in grado di dimostrare la *ratio* e la ragionevolezza delle valutazioni discrezionali effettuate (29).
Anche l'art. 5, par. 1, lett. f, GDPR stabilisce che i dati devono essere trattati in maniera tale da garantire la sicurezza, «*compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*».

*mercato*, Milano, 2019, 445 ss.; Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, 2018, 125.

(12) Tosi, *Responsabilità*, cit., 136; G. Calabrese, *Il danno da "perdita di controllo dei dati personali" nel pensiero della Corte di Giustizia UE*, in *Nuova giur. civ. comm.*, 2023, 1114.

(13) Bilotta, *La responsabilità*, cit., 642.

(14) Tosi, *Responsabilità*, cit., 121.

(15) Camardi, *Note critiche*, cit., 795.

(16) Trimarchi, *La responsabilità civile: atti illeciti, rischio, danno*, Milano, 2021, 574.

(17) Tosi, *Responsabilità*, cit., 131.

(18) Malgieri, *Art. 5. Principi applicabili al trattamento di dati personali*, in D'Orazio et al. (a cura di), *Codice*, cit., 188.

(19) Trimarchi, *La responsabilità civile*, cit., 309.

(20) Esposito, *Art. 32. Sicurezza del trattamento*, in D'Orazio et al. (a cura di), *Codice*, cit., 506.

(21) Trimarchi, *La responsabilità civile*, cit., 576.

(22) Tosi, *Responsabilità*, cit., 121.

(23) Trimarchi, *ibidem*.

(24) Tosi, *Responsabilità*, cit., 122.

(25) Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, in Cuffaro - D'Orazio - Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 1017 ss.; Id., *Principio di responsabilità e tutela aquiliana dei dati personali*, Napoli, 2018, 68 ss.; Caterina - Thobani, *Il diritto al risarcimento dei danni*, in *Giur. it.*, 2019, 2805 ss.; Ratti, *La responsabilità da illecito trattamento dei dati personali nel nuovo regolamento*, in Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 615 ss.

(26) Mollo, *Gli obblighi previsti in funzione di protezione dei dati personali*, in Zorzi Galgano (cur.), *Persona e mercato dei dati: riflessioni sul GDPR*, Padova, 2019, 262.

(27) Gambini, *Principio*, cit., 76.

(28) Salanitro, *Illecito*, cit., 439.

(29) Pizzetti - Greco, *Art. 24. Responsabilità del titolare del trattamento*, in D'Orazio et al. (a cura di), *Codice*, cit., 405.

Il combinato disposto di queste norme, in materia di misure di sicurezza, solo apparentemente impone il conseguimento di un risultato in quanto, in realtà, obbliga all'adozione di misure normalmente osservabili da un operatore del settore economico di riferimento, per mantenere la sicurezza e prevenire i pregiudizi che possano derivare dall'attività svolta (30).
Secondo tale lettura delle disposizioni del Regolamento, non emerge in capo al titolare un obbligo di evitare il danno e pertanto la regola vigente, di matrice europea, riduce la tutela dei dati personali rispetto alla previgente normativa nazionale, che faceva richiamo alla disciplina più rigorosa dell'art. 2050 c.c. (31).
In tale prospettiva, il danno da violazione della *privacy* viene a configurarsi quale conseguenza colposa della mancata adozione delle misure tecniche e organizzative, anche di sicurezza, ragionevoli e comunque adeguate a scongiurarlo (32).
Se una violazione dei dati oggettivamente vi è stata, il titolare del trattamento può liberarsi da responsabilità dimostrando che l'evento dannoso non è in alcun modo a lui imputabile e l'evento non sembra possa dirsi imputabile, qualora il titolare dimostri di aver rispettato gli obblighi posti a suo carico (33).
Tale contenuto della prova liberatoria è conforme al principio di *accountability* (34), perché sarebbe poco coerente predisporre, come fa il Regolamento, un sistema volto a obbligare chi tratta i dati ad adottare una serie di misure e strumenti finalizzati non solo a garantire la liceità del trattamento, ma anche a dimostrare il rispetto delle prescrizioni normative, per poi non ammettere che tale dimostrazione sia idonea a escludere la responsabilità (35).
Con riguardo all'articolazione dell'onere probatorio, la dottrina prevalente riconduce alla nozione di non imputabilità di cui all'art. 82, par. 3, GDPR sia le ipotesi di caso fortuito, forza maggiore e fatto del danneggiato (eventi tradizionalmente considerati interruttivi del nesso causale), sia la dimostrazione da parte del titolare del trattamento di aver posto in essere tutte le misure di protezione possibili secondo la diligenza professionale (36).
Questa interpretazione estesa dell'art. 82, par. 3, GDPR è consentita dal fatto che nel Regolamento le tradizionali cause oggettive e assolute di non imputabilità della forza maggiore o del fatto del danneggiato non sono segnatamente richiamate, come invece accadeva nella Direttiva 95/46/Ce al considerando 55, ma sostituite dal generico riferimento a un evento dannoso che non è in alcun modo imputabile al danneggiante (37).
Tale impostazione trova pieno riscontro anche nelle *Conclusioni dell'Avvocato generale* nell'ambito della causa decisa con la sentenza della Corte giustizia UE del 14 dicembre 2023, C-340/2021, nelle quali si afferma che l'art. 82 GDPR «*non sembra individuare un regime di responsabilità oggettiva*», che il danno da violazione dei dati personali può configurarsi quale conseguenza colposa della mancata adozione delle misure tecniche e sussiste una «*responsabilità aggravata per colpa presunta*» (38). Si precisa inoltre che l'art. 82, par. 3, del Regolamento dispone una forma di inversione dell'onere della prova della colpa del danneggiante, in piena simmetria con l'inversione dell'onere della prova dell'adeguatezza delle misure adottate, perché «*il titolare del trattamento si trova nella migliore posizione per offrire la prova liberatoria per dimostrare che l'evento dannoso non gli è in alcun modo imputabile*» (39).

## 5. Il caso di cui si è occupata la Corte

L'Agenzia nazionale per le entrate pubbliche della Bulgaria era stata oggetto di un accesso non autorizzato da parte di terzi (c.d. *hacker*) che ha comportato la diffusione su *internet* dei dati personali contenuti nel sistema e appartenenti a più di sei milioni di persone fisiche, sia bulgare che straniere.
La ricorrente, che aveva visto i suoi dati pubblicati su *internet*, aveva convenuto in giudizio l'Agenzia richiedendo il risarcimento del danno consistente «*nel timore che i suoi dati personali che sono stati pubblicati senza il suo consenso siano oggetto di un utilizzo abusivo, in futuro, o che essa subisca un ricatto, un'aggressione, o addirittura un rapimento*» (40).
La Corte suprema amministrativa della Bulgaria, con la decisione del 14 maggio 2021, sospendeva il procedimento chiedendo alla Corte di Giustizia UE di pronunciarsi su cinque questioni pregiudiziali.

(30) Gambini, *Principio*, cit., 78.

(31) Salanitro, *Illecito*, cit., 429.

(32) Gambini, *Principio*, cit., 83.

(33) Caterina - Thobani, *Il diritto*, cit., 2806.

(34) Gambini, *ibidem*.

(35) Caterina - Thobani, *Il diritto*, cit., 2807. Lo stesso argomento è stato successivamente esposto in termini pressoché identici nella sentenza oggetto del presente saggio, CGUE 14 dicembre 2023, C-340/2021, in *One legale*, punto 34; in questa ***Rivista***, 2024, 49, con nota di Russo, *CGUE, danno morale e data breach: il timore da utilizzo illecito dei dati personali*.

(36) Caterina - Thobani, *Il diritto*, cit. 2805.

(37) Gambini, *ibidem*.

(38) Pitruzzella, *Conclusioni dell'Avvocato generale* presentate il 27 aprile 2023 nella causa C-340/2021, punti 61 e 62.

(39) Pitruzzella, *Conclusioni dell'Avvocato generale*, cit., punto 63.

(40) CGUE 14 dicembre 2023, C-340/2021, cit., punto 13.

## 6. La violazione dei dati personali non è di per sé prova dell'inadeguatezza delle misure tecniche e organizzative

La prima pregiudiziale pone il problema se ogni volta che si sia verificata una violazione dei dati personali, in particolare una divulgazione o un accesso non autorizzati da parte di terzi, si debba automaticamente affermare l'inadeguatezza delle misure tecniche e organizzative adottate dal titolare e, dunque, la sua responsabilità risarcitoria ai sensi dell'art. 82 GDPR, come se sussistesse quella che la stessa sentenza definisce una presunzione assoluta (41) e la dottrina potrebbe definire una responsabilità assoluta (42).

La Corte di Giustizia UE fornisce una risposta negativa, principalmente sulla base del seguente percorso argomentativo.

La Corte afferma, innanzitutto, il principio per il quale «*Il riferimento, contenuto nell'articolo 32, paragrafi 1 e 2, del RGPD, a "un livello di sicurezza adeguato al rischio" e a un "adeguato livello di sicurezza" dimostra che tale regolamento istituisce un regime di gestione dei rischi e che esso non pretende affatto di eliminare i rischi di violazione dei dati personali*» (43). Il titolare, ai sensi degli artt. 24 e 32 GDPR, deve limitarsi ad adottare «*misure tecniche e organizzative destinate ad evitare, per quanto possibile, qualsiasi violazione di dati personali*» (44).

In secondo luogo, afferma che ammettere una presunzione assoluta svuoterebbe di significato l'art. 24 GDPR, privando il titolare della possibilità di dimostrare la conformità al Regolamento delle misure adottate.

La Corte utilizza, inoltre, un argomento di carattere teleologico e contestuale sostenendo che il principio di *accountability* che impone al titolare di adottare ed essere in grado di dimostrare l'adeguatezza delle misure, «*non avrebbe senso se il titolare del trattamento fosse obbligato ad impedire qualsiasi danno di detti dati*» (45).

In ultimo si scorge un argomento che attiene alla volontà del legislatore: il considerando 83 GDPR prevede che il titolare e il responsabile, dopo aver valutato i rischi inerenti al trattamento, adottino misure al fine di limitarli. La Corte afferma che si può, dunque, ritenere che «*il legislatore dell'Unione* [abbia] *manifestato la sua intenzione di «limitare» i rischi di violazione dei dati personali, senza affermare che sarebbe possibile eliminarli*» (46).

## 7. La valutazione dell'adeguatezza delle misure tecniche e organizzative deve essere operata, in concreto, dai giudici nazionali

Con la seconda questione pregiudiziale il giudice *a quo* chiede, «*in caso di risposta negativa alla prima questione, quale debba essere l'oggetto e la portata del controllo giurisdizionale di legittimità nell'esame dell'adeguatezza delle misure tecniche e organizzative adottate dal titolare del trattamento ai sensi dell'articolo 32 del [RGPD]*» (47).

La Corte afferma che il margine di discrezionalità di cui gode il titolare per adottare le misure tecniche e organizzative non toglie che un giudice possa valutare, nel suo complesso, la ponderazione effettuata e l'idoneità delle stesse a garantire un livello di sicurezza adeguato al rischio.

Il controllo di legittimità viene effettuato in due tempi: in un primo momento, vengono individuati in concreto i rischi di violazione dei dati personali, considerando il grado di probabilità e gravità, nonché le eventuali conseguenze per i diritti e le libertà delle persone fisiche; successivamente, occorre verificare se le misure attuate siano adeguate a tali rischi.

Il giudice valuta l'adeguatezza tenuto conto sia dei criteri menzionati dall'art. 32 GDPR (lo stato dell'arte, i costi di attuazione e la natura, la portata, il contesto e le finalità del trattamento) che «*delle circostanze proprie del caso di specie e degli elementi di prova di cui tale giudice dispone al riguardo*» (48).

La Corte precisa, inoltre, che il giudice deve valutare la natura, il contenuto, il modo in cui le misure sono state applicate e gli effetti pratici delle stesse sul livello di sicurezza che il titolare era tenuto a garantire in base al rischio.

Anche in questo caso, oltre al dato letterale, la Corte tiene conto della congruità di siffatta interpretazione rispetto alle finalità del GDPR: solo l'attribuzione al giudice di questo sindacato consente di garantire l'effettività della protezione dei dati personali e il diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento.

## 8. Incombe sul titolare del trattamento l'onere di provare l'adeguatezza delle misure tecniche e organizzative

La sentenza affronta il tema della sussistenza del principio generale in forza del quale l'onere della prova, circa

(41) *Ibidem*, punto 32.

(42) Gallo, *Trattato di diritto civile*, VII, *L'arricchimento senza causa, la responsabilità civile*, Torino, 2018, 404.

(43) CGUE 14 dicembre 2023, C-340/2021, cit., punto 29.

(44) *Ibidem*, punto 30.

(45) *Ibidem*, punto 34. Lo stesso argomento era già stato formulato in termini pressoché identici in precedenza in dottrina: si veda Caterina - Thobani, *Il diritto*, cit., 2807.

(46) CGUE 14 dicembre 2023, C-340/2021, cit., punto 38.

(47) *Ibidem*, punto 21.

(48) *Ibidem*, punto 45.

l'adeguatezza delle misure tecniche e organizzative adottate ai sensi dell'art. 32 GDPR, incombe sul titolare del trattamento.
L'art. 32, par. 1, GDPR non afferma esplicitamente che il titolare debba essere in grado di dimostrare che il trattamento è effettuato conformemente al Regolamento e probabilmente proprio questa carenza è alla base della questione pregiudiziale sollevata dal giudice bulgaro.
Tale soluzione risulta, al più, suggerita dal paragrafo 3 dello stesso articolo, nella parte in cui prevede che l'adesione a codici di condotta o a meccanismi di certificazione approvati possa essere utilizzata per dimostrare la conformità delle misure adottate ai requisiti di cui al paragrafo 1. Non è chiaro, tuttavia, se la dimostrazione costituisca la prova liberatoria a fronte di una sorta di presunzione superabile di inadeguatezza, oppure se l'adesione a un codice di condotta approvato sia un elemento utile per resistere alla prova dell'inadeguatezza che incombe comunque, e nel silenzio, sul ricorrente, oltre che un'attenuante (49).
La Corte afferma che l'inversione dell'onere della prova in capo al titolare del trattamento trova il proprio fondamento nel principio di *accountability*, espresso in via generale all'art. 5, par. 2, GDPR e attuato dagli artt. 24 e 32; principio che impone al titolare «*di mettere in atto misure tecniche e organizzative adeguate per assicurarsi ed essere in grado di dimostrare che il trattamento è effettuato conformemente a detto regolamento*» (50).
Dal combinato disposto delle citate tre norme risulta «*una regola, di applicazione generale, che occorre, in mancanza di indicazione contraria nel RGPD, applicare anche nell'ambito di un'azione di risarcimento fondata sull'articolo 82 di tale regolamento*» (51).
La Corte evidenzia che, se gravasse sugli interessati l'onere della prova sull'adeguatezza delle misure, il diritto al risarcimento di cui all'art. 82, par. 1, GDPR «*sarebbe privato di gran parte del suo effetto utile*» (52) e che tale soluzione contrasterebbe con il considerando 11 del Regolamento, secondo cui un'efficace protezione dei dati personali presuppone un rafforzamento dei diritti degli interessati e degli obblighi degli autori del trattamento.

## 9. La non imputabilità dell'evento dannoso ai sensi dell'art. 82, paragrafo 3, GDPR

Con la quarta questione pregiudiziale il giudice *a quo* chiede se l'articolo 82, par. 3, GDPR debba essere interpretato nel senso che la divulgazione o l'accesso non autorizzati a dati personali riconducibile a un "attacco *hacker*", da parte di persone che non sono dipendenti del titolare e non sono soggette al suo controllo, configuri «*un evento che non è in alcun modo imputabile a quest'ultimo e che gli consente di essere esonerato dalla responsabilità*» (53).
La Corte afferma che qualora una violazione di dati personali sia stata commessa da criminali informatici, e quindi da «*terzi*», il danno non è imputabile al titolare del trattamento «*a meno che quest'ultimo non abbia reso possibile detta violazione violando un obbligo previsto dal RGPD*» (54), in particolare gli obblighi di protezione dei dati cui è tenuto in forza degli artt. 5, par. 1, lett. f, 24 e 32 GDPR.
Il titolare e il responsabile, dunque, rispondono delle violazioni operate da terzi qualora non riescano a dimostrare l'adeguatezza *ex* art. 32 GDPR delle misure di sicurezza in concreto adottate; in tal caso potranno ancora andare esenti da responsabilità, in forza dell'art. 82, par. 3, GDPR, dimostrando che non sussiste alcun nesso di causalità tra l'eventuale violazione dell'obbligo di protezione dei dati e il danno subito dalla persona fisica (55).
La sentenza è importante perché si inserisce nell'ampio dibattito dottrinario relativo alla portata dell'esimente di responsabilità previsto dall'art. 82, par. 3, GDPR, formulato in termini assolutamente generici e di cui risulta dubbio il contenuto (56).
La Corte chiarisce che la prova liberatoria dell'esimente prevista dal paragrafo 3 riguarda l'insussistenza del nesso causale, pur in presenza di un'accertata violazione dell'obbligo di protezione posto dal Regolamento a carico del titolare.
Trattasi, quindi, di una prova liberatoria diversa dall'«*onere di dimostrare l'adeguatezza delle misure di sicurezza da esso attuate ai sensi dell'articolo 32*» (57), che, secondo quanto affermato dalla Corte, incombe sul titolare del trattamento ai sensi dei primi due paragrafi dell'art. 82, come interpretati in forza del combinato disposto degli artt. 5, par. 2 e 24 GDPR, letti alla luce del considerando 74.

(49) Tosi, *Responsabilità*, cit., 93.

(50) CGUE 14 dicembre 2023, C-340/2021, cit., punto 51.

(51) *Ibidem*, punto 53.

(52) *Ibidem*, punto 56.

(53) *Ibidem*, punto 21.

(54) *Ibidem*, punto 71.

(55) *Ibidem*, punto 72.

(56) Salanitro, *Illecito*, cit., 426.

(57) CGUE 14 dicembre 2023, C-340/2021, cit., punto 57.

## 10. Il contributo della sentenza della Corte di Giustizia UE del 14 dicembre 2023, C-340/2021, alla definizione della responsabilità di cui all'art. 82 GDPR

La Corte, affermando che il titolare «*deve in linea di principio risarcire un danno causato da una violazione di tale regolamento*» e che può essere esonerato dalla responsabilità solo se fornisce la prova che il fatto non gli è in alcun modo imputabile (58), corrobora l'impostazione dottrinaria secondo cui gli elementi costituivi della fattispecie prevista dall'art. 82 GDPR sono: la violazione del Regolamento, il danno e il nesso causale tra la predetta violazione e il danno stesso (59).

La responsabilità civile del titolare del trattamento si fonda, dunque, sull'antigiuridicità della condotta e il GDPR fissa gli obblighi in capo al titolare che concorrono a tipizzare il fatto illecito (60), mentre l'art. 82, par. 3, GDPR prevede l'esimente, configurata in termini generici, che l'evento dannoso non risulti allo stesso «*in alcun modo imputabile*» (61).

La sentenza conferma anche le tesi dottrinarie secondo cui al titolare del trattamento viene richiesta la prova di aver adottato tutte le misure adeguate secondo la diligenza professionale (62) o astrattamente possibili allo stato dell'arte e per i costi di attuazione (63).

La sentenza risulta, invece, innovativa laddove pare fondare l'inversione dell'onere della prova, in merito all'adeguatezza delle misure di protezione, non tanto sul paragrafo 3, quanto sul combinato disposto dei paragrafi 1 e 2 dell'art. 82 e degli artt. 32, 24 e 5 GDPR.

Secondo il percorso argomentativo della Corte, l'inversione dell'onere della prova opererebbe già a livello della definizione dell'antigiuridicità della condotta e, dunque, dell'accertamento della violazione di una disposizione del Regolamento (ad esempio dell'art. 32 GDPR), senza bisogno di ricorrere al paragrafo 3 dell'art. 82 GDPR.

Il paragrafo 3, secondo la prospettazione della Corte, pare operare "a valle" dell'accertamento della violazione in quanto presuppone, da parte del titolare, la «*eventuale violazione dell'obbligo di protezione dei dati*» (64) (dunque, che il titolare non abbia fornito la prova dell'adeguatezza delle misure adottate): pur in presenza di tale violazione dell'obbligo di protezione, il titolare può andare comunque esente da responsabilità «*dimostrando che non sussiste alcun nesso di causalità tra la sua eventuale violazione dell'obbligo di protezione dei dati e il danno subito dalla persona fisica*» (65).

La pronuncia conforta, quindi, la tesi degli autori che riconducono la fattispecie dell'art. 82 GDPR a un'ipotesi di colpa presunta, secondo i quali non ci sono dubbi rispetto al fatto che la più rigorosa prova di eventi interruttivi del nesso causale (tradizionalmente ricondotti al caso fortuito o alla forza maggiore) escluderà la responsabilità e che, laddove vi sia stata una violazione dei dati personali, il titolare possa esonerarsi dalla responsabilità dimostrando di aver adempiuto ai propri obblighi (66).

In questo modo la sentenza in commento pare anche confortare la tesi dottrinaria secondo cui non è tanto l'art. 82 del Regolamento a esimere l'interessato dall'onere di prova della violazione della regola di condotta (violazione che anzi è espressamente contemplata dal paragrafo 1 quale elemento costitutivo della fattispecie), ma piuttosto altre norme del Regolamento: in particolare quelle che pongono il principio di *accountability*, in virtù del quale innanzi a un trattamento incombe su chi tratta i dati l'onere di dimostrare che esso è lecito (67); principio generale del Regolamento che in quanto tale deve essere considerato operante anche in sede risarcitoria (68).

Si è osservato in dottrina che le norme del Regolamento prevedono di regola obblighi di comportamento generici, rimessi alla valutazione in concreto del titolare del trattamento e che in questi casi l'imputazione si sovrappone all'antigiuridicità, in quanto se il titolare non avesse adottato la misura che si sarebbe rivelata necessaria *ex post*, perché ad esempio la lesione era imprevedibile, più che essere rilevante l'esimente, sarebbe già venuto meno il requisito della violazione della norma e che pertanto la sfera di rilevanza dell'esimente di cui al par. 3 dell'art. 82 GDPR si limita all'evento espressione di un rischio atipico (69).

## 11. Le ipotesi residue di responsabilità oggettiva e responsabilità indiretta

Pur nel contesto degli orientamenti predetti, secondo cui l'art. 82 GDPR configura un'ipotesi di responsabilità oggettiva o aggravata da colpa presunta, limitata dall'operatività del parametro della ragionevolezza delle misure nei termini dello stato dell'arte e dei costi di

(58) *Ibidem*, punto 71.

(59) Caterina - Thobani, *ibidem*.

(60) Gambini, *Principio*, cit., 53.

(61) Salanitro, *Illecito*, cit., 433.

(62) Caterina - Thobani, *Il diritto*, cit., 2808; Gambini, *Principio*, cit., 84.

(63) Tosi, *Responsabilità*, cit., 121; Camardi, *Note critiche*, cit., 797.

(64) CGUE 14 dicembre 2023, C-340/2021, cit., punto 72.

(65) *Ibidem*.

(66) Caterina - Thobani, *ibidem*.

(67) Caterina - Thobani, *Il diritto*, cit., 2807.

(68) Caterina - Thobani, *Il diritto*, cit., 2808.

(69) Salanitro, *Illecito*, cit., 447.

attuazione, quali parametro di diligenza o limiti alla responsabilità per rischio evitabile, si possono eccezionalmente scorgere ipotesi in cui il titolare è chiamato a rispondere oggettivamente, senza poter dimostrare, ai fini della prova liberatoria la mancanza di colpa o l'inevitabilità del rischio.
La prima ipotesi, definita anche responsabilità indiretta, è costituita dalla responsabilità solidale del titolare per il danno causato dal responsabile del trattamento: secondo la prevalente dottrina trattasi di responsabilità oggettiva dalla quale il titolare non può andare esente, neppure provando di aver diligentemente scelto un responsabile che presentava adeguate garanzie, operando la ripartizione di responsabilità nei rapporti interni (il titolare che abbia risarcito i danni potrà, al più, rivalersi sul responsabile nella misura in cui il danno sia allo stesso imputabile) (70).
Si osserva, a sostegno di tale tesi, che il considerando 74 GDPR afferma la responsabilità generale del titolare per qualsiasi trattamento che abbia «*effettuato direttamente o che altri abbiano effettuato per suo conto*» (71) e che pertanto il titolare del trattamento risponde della violazione del Regolamento nei confronti dei terzi, in solido con il responsabile del trattamento, anche se il danno derivi da obblighi specificamente rivolti al responsabile o per i quali questi abbia ricevuto legittime istruzioni (72).
Si richiama altresì l'art. 28, par. 10, GDPR che disciplina l'ipotesi in cui il responsabile del trattamento, fuoriuscendo dalle indicazioni del titolare, determini egli stesso «*le finalità e i mezzi del trattamento*»: la norma statuisce che il predetto responsabile del trattamento «*è considerato un titolare del trattamento in questione*», ma fa tuttavia salvo l'art. 82 GDPR, che prevede la responsabilità del titolare per i danni cagionati dal suo trattamento, cosicché l'originario titolare rimane responsabile in solido (73).
La dottrina che, in senso contrario, nega la natura oggettiva di tale responsabilità solidale afferma che la decisione di ricorrere alla nomina di uno o più responsabili è rimessa alla discrezionalità del titolare e rientra tra le misure organizzative che questi è tenuto a mettere in atto, in quantità e qualità adeguata, per cui sussiste in capo al titolare una responsabilità per *culpa in eligendo* e *in vigilando*, per violazione del dovere di diligenza nella designazione del responsabile e nella vigilanza sul suo operato (74).

Il responsabile del trattamento per andare esente da responsabilità deve, come detto, dimostrare di avere adempiuto agli obblighi previsti dal GDPR specificatamente diretti ai responsabili del trattamento e di aver agito in modo conforme alle legittime istruzioni del titolare. Pare potersi ritenere che, alla luce dalla sentenza della Corte giustizia UE del 14 dicembre 2023, C-340/2021, qualora il responsabile non riesca a fornire la predetta prova, lo stesso possa ancora invocare l'art. 82, par. 3, GDPR, «*dimostrando che non sussiste alcun nesso di causalità tra la sua eventuale violazione dell'obbligo di protezione dei dati e il danno subito dalla persona fisica*» (75).
Se il responsabile non riuscirà a fornire tali prove sarà quindi tenuto a risarcire il danno *ex* art. 82 GDPR e risponderà solidalmente con il medesimo anche il titolare del trattamento, a meno che a sua volta non riesca a dimostrare la sussistenza dell'esimente di cui al paragrafo 3, che potrebbe in teoria (anche se non risulta semplice ipotizzare casi concreti) sussistere con riferimento al solo titolare.
È altresì pacifico, per le stesse ragioni evocate in relazione alla figura del responsabile del trattamento, che il titolare risponde anche dei danni provocati da ausiliari diversi dal responsabile, per i quali il Regolamento neppure prevede una esplicita responsabilità (76) e per le quali a livello di ordinamento interno opera l'art. 2049 c.c. (77).
Anche in questo caso, per andare esente da responsabilità, il titolare del trattamento dovrà dimostrare che il proprio ausiliario non ha violato il Regolamento e, qualora non possa dare tale prova, potrà soltanto avvalersi dell'esimente di cui al par. 3 dell'art. 82 GDPR e quindi dare la prova, per usare le parole della sentenza, «*che non sussiste alcun nesso di causalità tra la sua eventuale violazione dell'obbligo di protezione dei dati e il danno*» (78).

## 12. Non è necessaria una perizia per valutare l'adeguatezza delle misure di sicurezza

La Corte risponde negativamente alla richiesta se, per valutare l'adeguatezza delle misure tecniche e organizzative adottate dal titolare del trattamento, sia necessario e sufficiente ricorrere a una perizia.
Secondo la Corte il principio di effettività della tutela giurisdizionale potrebbe risultare violato attraverso il ricorso «*necessario*» a una perizia, quando alla luce delle prove detenute dal giudice adito questa si riveli superflua. Tale principio risulterebbe violato anche se si

(70) Caterina - Thobani, *Il diritto*, cit., 2806; Salanitro, *Illecito*, cit., 449.

(71) Caterina - Thobani, *ibidem*.

(72) Salanitro, *ibidem*.

(73) Caterina - Thobani, *ibidem*.

(74) Gambini, *Principio*, cit., 33.

(75) CGUE 14 dicembre 2023, C-340/2021, cit., punto 72.

(76) Salanitro, *ibidem*.

(77) Caterina - Thobani, *ibidem*.

(78) CGUE 14 dicembre 2023, C-340/2021, cit., punto 72.

considerasse il termine «*sufficiente*» nel senso che l'adeguatezza della misura deve essere dedotta «*esclusivamente o automaticamente da una perizia giudiziaria*» (79), perché ciò impedirebbe l'esercizio del diritto a un ricorso giurisdizionale effettivo (garantito all'art. 79, par. 1, GDPR), il quale comporta che un giudice imparziale effettui una valutazione obbiettiva dell'adeguatezza delle misure e non si limiti a tale deduzione.

## 13. Il danno immateriale risarcibile a seguito della violazione del Regolamento

La disciplina contenuta nell'art. 82 GDPR risulta più chiara rispetto a quella contenuta nell'art. 15 Codice della *Privacy*, che prevedeva al primo comma che «*chiunque*» cagiona danno ad altri per effetto del trattamento di dati personali era tenuto al risarcimento ai sensi dell'articolo 2050 c.c. e solo al secondo comma il riferimento al «*danno non patrimoniale*», indicato come risarcibile «*anche in caso di violazione dell'articolo 11*».

La vecchia disposizione lasciava un margine di dubbio interpretativo circa il fatto che il danno morale fosse risarcibile solo nel caso della violazione dell'art. 11 Codice della *Privacy* (previsto dal secondo comma): prevaleva comunque l'orientamento secondo cui, facendo il primo comma riferimento al risarcimento del danno in generale, senza ulteriori distinzioni, la risarcibilità del danno non patrimoniale dovesse essere ammissibile anche con riferimento a ogni ipotesi di danno causato «*per effetto del trattamento*» (80).

La previsione esplicita della risarcibilità del danno non patrimoniale nel previgente art. 15 Codice della *Privacy*, nonostante tale precisazione non fosse contenuta nella Direttiva 95/46/Ce, risultava particolarmente importante alla luce della tradizione giuridica di diritto interno, che distingue e tratta diversamente la risarcibilità del danno patrimoniale e non patrimoniale (81).

Si è osservato in dottrina che, sebbene spesso la locuzione usata dall'art. 82 del Regolamento, «*danno materiale o immateriale*», venga ritenuta corrispondente a quella di danno patrimoniale e non patrimoniale (82), sia preferibile attenersi alla nozione europea di danno, senza rimanere eccessivamente legati alla tradizione del diritto interno, anche alla luce del considerando 146 GDPR in base al quale «*il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento*» (83).

Tale tesi è stata confermata dalla sentenza della Corte di Giustizia UE 4 maggio 2023, C-300/2021, la quale ha affermato che *la nozione di* «*danno*» e di «*danno immateriale*», ai sensi dell'art. 82 GDPR, devono essere intesi secondo una definizione autonoma e uniforme, propria del diritto dell'Unione (84).

La sentenza riafferma la sussistenza, sul punto, della primazia del diritto comunitario (85) e la necessità che anche l'interpretazione delle norme comunitarie avvenga tramite una metodologia ricostruttiva che ricerchi le soluzioni ai problemi nell'ottica di una dogmatica europea, quale emergente dalla normativa dell'Unione e dalla giurisprudenza della Corte di Giustizia UE, poiché il ricorso ai moduli interpretativi propri dei singoli ordinamenti nazionali potrebbe avere un effetto fuorviante (86).

Come è noto la giurisprudenza interna a partire dalle c.d. "sentenze gemelle" della Cassazione del 31 maggio 2003, n. 8827 e n. 8828 (87), ha qualificato il danno non patrimoniale come danno-conseguenza, che deve essere debitamente allegato e provato, ancorché ricorrendo a presunzioni o valutazioni prognostiche (88).

Si afferma in dottrina che anche l'impianto previsto dall'art. 82 GDPR appare in linea con questa impostazione, secondo cui a dar luogo a un risarcimento non

(79) *Ibidem*, punto 63.

(80) Di Ciommo, *La risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali*, in *Danno e resp.*, 2005, 802; Gambini, *Principio*, cit., 101; Caringella, *La tutela aquiliana della privacy nel codice per la protezione dei dati personali (d.lgs. n. 196/2003)*, in Caringella, *Studi di Diritto civile*. III. *Obbligazioni e responsabilità*, Milano, 2007, 724.

(81) Tosi, *Responsabilità*, cit., 220; Gambini, *Principio*, cit., 97 che cita a sua volta Franzoni, *Responsabilità derivante da trattamento dei dati personali*, in Finocchiaro - Delfini (a cura di), *Diritto dell'informatica*, Milano, 2014, 830. Cfr. le osservazioni di Perlingieri, *La responsabilità civile tra indennizzo e risarcimento*, in *Rass. dir. civ.*, 2004, 1061 ss.

(82) Gambini, *Principio*, cit., 98.

(83) Caterina - Thobani, *Il diritto*, cit., 2809.

(84) CGUE 4 maggio 2023, C-300/2021, in *Dir. giust.*, 2023, 5, con nota di Milizia, *Linee guida dalla CGUE sul risarcimento del danno per violazione del GDPR*; in *Foro it.*, 2023, IV, 268 ss., con nota di Palmieri - Pardolesi, *Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)*, 278; *ibidem*, Pagliantini, *Un altro palcoscenico della «guerra» tra le corti: il danno (immateriale) bagatellare dell'art. 82 Gdpr*, 285; in *Nuova giur. civ. comm.*, 2023, 1112 ss., con nota di Calabrese, *Il danno*, cit. Conforme CGUE 14 dicembre 2023, C-456/2022, in *One legale*.

(85) Camardi, *Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea*, in *Nuova giur. civ. comm.*, 2023, 1137.

(86) Scognamiglio, *Danno e risarcimento nel sistema del Rgpd: un primo nucleo di disciplina eurounitaria della responsabilità civile?*, in *Nuova giur. civ. comm.*, 2023, 1152.

(87) Cass. 31 maggio 2003, n. 8827 e 8828, in *Danno e resp.*, 2003, 816 ss., con nota di Busnelli, *Chiaroscuri d'estate. La Corte di Cassazione e il danno alla persona*.

(88) Gambini, *Principio*, cit., 105. Per la tesi minoritaria cfr. Alpa, *Danno in re ipsa e tutela dei diritti fondamentali (Diritti della personalità e diritto di proprietà)*, in *Resp. civ.*, 2023, 6 ss.; Tosi, *Responsabilità*, cit., 231, Id., *Tutela della persona nella società digitale e responsabilità oggettiva per illecito trattamento dei dati personali*, in D'Auria (a cura di), *I problemi dell'informazione nel diritto civile, oggi*, Roma, 2022, 404.

è il trattamento illecito in sé, ma le conseguenze pregiudizievoli che ne derivano (89): tale interpretazione si ricava dalla lettura dei considerando 75, che reca un elenco di casi in cui «*i rischi per i diritti e le libertà delle persone fisiche* [...] *possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale*» e 85, che contiene un elenco di «*danni fisici, materiali o immateriali*» che possono essere causati alle persone fisiche da una violazione dei dati personali.
Si supera in questo modo anche la discussione sulla sufficienza della mera antigiuridicità della condotta ai fini risarcitori, atteso che comunque, perché sussista un danno risarcibile, oltre alla violazione di una regola di condotta, occorre la lesione di un interesse o una situazione giuridica in capo al danneggiato (90).
La Corte, nella sentenza 4 maggio 2023, C-300/2021, ha confermato questa tesi, affermando che, in base all'art. 82 GDPR, condizioni cumulative del diritto al risarcimento sono l'esistenza di un danno «*subito*», l'esistenza di una violazione del GDPR e di un nesso di causalità tra il danno e la violazione (91). L'art. 82, par. 1, GDPR deve essere interpretato nel senso che la mera violazione delle disposizioni di tale regolamento non è sufficiente per conferire un diritto al risarcimento (92).
L'elemento di frizione tra la giurisprudenza interna e quella comunitaria si poteva invece concretizzare nell'orientamento, assunto dalla giurisprudenza interna a seguito del principio affermato dalle sentenze gemelle delle Sezioni Unite del 2008, secondo cui la gravità dell'offesa costituisce requisito per l'ammissione a risarcimento dei danni non patrimoniali alla persona conseguenti alla lesione di diritti costituzionalmente inviolabili. Il filtro della gravità della lesione e della serietà del danno attua il bilanciamento tra il principio di solidarietà verso la vittima e quello di tolleranza, con la conseguenza che il risarcimento del danno non patrimoniale è dovuto solo nel caso in cui «*sia superato il livello di tollerabilità e il pregiudizio non sia futile*» (93).
Si è osservato che, applicando questo principio, la risarcibilità del pregiudizio subito, pur se conseguente alla lesione di un diritto tutelato dagli artt. 2 e 21 Cost. e dall'art. 8 Conv. eur. dir. umani, qual è il diritto alla protezione dei dati personali, viene subordinato alla preventiva verifica della "gravità della lesione" e della "serietà del danno" (94).
La dottrina si è quindi opportunamente interrogata sul fatto che sia legittima questa restrizione introdotta dalla giurisprudenza di diritto interno, che pare richiedere il superamento di una certa soglia di gravità dell'offesa (95): si è affermato che tale limitazione può essere accettabile in quanto corrisponde a una ragionevole esigenza di identificabilità di un danno che, essendo per la sua stessa natura soggettivo, necessita comunque di un vaglio sulla base di valutazioni social-tipiche, ma che comunque non può estendersi fino a considerare di per sé non risarcibili i meri disagi e fastidi (96).
A supporto di tale tesi gli autori hanno evidenziato che il considerando 146 GDPR che parla di «*pieno ed effettivo risarcimento per il danno subito*» e richiamato le indicazioni del Gruppo di lavoro Articolo 29 nell'ambito dei lavori preparatori del GDPR, nei quali si afferma che il danno deve includere anche situazioni di "*distress*" (97) e si cita ad esempio il caso in cui l'interessato soffra di un «*sense no longer to be able to move through the public and private sector without being watched*» (98).
Hanno altresì evidenziato (99) che la giurisprudenza comunitaria ha adottato una nozione di danno morale che comprende disagi, fastidi, disturbi, ad esempio allorché si è occupata del danno da vacanza rovinata, affermando che il turista va risarcito per il mancato godimento della vacanza, in ragione delle "sensazioni spiacevoli" e delle "impressioni negative" suscitate dall'inadempimento del professionista (100) e che tutto sommato anche la giurisprudenza interna, allorché afferma che non sono risarcibili i "meri disagi e fastidi", si riferisce a casi in cui in realtà esclude l'ingiustizia del danno, ritenendo sussistente una mera «*lesione di diritti del tutto immaginari,*

(89) Caterina - Thobani, *ibidem.*

(90) Thobani, *Il danno non patrimoniale da trattamento illecito dei dati personali*, in *Dir. inf. e inform.*, 2017, 430.

(91) CGUE 4 maggio 2023, C-300/2021, cit., punto 32.

(92) *Ibidem*, punto 42.

(93) Cass. 11 novembre 2008, n. 26972, n. 26973, n. 26974 e n. 26975, in *Danno e resp.*, 2009, 19 ss., con nota di Procida Mirabelli di Lauro, *Il danno non patrimoniale secondo le Sezioni Unite. Un "de profundis" per il danno esistenziale*.

(94) Gambini, *Principio*, cit., 108 s. Per la giurisprudenza di legittimità: Cass. 7 ottobre 2022, n. 29323, in *Dir. giust.*, 2022; Cass. 10 giugno 2021, n. 16402, in *Foro it.*, 2021, I, 3589; Cass. 17 settembre 2020, n. 19328, cit. Per la giurisprudenza di merito: Trib. Napoli 21 febbraio 2023, n. 1169, in *One legale*; Trib. Milano, 13 settembre 2022, n. 2016, in *One legale*.

(95) Nel senso della inammissibilità di tale soglia nell'ambito della violazione dei dati personale si veda Tosi, *Responsabilità*, cit., 239, Id., *Tutela*, cit., 402.

(96) Caterina - Thobani, *Il diritto*, cit., 2810.

(97) Article 29, Data Protection Working Party, *Opinion 01/2012 on the data protection reform proposals*, 23 March 2012.

(98) Article 29, Data Protection Working Party, *The future of privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, 1 December 2009, nota 21.

(99) Caterina - Thobani, *Il diritto*, cit., 2809.

(100) CGCE 12 marzo 2002, C-168/2000 in *Nuova giur. civ. comm.*, 2003, I, 861, con nota di Farkas, *Il danno da vacanza rovinata: nuove tendenze e vecchie questioni*.

*come quello alla qualità della vita o alla felicità»*, che non integrano interessi costituzionalmente protetti (101).
Anche la recente ordinanza della Corte di Cassazione 12 maggio 2023, n. 13073, ha del resto affermato il principio secondo cui, alla luce dell'art. 82 GDPR, ancorché non sia accoglibile la tesi del danno "*in re ipsa*" per la violazione della regola di condotta, comunque il danneggiato «*può ottenere il risarcimento di qualunque danno occorsogli, anche se la lesione sia marginale*» (102).
Si è osservato che alla luce del considerando 75 GDPR, che contiene un elenco non tassativo di ipotesi in cui i diritti e le libertà dei soggetti interessati possono essere messi a rischio, il principio enunciato dalla citata ordinanza della Cassazione consente di utilizzare quale parametro per affermare la risarcibilità del danno, una valutazione casistica che tenga conto dell'incidenza della condotta del titolare o del responsabile del trattamento, rispetto ai diritti e alle libertà del soggetto interessato e dunque non solo della concreta lesione, ma anche dell'esposizione al rischio della posizione del danneggiato (103).
Si è osservato che, una volta che il legislatore ha presidiato una norma di condotta a tutela di un determinato interesse con la sanzione del risarcimento del danno non patrimoniale, tale interesse non potrebbe ritenersi di per sé futile e non vi sarebbe spazio per una valutazione giudiziale di non serietà del pregiudizio che ne deriva, mentre potrà effettuarsi una valutazione in merito alla serietà del danno (104).
La Corte di Giustizia UE, con la sentenza 4 maggio 2023, C-300/2021, corrobora tale interpretazione in quanto da un lato afferma che l'art. 82, par. 1, GDPR osta a una norma o a una prassi nazionale che subordini il risarcimento di un danno immateriale alla condizione che il danno subito dall'interessato abbia raggiunto un certo grado di gravità (105), ma dall'altro conferma che permane in capo al ricorrente, che ha subito la violazione dei dati personali, l'onere di dimostrare che le conseguenze della violazione costituiscano un danno immateriale ai sensi di tale norma (106).
Si afferma che la sentenza, riconoscendo i patimenti interiori causati dalla perdita di controllo dei dati, anche laddove costituiscano un mero fastidio interiore, senza alcuna conseguenza esteriore, implicherebbe la risarcibilità anche di quei danni "bagatellari" esclusi dalla nostra giurisprudenza, perché non assurgono a pregiudizio "grave" per l'individuo (107): come sopra detto, in realtà, anche l'ordinamento interno, ormai, considera risarcibile il danno di modesta entità, purché configurabile non "*in re ipsa*" (108) ma quale "danno conseguenza" della lesione del diritto (109). Pare dunque preferibile l'affermazione secondo cui vi sarebbe sostanziale identità tra l'orientamento della Corte di Giustizia UE e gli ultimi approdi della citata giurisprudenza interna (110).
Nello stesso senso si è affermato che, anche alla luce della sentenza citata, il danno immateriale risarcibile si configura comunque come un pregiudizio che, ancorché non tale da raggiungere un livello predeterminato di gravità, deve comunque poter essere oggettivamente apprezzato anche sulla base di una valutazione social-tipica delle conseguenze, in termini di disagio (111), come era stato sostenuto da parte della dottrina anche prima della pronuncia della Corte di Giustizia UE (112).
Dato per acquisito il principio secondo cui una soglia di gravità contrasterebbe con la *ratio* del GDPR e delle sue tutele (113), la sentenza della Corte di Giustizia UE 14 dicembre 2023, C-340/2021, affronta quindi il problema della rilevanza delle inquietudini, delle ansie

(101) Cass. Sez. Un. 25 febbraio 2016, n. 3727, in *Nuova giur. civ. comm.*, 2016, 1012 ss., con nota di Delli Priscoli, *La non risarcibilità del danno non patrimoniale di lieve entità, anche se derivante da reato*; Cass. 10 ottobre 2014, n. 21415, in *DeJure*; Cass. 12 settembre 2014, n. 19327, *DeJure*; Cass. 28 febbraio 2013, n. 5096, *DeJure*.

(102) Cass. 12 maggio 2023, n. 13073, in *Nuova giur. civ. comm.*, 2023, 1125 ss., con nota di Riccio, *Dati personali e rimedi: diritti degli interessati e profili risarcitori*. Nel caso di specie un comune aveva pubblicato per errore i dati personali di una dipendente sull'albo pretorio e il giudice di merito aveva accertato che «*un danno era stato integrato dall'ostensione del dato per tipologia e contesto, sebbene solo per un tempo ridotto*».

(103) Riccio, *Dati*, cit., 1129.

(104)Thobani, *Il danno*, cit., 442.

(105) CGUE 4 maggio 2023, C-300/2021, cit., punto 51, la sentenza si riferisce al risarcimento richiesto a una società di diritto austriaco che commercializzava dati personali (indirizzi) e un singolo utente, i cui dati erano stati raccolti dalla società e abbinati, nei database di quest'ultima, ad un partito politico nel quale l'utente non riconosceva di appartenere e che affermava che tale accostamento gli avrebbe arrecato «*una grave contrarietà, una perdita di fiducia, nonché un sentimento di umiliazione*», sebbene non fosse stato accertato, in sede di merito «*alcun danno diverso da tali afflizioni di carattere temporaneo e di ordine emotivo*». Conforme CGUE 14 dicembre 2023, C-456/2022, cit.

(106) CGUE 4 maggio 2023, C-300/2021, cit., punto 50.

(107) Calabrese, *Il danno*, cit., 1117.

(108) Pare configurare la risarcibilità del danno *in re ipsa* Cass. 4 giugno 2018, n. 14242, in *Giur. it.*, 2019, 41, con nota di Thobani, *Protezione dei dati personali - Il danno non patrimoniale da trattamento di dati tra danno presunto e danno evento*. Cfr. altresì nota critica di Esposito, *Il risarcimento del danno non patrimoniale da illecito trattamento dei dati personali*, in *Corr. giuridico*, 2019, 625.

(109) Caterina - Thobani, *ibidem*; Riccio, *Dati*, cit., 1129. Cass. 12 maggio 2023, n. 13073, cit., 1125 ss.; Cass. Sez. Unite 25 febbraio 2016, n. 3727, cit., 1012 ss.; Cass. 10 ottobre 2014, n. 21415, cit.; Cass. 12 settembre 2014, n. 19327, cit.; Cass. 28 febbraio 2013, n. 5096, cit.

(110) Riccio, *Dati*, cit., 1131.

(111) Scognamiglio, *Danno*, cit., 1157.

(112) Caterina - Thobani, *Il diritto*, cit., 2810.

(113) Milizia, *Linee guida*, cit., 5.

e dei timori di un eventuale futuro uso improprio dei dati personali, anche se tale uso improprio non sia stato accertato *«e/o la persona interessata non abbia subito alcun ulteriore danno»*.
In dottrina (114) si era già osservato che la giurisprudenza interna ammette il risarcimento anche allorché i disagi e disturbi all'interessato non si siano ancora verificati, ma vi sia il ragionevole timore che si possano verificare in futuro, come nel caso della pubblicazione dell'indirizzo di abitazione, laddove si tema che l'interessato possa essere importunato (115), anche se tali pronunce non chiariscono se il risarcimento sia ammesso in ragione della probabilità del verificarsi in futuro di conseguenze pregiudizievoli, o dello stato ansioso provocato all'interessato (116).
La sentenza annotata conferma tale impostazione interpretativa, osservando che l'art. 82 GDPR, una volta che sia stata accertata la violazione del Regolamento, non opera una distinzione tra il caso in cui il danno immateriale lamentato dall'interessato sia collegato ad un utilizzo abusivo dei dati personali che si sia già prodotto, oppure sia collegato alla paura percepita da tale persona che un siffatto utilizzo possa prodursi in futuro.
Il considerando 85 contiene inoltre un elenco esemplificativo dei danni che possono essere subiti dagli interessati a causa di una violazione del Regolamento e, tra le altre ipotesi, contempla «*la perdita di controllo dei dati personali*», che quindi può di per sé costituire un danno, «*quand'anche un utilizzo abusivo dei dati di cui trattasi non si sia verificato concretamente a danno di dette persone*» (117).
La Corte afferma che se la nozione di danno immateriale fosse interpretata nel senso di non considerare tali situazioni, non potrebbe dirsi raggiunto l'elevato livello di protezione delle persone con riguardo al trattamento dei dati personali, richiesto dal considerando 146.
Osserva, inoltre, che il citato considerando 146 affida alla Corte di Giustizia UE l'interpretazione della nozione di «*danno*» e che il testo del GDPR non attribuisce agli Stati membri alcun potere di incidere sul significato e sulla portata dei termini di «*danno materiale o immateriale*», cosicché tali clausole devono essere considerate, ai fini dell'applicazione del Regolamento, come costitutive di nozioni autonome del diritto dell'Unione, che devono essere interpretate in modo uniforme in tutti gli Stati membri (118).
La Corte osserva, dunque, che il timore di un potenziale utilizzo abusivo dei dati personali da parte di terzi può, di per sé, costituire un «*danno immateriale*» ai sensi dell'art. 82 GDPR e pertanto il giudice nazionale adito è tenuto a «*verificare che tale timore possa essere considerato fondato, nelle circostanze specifiche di cui trattasi e nei confronti dell'interessato*» (119).
Si osserva in dottrina che questi danni devono essere valutati secondo criteri di normalità sociale, trattando diversamente i casi di lesione dei diritti della personalità tradizionalmente intesi, ove il danno può essere tendenzialmente presunto, da quelli in cui tali diritti non sono coinvolti (120).
Si rileva, infine, che se tale parametro venisse inteso come criterio descrittivo, il danneggiato potrebbe chiedere, fornendone la prova, il risarcimento dei danni riconducibili alle idiosincrasie che lo inducono a provare patimenti maggiori rispetto alla media dei consociati; al contrario se tale criterio venisse inteso in maniera prescrittiva, il danneggiato non potrebbe chiedere il risarcimento del danno riconducibile alle proprie idiosincrasie, il cui costo non dovrebbe essere sopportato dai terzi ma rimanere a carico del portatore delle stesse (121).

(114) Caterina - Thobani, *Il diritto*, cit., 2809.

(115) Cass. 13 febbraio 2018, n. 3426, in *Nuova giur. civ. comm.*, 2018, 1270, in relazione al caso di diffusione senza consenso nel corso di una trasmissione televisiva del nominativo dell'attore in associazione alla localizzazione del proprio studio professionale; Cass. 14 agosto 2014, n. 17974, in *DeJure*, in relazione a un caso di pubblicazione nell'elenco cartaceo e on line di "Pagine Bianche" del nominativo, comprensivo di numero telefonico e indirizzo di residenza, dell'interessata che secondo quanto accertato dal giudice di merito era «*caduta in uno stato ansioso depressivo per il timore di essere ritrovata dalla persona che l'aveva in precedenza aggredita*».

(116) Caterina - Thobani, *Il diritto*, cit., 2810.

(117) CGUE 14 dicembre 2023, C-340/2021, cit., punto 82.

(118) Milizia, *ibidem*.

(119) CGUE 14 dicembre 2023, C-340/2021, cit., punto. 85.

(120) Thobani, *Il danno*, cit., 445.

(121) Thobani, *ibidem*.

# Sanità digitale ed intelligenza artificiale: profili penali

**di Lorenzo Picotti**



La digitalizzazione della sanità e l'impiego di sistemi AI in tale campo tocca molteplici ambiti di possibile rilevanza penale, fermo restando che l'applicazione delle relative sanzioni deve sempre rispettare i principi di garanzia della legalità e della colpevolezza. Innanzitutto, viene in rilievo il tema del consenso informato, che deve estendersi a ricomprendere il ricorso a sistemi AI, ma la cui eventuale invalidità, secondo l'attuale giurisprudenza in materia, non potrebbe di per sé essere fonte di responsabilità penale. In secondo luogo, la digitalizzazione del fascicolo sanitario elettronico e della cartella clinica elettronica pone rilevanti questioni relative al trattamento dei dati personali "particolari", quali sono quelli sanitari, rispetto a cui la vigente disciplina del GDPR e del Codice privacy deve confrontarsi con le innovazioni che emergono dall'AI Act dell'Unione europea e dalla prossima prospettiva dello "spazio europeo dei dati sanitari", oltre che dal recente schema di disegno di legge governativo in materia. Le violazioni di queste norme possono costituire reato, per cui occorre tratteggiarne il quadro, al pari di quelle in materia di cybersecurity e di valore probatorio degli atti e documenti digitali. Il tema più delicato è, infine, quello dell'eventuale responsabilità medica per colpa, nel caso di eventi avversi, quali la morte o le lesioni personali dei pazienti, nella cui causazione sia ravvisabile l'intervento, in fase diagnostica, chirurgica o terapeutica, di un sistema AI. L'esigenza di tutelare anche penalmente i beni giuridici e i diritti fondamentali che sono in gioco, richiede un'analisi critica delle categorie penalistiche della causalità e della colpa che vengono in rilievo, per adeguarne l'interpretazione e la possibilità di applicazione di fronte ai nuovi fenomeni, anche mediante eventuali interventi normativi, soprattutto considerando il modello di disciplina della responsabilità da reato degli enti.

*The digitisation of healthcare and the use of AI systems in this field touches on many areas of possible criminal relevance, it being understood that the application of the related sanctions must always respect the principles of guaranteeing legality and culpability. First of all, the issue of informed consent comes to the fore, which must be extended to include the use of AI systems, but whose possible invalidity, according to the current case law on the subject, could not in itself be a source of criminal liability. Secondly, the digitisation of the electronic health file and the electronic medical record raises important issues concerning the processing of 'special' personal data, such as health data, with respect to which the current regulations of the GDPR and the Privacy Code must be compared with the innovations emerging from the European Union's AI Act and the forthcoming 'European health data space', as well as the recent draft government bill on AI. Violations of these rules may constitute a crime, so the framework must be outlined, as well as those on cybersecurity and the evidentiary value of digital acts and documents. Finally, the most delicate issue is that of possible medical liability for negligence in the case of adverse events, such as death or personal injury of patients, in the causation of which the intervention of an AI system in the diagnostic, surgical or therapeutic phase can be recognised. The need to protect the legal assets and fundamental rights that are also at stake under criminal law requires a critical analysis of the criminal law categories of causality and fault that come to the fore, in order to adapt their interpretation and the possibility of their application in the face of new phenomena, including through possible regulatory interventions, especially considering the model of the regulation of the criminal liability of entities.*

## 1. Ambiti di rilevanza penale della digitalizzazione della sanità e dell'impiego di sistemi AI di fronte ai principi di garanzia della legalità e della personalità della responsabilità penale

Siamo tutti consapevoli che l'introduzione sempre più estesa di sistemi di intelligenza artificiale (d'ora in poi: AI [*Artificial Intelligence*]), comporta enormi vantaggi, ma anche nuovi tipi di rischi, tanto più insidiosi, in quanto difficili da riconoscere e, di conseguenza, da contrastare tempestivamente.

Non potendosi lasciare al mercato la risposta ad essi, la necessità di un intervento giuridico regolatore è già emersa in molti campi, che vanno da quello delle auto a guida autonoma e dei trasporti, a quello dei mercati finanziari, da quello dell'amministrazione pubblica e

dell'accesso a servizi e prestazioni, fino a quello delle c.d. armi intelligenti, nei quali, per presidiare l'efficacia delle regole introdotte o in corso di introduzione, viene via via riconosciuta la necessità di presidi sanzionatori, anche di natura penale, nel rispetto dei fondamentali principi di legalità e di personalità della responsabilità penale, oltre che di *ultima ratio* e proporzione (1).

Nel regolamento europeo sull'AI (d'ora in poi: *AI-Act*), prossimo alla sua entrata in vigore, si ravvisa nel settore sanitario uno di quelli "*ad alto rischio*" (2), fermo restando che l'AI garantisce un miglioramento delle previsioni, un'ottimizzazione delle operazioni e dell'assegnazione delle risorse, la personalizzazione dei servizi, ed in particolare, sul piano terapeutico, la sicurezza e tempestività delle diagnosi, da un lato, e l'efficacia e precisione delle cure, dall'altro (si pensi alla chirurgia robotica di precisione, poco invasiva, ad esempio per interventi urologici, per calcoli renali o biliari, per interventi oftalmici, ecc.) (3).

Ma proprio tale impetuoso sviluppo tecnologico fa emergere, da un lato, rischi empirici e limiti tecnici, manifestatisi anche in molteplici eventi avversi; dall'altro preoccupazioni etiche e giuridiche, a partire dai rapporti con i pazienti, che pongono con forza la necessità di una tutela efficace di fronte a danni ed offese a beni giuridici e diritti fondamentali esposti a tali rischi, che vanno dalla vita ed integrità fisica e psichica, alla libertà di autodeterminazione rispetto al trattamento sanitario, dalla *privacy* e tutela dei dati personali, al buon andamento della pubblica amministrazione, fino alla fede pubblica.

Il diritto penale e la responsabilità penale sono però l'*ultima ratio* degli strumenti di tutela, potendo intervenire solo quando altre tecniche alternative siano per la loro natura inadeguate o, comunque, insufficienti a garantire il necessario livello di protezione. Inoltre, la configurazione di una responsabilità penale richiede il rispetto dei superiori principi garantistici imposti dalla Costituzione e dalle Carte internazionali, quali quelli di legalità e di tassatività (artt. 25, comma 2, Cost., 7 CEDU, 49 CDFUE), nonché di personalità e di colpevolezza (art. 27, commi 1 e 3 Cost., e giurisprudenza della Corte di Strasburgo sull'art. 7 CEDU, relativa all'esigenza di "prevedibilità" della sanzione penale per l'autore del comportamento punibile).

Il principio euristico che deve orientare le scelte di criminalizzazione in questi nuovi ambiti si dovrebbe basare, in prima approssimazione, su un criterio di analogia (non certo invocabile nell'esercizio del magistero punitivo, vincolato al principio di stretta legalità), in forza del quale quanto sarebbe penalmente rilevante, se il fatto fosse commesso da una persona umana, non può essere penalmente irrilevante sol perché vi è l'intervento di un sistema AI. Tanto più che, di fronte ai nuovi sviluppi tecnologici ed all'estensione tumultuosa delle relative applicazioni, si estenderebbero inaccettabili aree di impunità (4).

Si tratta, quindi, di verificare, se ed in che misura possano o debbano configurarsi forme di responsabilità penale nel settore sanitario, di fronte all'ormai estesa digitalizzazione ed all'impiego di sistemi AI, guardando ad alcuni essenziali nuclei problematici in cui potrebbero emergere: da quello del consenso informato (par. 2),

(1) Nella sterminata letteratura, non solo internazionale, in argomento, basti per ora il rinvio ai lavori promossi dall'*Association Internationale de Droit Pénal* in vista del Congresso internazionale di Parigi del 25-28 giugno 2024 avente per tema "*Artificial Intelligence and Criminal Justice*". Nei lavori sviluppati nelle quattro sezioni in cui si articola, dedicate al diritto penale generale, al diritto penale speciale, al processo penale ed al diritto internazionale, sono stati raccolti i rapporti nazionali, elaborati sulla loro base i rispettivi rapporti generali e quindi discusse ed approvate, in specifici Colloqui internazionali, le relative risoluzioni, contenenti raccomandazioni indirizzate a legislatori, magistrati, politici, operatori, cittadini oltre che studiosi del diritto penale, reperibili al sito <www.penal.org>.

(2) Si veda l'Allegato III, paragrafo 5, lettera a), dell'elenco dei sistemi classificati "*ad alto rischio*", ai sensi dell'art. 6, par. 2 del regolamento UE che "*stabilisce regole armonizzate sull'intelligenza artificiale*" – c.d. *AI Act* – e modifica norme di precedenti regolamenti (fra cui il regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici), perché si stratta di sistemi che possono avere un "*impatto negativo sulla salute, sicurezza ed i diritti fondamentali*". Il Considerando (58) del regolamento – che viene in questo lavoro citato nel testo approvato dal Parlamento europeo il 13.3.2024 – riferendosi espressamente ai "*servizi sanitari*", sottolinea che, insieme agli altri elencati, la classificazione "*ad alto rischio*" dipende dal fatto che sono "*utilizzati per determinare se le* [relative] *prestazioni e servizi debbano essere concessi, negati, ridotti, revocati o recuperati dalle autorità*" e che le "*persone fisiche che* [li] *richiedono o ricevono* [...] *sono di norma dipendenti da tali prestazioni e servizi e si trovano generalmente in una posizione vulnerabile rispetto alle autorità competenti*".

(3) Fra i moltissimi studi e contributi in materia, si veda la ricerca disposta da European Commission, Directorate-General for Communications Networks, Content and Technology, *Study on eHealth, Interoperability of Health Data and Artificial Intelligence for Health and Care in the European Union*, in specie Lot 2, PwC (ed.), *Final Study Report*, 2021. Nella dottrina penalistica italiana, fra i lavori recenti si vedano Terrizzi, Medical devices *e diritto penale. Profili di responsabilità del produttore e dell'utilizzatore*, Milano, 2023, e per un'indagine anche sociologica, Amore, Rossero, *Robotica e intelligenza artificiale nell'attività medica. Organizzazione, autonomia, responsabilità. Una ricerca sociologica e giuridico-penale*, Torino, Bologna, 2023.

(4) In tal senso si veda la risoluzione approvata all'esito del Colloquio internazionale di Siracusa del 15-16.9.2022, che ha concluso i lavori della Sezione I – dedicata al tema "*Traditional Criminal Law Categories and AI: Crisis or Palingenesis?*" per cui ero *rapporteur général* – organizzato dall'*Association Internationale de Droit Pénal* (AIDP) in vista del Congresso internazionale di cui si è detto alla nota 1. I relativi atti sono pubblicati (a cura di Picotti, Panattoni), nel fascicolo 1/2023 della *Revue Internationale de Droit Pènal*. Volendo cfr. in argomento da ultimo Picotti, *Intelligenza artificiale e diritto penale: le sfide ad alcune categorie tradizionali*, in *Dir. pen. proc.*, 3/2024, 293 s.

a quello del fascicolo sanitario elettronico, che tocca la *privacy*, la *cybersecurity* e la fede pubblica (par. 3), fino a quello della colpa medica (par. 4). O se invece debbano essere escluse, oppure si debbano suggerire soluzioni interpretative o modifiche normative per applicarla.

## 2. Consenso informato: presupposto di liceità penale del trattamento medico chirurgico tramite AI?

### *2.1. Consenso al trattamento sanitario mediante sistemi di intelligenza artificiale*

Notoriamente il consenso libero ed informato è un presupposto generale di liceità dei trattamenti sanitari, enunciato solennemente nella Convenzione di Oviedo del 1997 e nella consolidata interpretazione estensiva della Corte di Strasburgo relativa all'art. 6 della Convenzione europea dei diritti dell'uomo e delle libertà fondamentali (CEDU) sul diritto alla vita privata, oltre che nell'art. 3 della Carta dei diritti fondamentali dell'Unione europea (CDFUE), che è vincolante nell'ambito dell'Unione, nell'estensione di cui al suo art. 52 (5).

Nel nostro ordinamento interno la fonte essenziale è rappresentata dall'art. 32 Cost., che ha trovato un'importante articolazione positiva negli artt. 1-3 legge 22.12.2017, n. 219, in linea con le molteplici previsioni del Codice di deontologia medica (cfr. i relativi artt. 16 e 33-39).

In dottrina (6) e giurisprudenza (7) si è sottolineato che il consenso informato del paziente non dovrebbe ridursi ad un mero scambio burocratico di moduli e di firme, ma dovrebbe consistere in un "percorso informativo e dialogico" con il medico, finalizzato alla alleanza terapeutica. Obiettivo che non è questa la sede per discutere se sia raggiunto o meno nella prassi quotidiana della medicina.

Piuttosto è qui da chiedersi come si debba atteggiare la disciplina e la prassi del consenso infornato, se intervengano sistemi AI in fase di diagnosi o di cura, o nell'uso di dispositivi a domicilio che ricorrano a tali tecnologie, anche con connessioni a distanza. Infatti, rispetto all'obbligo di fornire un'informazione completa e chiara da parte del medico o della struttura, si frappongono (anche a prescindere dai limiti posti dal segreto industriale) gli ostacoli più specifici della c.d. opacità con cui i sistemi operano, per la cripticità del linguaggio, per i contenuti dei data base e dei possibili *bias* cognitivi, per gli effetti di imprevedibilità del *machine learning* o addirittura l'"imperscrutabilità" della c.d. *black box*.

La soluzione non può essere l'affidamento cieco del paziente e, per certi aspetti, anche del medico e dell'operatore sanitario nell'operato dei sistemi AI, vale a dire nelle "decisioni" da essi suggerite od attuate (8), che possono presentare anche un deficit etico, dato che nelle scelte del medico persona umana si deve o si può tenere conto di circostanze e caratteristiche personali o variabili di contesto, che possono condizionare le decisioni sul trattamento in termini diversi rispetto all'output cui può pervenire il sistema AI sulla base di dati statistici e cognitivi generali relativi alla patologia da trattare (si può fare l'esempio di un tumore maligno genitale di una giovane donna, in cui si debba optare fra un intervento demolitivo ed uno conservativo).

Certamente il paziente deve essere reso "edotto" del ricorso ad un sistema AI nel trattamento cui viene sottoposto, come ha affermato condivisibilmente il Comitato nazionale di bioetica in una risoluzione su "Intelligenza artificiale e medicina: aspetti etici" (9), e come si desume anche dall'obbligo generale di trasparenza stabilito

(5) L'art. 3 – collocato nel Capo I dedicato alla "Dignità", subito dopo l'art. 1 dedicato alla "Dignità umana" ed all'art. 2 dedicato al "Diritto alla vita" – sotto la rubrica: "Diritto all'integrità della persona" recita: "*1. Ogni individuo ha diritto alla propria integrità fisica e psichica. 2. Nell'ambito della medicina e della biologia devono essere in particolare rispettati: - il consenso libero e informato della persona interessata, secondo le modalità definite dalla legge, - il divieto delle pratiche eugenetiche, in particolare di quelle aventi come scopo la selezione delle persone, - il divieto di fare del corpo umano e delle sue parti in quanto tali una fonte di lucro, - il divieto della clonazione riproduttiva degli esseri umani*". Mentre ai sensi dell'art. 52, par. 3, viene precisato che "*Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione*", salva una "*protezione più estesa*".

(6) Cfr. nell'ampia bibliografia Canestrari, *Il consenso informato e il rifiuto informato delle cure come "baluardi" di intangibilità corporea. Riflessioni a margine della l. 219/2017*, in *Per una ragione artificiale. In dialogo con Lorenzo d'Avack su Costituzione, ordine giuridico e biodiritto*, Roma, 2023, 137 s.; Eusebi, *Il consenso informato e le disposizioni anticipate di trattamento*, in Oliva - Caputo (a cura di), *Itinerari di medicina legale e delle responsabilità in campo sanitario*, Milano, 2021, 418 s.; già ampiamente Vallini, *Trattamento medico e consenso informato del paziente*, Roma, 2012, cui si rinvia anche per gli ampi richiami bibliografici e giurisprudenziali.

(7) Nel tormentato succedersi di orientamenti sulla rilevanza del consenso del paziente quale fondamento di legittimazione dell'attività medico chirurgica (anche) ai fini penali, basti qui il richiamo alla sentenza della Cass. sez. un. pen., ud. 28.12.2008, dep. 21.1.2009, n. 2437, con nota di Viganò, *Omessa acquisizione del consenso informato del paziente e responsabilità penale del chirurgo: l'approdo (provvisorio?) delle Sezioni Unite*, in *Cass. pen.*, 2009, 1811 s., che ha inteso ricomporre il contrasto di giurisprudenza emerso negli anni, su cui si tornerà nel testo.

(8) Si parla non solo in letteratura del rischio di automatico od eccessivo affidamento sugli *output* dei sistemi AI: tanto che l'*AI Act* prevede, fra i requisiti della persona fisica che deve garantire la "sorveglianza umana" su un sistema AI ad alto rischio, come sono quelli in esame, che essa debba "*restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio ("distorsione dell'automazione"), in particolare per i sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche*" (art. 14, par. 3, lett. b).

(9) <https://bioetica.governo.it/it/documenti/pareri-gruppo-misto-cnbcnbbsv/intelligenza-artificiale-e-medicina-aspetti-etici/> del 29.5.2020.

dall'*AI Act*, che all'art. 50, par. 1, fissa l'obbligo per i fornitori di garantire che i sistemi destinati ad interagire direttamente con le persone fisiche siano progettati e sviluppati in modo che gli interessati siano informati che un sistema AI sta interagendo con loro: obbligo che deve operare, quindi, non solo a tutela del paziente, ma anche del medico e del personale sanitario che ne facciano uso, e che indirettamente grava anche sull'ente sanitario che rende disponibili all'uso tali sistemi (*disployer*, secondo la terminologia dell'*AI Act*).

Ma il primo problema sorge nello stabilire fino a che punto l'informazione debba e possa essere dettagliata anche dal punto vista tecnico (sul contenuto e sull'operatività degli algoritmi, sulle tecniche di *machine learning*, sul novero dei rischi che possano prevedersi, ecc.), affinché il consenso stesso possa poi dirsi "cosciente" e consapevolmente prestato.

Già si è rilevato che l'informazione non può e non deve essere "eccessiva", sia perché può essere opportuno tacere nei dettagli l'intero novero dei possibili rischi, per non instillare spropositate paure, sia perché potrebbe addirittura viziare il consenso, se andasse oltre la "*capacità di comprensione*" del destinatario, richiamata espressamente dall'art. 33 Codice di deontologia medica (10): capacità, si può aggiungere, da valutare anche in relazione ai contenuti tecnici che vengano in rilievo.

Un'informazione non solo sull'uso, ma anche sui rischi e sul possibile malfunzionamento del sistema AI dovrebbe comunque essere data, pur se fossero statisticamente rari, ma non imprevedibili.

Nelle regole cautelari stabilite dal regolamento europeo relative alla "*sorveglianza umana*" obbligatoria per un sistema AI ad altro rischio, come è quello che coinvolge la salute e i diritti fondamentali della persona, è espressamente previsto che si debbano considerare i rischi sia quando il sistema è "*utilizzato conformemente alla sua finalità prevista*", sia quando possa essere "*in condizioni di uso improprio ragionevolmente prevedibile*" (così l'art. 14 dell'*AI Act*). E dunque di questi rischi deve essere informato il paziente, che deve aver conoscenza delle "*conseguenze delle scelte operate*" (11).

Di certo, nel rapporto medico-paziente non basta dar rilievo alla *voluntas* della "parte debole", in qualsivoglia modo espressa o fondata, poiché il paziente non si trova in posizione di parità: per cui è necessario stabilire a livello pubblicistico limiti e garanzie per tutelarla (come avviene a tutela di lavoratori, consumatori, investitori, ecc.) (12).

Ed al riguardo può essere interessante menzionare anche l'art. 7, rubricato: "*Uso dell'intelligenza artificiale in ambito sanitario e disabilità*", del recente schema di disegno di legge "Recante disposizioni e delega al governo in materia di intelligenza artificiale", approvato dal Consiglio dei Ministri il 23.4.2024.

Infatti, dopo aver dato atto, al primo comma, dell'utilità dei sistemi di intelligenza artificiale "*per il miglioramento del sistema sanitario e la prevenzione e cura delle malattie*", ribadendo che il loro utilizzo "*deve avvenire nel rispetto dei diritti, delle libertà e degli interessi della persona, anche in materia di protezione dei dati personali*" (aspetto quest'ultimo regolato dal successivo art. 8, su cui si tornerà *infra*, par. 3.1.1), si stabilisce al terzo comma il "*diritto*" dell'interessato "*di essere informato circa l'utilizzo di tecnologie di intelligenza artificiale e sui vantaggi, in termini diagnostici e terapeutici, derivanti dall'utilizzo delle nuove tecnologie, nonché di ricevere informazioni sulla logica decisionale utilizzata*".

Se appare senz'altro opportuno un tale riconoscimento, che nel contempo delimita l'oggetto dell'informativa alla "*logica decisionale*" che viene utilizzata dal sistema, allineandosi alla posizione intermedia sull'inopportunità di un obbligo di informativa eccessivamente dettagliata dal punto di vista tecnico, garantendone però l'essenziale contenuto sul ruolo concreto che il sistema di intelligenza artificiale può assumere, non si comprende per quale ragione non siano poi menzionati espressamente, accanto ai "*vantaggi*" in termini diagnostici e terapeutici, anche i "*rischi*" che l'uso di siffatte tecnologie può comportare, essendo fondamentale, nella finalità stessa dell'informazione in materia, quale base dell'espressione del consenso consapevole al trattamento sanitario, che l'interessato sia avvertito anche dei rischi specifici inerenti al trattamento così realizzato. Di certo, l'espressa finalità perseguita dal legislatore di "*promuovere*" lo sviluppo, la ricerca e la diffusione di tali sistemi (comma 4), non può spingersi fino a violare la soprastante affermazione del rispetto dei diritti e delle libertà fondamentali della persona nell'utilizzo dei sistemi stessi, solennemente proclamati nelle Carte internazionali. Per cui non si può che auspicare una più completa formulazione di tale disposizione.

(10) Secondo cui "*Il medico deve fornire al paziente la più idonea informazione sulla diagnosi, sulla prognosi, sulle prospettive e le eventuali alternative diagnostico terapeutiche e sulle prevedibili conseguenze delle scelte operate. Il medico dovrà comunicare con il soggetto tenendo conto delle sue capacità di comprensione, alfine di promuoverne la massima partecipazione alle scelte decisionali e l'adesione alle proposte diagnostico terapeutiche. [omissis]*". In argomento cfr. De Menech, *Intelligenza artificiale e autodeterminazione in materia sanitaria*, in Faccioli (a cura di), *Profili giuridici della robotica e dell'intelligenza artificiale in medicina*, Napoli, 2022,9 s., in specie 23.

(11) Così il citato art. 33 del Codice di deontologia medica.

(12) Così sottolinea opportunamente De Menech, *Intelligenza artificiale e autodeterminazione*, cit., 22, con essenziali richiami bibliografici cui si rinvia.

### *2.2. Sulla marginale rilevanza penale di un consenso non adeguatamente informato*

Sul piano della responsabilità penale la questione è però sdrammatizzata dalla evoluzione della giurisprudenza interna, circa il rilievo che può avere un invalido consenso al trattamento.

Se l'informazione non è "*adeguata*" certamente il consenso non è valido. Ma si è tuttavia evidenziato che tale vizio non ha di per sé valenza causale rispetto alla colpa per l'evento costitutivo di un eventuale reato in danno del paziente.

Rispetto ad un esito infausto o comunque avverso potrebbe delinearsi una responsabilità civile, ma non una responsabilità penale, come affermato ormai da numerose pronunce della Suprema Corte, a partire dalla citata sentenza delle Sezioni unite penali n. 2437/2009, con cui è stato escluso che si possa configurare il delitto di violenza privata (*ex* art. 610 c.p.) o, in caso di evento avverso, di lesioni personali dolose (*ex* art. 582 e 583 c.p.), o tantomeno di omicidio preterintenzionale (*ex* art. 584 c.p.), come in precedenza era stato ritenuto, per un trattamento medico chirurgico posto in essere in assenza di consenso o sulla base di un consenso invalido (13).

Il consenso che viene in rilievo in queste ipotesi, infatti, non ha funzione scriminante, *ex* art. 50 c.p., vale a dire di escludere l'antigiuridicità di un fatto che sarebbe altrimenti illecito, in quanto corrispondente ad una fattispecie di reato, perché l'attività medica persegue una finalità o, meglio, una funzione terapeutica rispetto ad una patologia in atto, per cui di per sé non integra una condotta penalmente tipica. La circostanza che essa incida, materialmente, sul corpo e sull'integrità fisica del paziente, non configura in altri termini il reato di lesioni dolose, anche se manchi o sia invalido il consenso ad essa. La responsabilità penale può, infatti, sorgere solo per una violazione della *lex artis*, che sia causale per la determinazione dell'evento. Oppure nel caso che dolosamente siano state omesse informazioni o date informazioni inveritiere per ottenerlo (14), od ancora, sul piano della colpa, se la carenza di informazioni al paziente abbia impedito di acquisire dallo stesso dati ed informazioni rilevanti ai fini del trattamento (15).

In conclusione, una seppur carente informazione sul ricorso a sistemi AI nel trattamento medico chirurgico, fermi i limiti sopraddetti, non potrebbe di per sé dar luogo ad una responsabilità penale, salvo non consenta di acquisire informazioni rilevanti anche per il sistema AI, sullo stato del paziente stesso.

## 3. Digitalizzazione dei dati sanitari: *privacy, cybersecurity* e falsità informatiche

Un vasto ambito di altre questioni di possibile rilievo penale suscita la digitalizzazione dell'attività sanitaria, anche a prescindere dall'impiego concreto di sistemi AI, da essa peraltro reso possibile e che si sta già diffondendo e certamente si diffonderà ulteriormente nei prossimi anni.

Mi riferisco soprattutto all'introduzione ed all'utilizzo del "Fascicolo sanitario elettronico" (FSE) e della "Cartella clinica elettronica" (CCE), oltre che al ricorso alla telemedicina e alla robotica, specie nella chirurgia di precisione e nei servizi assistenziali, da collocare nel quadro sovranazionale ormai delineato dal più recente regolamento dell'Unione europea per lo "*spazio europeo dei dati sanitari*" (c.d. *EHDS*) (16) e da quello generale sull'intelligenza artificiale (*AI Act*), entrambi di prossima entrata in vigore.

Del resto, si tratta di obiettivi di necessaria modernizzazione della sanità, che rientrano nell'area 6 del PNRR, per vero solo parzialmente raggiunti, e che coinvolgono i temi della *privacy*, da un lato, e della *cybersecurity*, dall'altro, oltre che del valore probatorio degli atti e documenti digitali.

(13) Cfr. Cass. pen., Sez. V, ud. 24.11.2015, dep. 21.4.2016, n. 16678, che si conforma a quanto espresso nella sentenza Cass. sez. un. pen., ud. 28.12.2008, dep. 21.1.2009, n. 2437, sopra citata a nota 7.

(14) Per un caso clamoroso di interventi chirurgici realizzati addirittura senza oggettive indicazioni terapeutiche, per scopi di lucro, causando lesioni e morte di pazienti, si veda Cass., Sez. I, 3 aprile 2018 (ud. 22 giugno 2017), n. 14776, a seguito della quale l'imputato Paolo Brega Massone è stato condannato a 21 anni e 4 mesi di reclusione per omicidio preterintenzionale di quattro pazienti, in luogo dell'iniziale condanna all'ergastolo per omicidio doloso.

(15) Così Cass. Sez. IV, 22.5.2015, n. 21537.

(16) Il testo approvato dal Parlamento europeo nell'aprile 2024, dopo l'accordo politico raggiunto con Consiglio e Commissione il 14 marzo precedente, è reperibile, in versione ufficiale anche italiana, al sito: <https://www.europarl.europa.eu/doceo/document/A-9-2023-0395-AM-558-558_IT.pdf>. Pur muovendo dalla base generale del regolamento (UE) 2022/868 sulla governance dei dati del 30.5.2022, fornisce norme più specifiche per il settore sanitario che riguardano lo scambio di dati sanitari digitalizzati e possono incidere sui fornitori di servizi di condivisione di dati, sui formati che garantiscono la portabilità dei dati sanitari, sulle norme di cooperazione per l'altruismo dei dati nel settore sanitario nonché sulla complementarità nell'accesso a dati privati per l'uso secondario (cfr. Relazione della Commissione alla proposta di regolamento del 3.5.2022 COM(2022) 197 final. Senza qui entrare nel dettaglio di questa nuova complessa disciplina, basti richiamare il comunicato dell'ufficio stampa del Parlamento europeo del 24.4.2024, secondo cui l'atto europeo consentirà agli operatori sanitari un accesso più rapido alle cartelle cliniche dei pazienti, anche per quelli provenienti da altri paesi dell'UE, grazie all'introduzione di un "formato europeo" comune, per cui il migliore accesso e scambio di dati sanitari non solo comporterà procedure amministrative più rapide ed economiche, ma nel contempo consentirà anche ai ricercatori un accesso ai dati sanitari più efficace e di qualità superiore, per migliorare i trattamenti e la ricerca. Di qui i vantaggi anche per i cittadini, cui le norme in materia di *privacy* e sicurezza dovranno garantire che nessuna informazione personale sia condivisa e che i pazienti abbiano sempre la possibilità di aggiungere informazioni, correggere dati errati, limitare l'accesso e ottenere informazioni sul trattamento dei propri dati.

### *3.1. Sul trattamento dei dati sanitari quali "dati personali particolari"* (privacy)

Muovendo dalla *privacy*, basti dire che la digitalizzazione della sanità implica una nuova modalità di raccolta e trattamento di "*dati particolari*" quali sono quelli concernenti la salute, che ricadono nella previsione degli artt. 5 e 6, par. 1, del regolamento (UE) 2016/679 (c.d. GDPR), per cui è necessario il consenso al trattamento, che deve essere dato, previa adeguata informazione, per uno o più "*scopi specifici*", come si evince anche dall'art. 9, par. 2, lett. a), secondo cui quelli relativi alla salute rientrano nei "*dati appartenenti a categorie particolari*" (precedentemente qualificati nel Codice *privacy* come "*dati sensibili*", sulla base delle distinzioni portate dall'oggi abrogata Direttiva CE 95/46).

La prima questione che si pone è se, oltre alla digitalizzazione, il ricorso a sistemi AI nel trattamento di questi "*dati particolari*" debba essere preciso oggetto dell'informativa sulla cui base viene richiesto il necessario consenso ed eseguito il successivo trattamento. La risposta ritengo debba essere senz'altro affermativa, pur nei limiti di ragionevolezza e proporzionalità dei contenuti dell'informazione, che non deve essere "eccessivamente" tecnica, proprio per essere comprensibile dall'interessato, come si è già detto sopra (par. 2.1) a proposito del pur distinto consenso al trattamento sanitario che implichi l'impiego di sistemi AI.

La seconda questione, di carattere più generale, è in che misura la digitalizzazione su larga scala ed il ricorso a sistemi AI in questo settore rappresenti un fattore strutturalmente "antagonista" rispetto al diritto al controllo del flusso dei propri dati ed al principio di minimizzazione.

In effetti, tali tecnologie aumentano in termini esponenziali le occasioni di compressione ed offesa della *privacy*, per la raccolta massiva che la digitalizzazione consente e nel contempo richiede, specie quando nel trattamento intervengano sistemi di AI, in quanto è necessaria per garantire precisione e accuratezza nella diagnosi e nel trattamento sanitario, oltre che per la miglior organizzazione e gestione dei servizi ed allocazione delle relative risorse umane e finanziarie.

Il tema non è dunque di impedire od ostacolare la raccolta e l'utilizzo di tali dati, che è anche a favore degli interessati, oltre che della collettività, ma piuttosto quello dei limiti e delle condizioni che devono porsi ed osservarsi, perché il loro trattamento, in tutte le sue diverse fasi, sia lecito, applicando la disciplina delineata dal GDPR ed, oggi, adattata dalle norme dell'*AI Act* in materia di raccolta e trattamento dei dati necessari all'addestramento ed al funzionamento corretto dei sistemi e modelli AI "*ad alto rischio*", oltre che dal regolamento sullo "*spazio europeo dei dati sanitari*" sopra richiamati (*EHDS*), per quanto riguarda soprattutto la loro possibilità di condivisione e trasferimento anche transfrontaliero.

Occorre, infatti, ricordare che la materia dell'"*Accesso* [...] *alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di* assistenza sanitaria, *nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi*" [evidenziazioni aggiunte] rientra nel paragrafo 5, lettera a), dell'elenco di cui all'Allegato III – concernente i sistemi AI classificati "*ad alto rischio*", ai sensi dell'art. 6, par. 2 dell'*AI Act* – in quanto possono avere un "*impatto negativo sulla salute, sicurezza ed i diritti fondamentali*" (17).

Alla stregua di questa disciplina, per il *training* di tali sistemi si deve ricorrere, di regola, ai c.d. dati sintetici od a "*dati derivati*", che tramite l'anonimizzazione e/o la pseudonimizzazione consentano di non individuare (se non in ipotesi tassative) l'identità personale dei singoli interessati, cui i dati in questione si riferiscono, pur acquisendo tutte le informazioni utili per l'elaborazione statistica, diagnostica, scientifica, ecc.

Ma vi possono essere situazioni in cui, se "*strettamente necessario*" per rilevare e correggere eventuali "*distorsioni*", i fornitori di sistemi AI sono autorizzati a trattare anche i "*dati particolari*" di cui si è detto, con i limiti e le condizioni stabilite in particolare dall'art. 10, par. 5, *AI Act*, rubricato "*Dati e governance dei dati*", che non collimano del tutto, nonostante le rassicuranti affermazioni normative, con quelle del GDPR.

Il primo problema è rappresentato dal diritto alla "revoca" del consenso, riconosciuto dall'art. 7, par. 3 GDPR, che può rappresentare un ostacolo a tali trattamenti, salvo ritenere, al contrario, che divenga addirittura impossibile il suo esercizio, negando inaccettabilmente tale diritto.

Il problema sembra superabile solo muovendo dal rilievo che il trattamento dei dati sanitari può trovare una base giuridica anche diversa dal consenso dell'interessato, già alla stregua delle previsioni contenute nell'art. 9, par. 2, lett. i) e j) GDPR, che menzionano le finalità di "*ricerca scientifica*" od i "*fini statistici*".

Ed al riguardo rileva a livello interno la disciplina di cui agli artt. 110 e 110-*bis* Codice *privacy*, che riguardano specificamente la "Ricerca medica, biomedica ed epidemiologica" ed il "Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici".

In forza della prima norma "*il consenso dell'interessato non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento*" oltre che "*quando, a causa di particolari ragioni,*

(17) Come si legge nel considerando (47). Ma la clausola, inclusiva della "*salute*", ricorre in molte altre parti dell'*AI Act*, sia nei suoi Considerando, sia nell'articolato.

*informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca*". Mentre in forza della seconda norma (18) spetta al Garante "*autorizzare il trattamento ulteriore di dati personali, compresi quelli dei trattamenti speciali di cui all'articolo 9 del Regolamento, a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attività quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca*" (*... omissis...*).

In termini più estesi è destinato però ad intervenire in materia il nuovo regolamento UE sullo "*spazio europeo dei dati sanitari*" (*EHDS*: cfr. *supra*, nota 16), che riconoscendo espressamente l'interesse pubblico nel settore della sanità pubblica, detta una specifica disciplina al riguardo.

Tornando all'ordinamento interno, occorre menzionare in specie l'art. 2-*sexies* del Codice *privacy*, rubricato: "*Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevanti*", che richiama, ma in realtà va potenzialmente oltre il disposto dell'art. 9, par. 1, GDPR, in quanto elenca una serie di fonti europee ed interne, di rango non soltanto legislativo, da cui si possa desumere che i trattamenti siano "*necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g)*" del medesimo articolo 9 GDPR: vale a dire "*qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*".

Ed il comma 1-*bis* dello stesso art. 2-*sexies*, nel testo introdotto dall'art. 44 del recentissimo decreto legge 2.3.2024 n. 19, convertito dalla legge 29.4.2024, n. 56, stabilisce che "*I dati personali relativi alla salute, pseudonimizzati, sono trattati, anche mediante interconnessione, dal Ministero della salute, dall'Istituto superiore di sanità (ISS), dall'Agenzia nazionale per i servizi sanitari regionali (AGENAS), dall'Agenzia italiana del farmaco (AIFA), dall'Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle malattie della povertà (INMP), nonché', relativamente ai propri assistiti, dalle regioni e dalle province autonome, nel rispetto delle finalità istituzionali di ciascuno, secondo le modalità individuate con decreto del Ministro della salute, adottato ai sensi del comma 1 previo parere del Garante per la protezione dei dati personali*".

Si tratta, dunque, di una disciplina di carattere generale, sostanzialmente indeterminata nei suoi contenuti concreti, che non sembra poter fungere adeguatamente da precetto di una fattispecie penale, quale quella di cui all'art. 167 *bis* dello stesso Codice, che ad essa soltanto però rinvia (senza menzionare gli artt. 110 e 110-*bis* appena citati), e di cui appresso si dirà (cfr. *infra* par. 3.1.2).

### *3.1.1. Considerazioni critiche sulle norme previste dallo schema di disegno di legge in materia di intelligenza artificiale riguardante i dati sanitari*

All'utilizzo dei dati personali anche "*particolari*" da parte di sistemi AI nell'ambito sanitario, il citato schema di disegno di legge governativo in materia di intelligenza artificiale (cfr. *supra*, par. 2.1) dedica l'intero art. 8.

Sotto la rubrica "*Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario*" la norma prevede, al primo comma, che "*sono dichiarati di rilevante* interesse pubblico *in attuazione dell'articolo 32 della Costituzione e nel rispetto di quanto previsto nell'articolo 9 lettera g) del Regolamento UE 679/16*" [...] "*I trattamenti di dati*, anche personali, *eseguiti da soggetti pubblici e privati* senza scopo di lucro *per la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale per finalità di prevenzione, diagnosi e cura di malattie, sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicali, incluse protesi e interfacce fra il corpo e strumenti di sostegno alle condizioni del paziente, di salute pubblica, incolumità della persona, salute e sicurezza sanitaria*, in quanto necessari *ai fini della realizzazione e dell'utilizzazione di banche dati e modelli di base*" [evidenziazioni aggiunte].

Su tale premessa, nel secondo comma sono indicati i requisiti di legittimazione del trattamento di queste categorie dati, superandosi con una certa disinvoltura il requisito del "*consenso dell'interessato*", anche "*ove inizialmente previsto dalla legge*", in quanto si stabilisce – peraltro senza stringenti condizioni – che, da un lato, "*l'obbligo di informativa dell'interessato*" (...) "*può essere assolto anche mediante messa a disposizione di un'*informativa generale sul sito web *del titolare*" e che, dall'altro, per i trattamenti che perseguano le finalità sopraddette è "*sempre autorizzato l'uso* secondario *di dati personali privi degli elementi identificativi* diretti, *anche appartenenti alle categorie indicate all'articolo 9 del regolamento UE n. 679/2016*" [evidenziazioni aggiunte].

A garanzia di un uso corretto di tali dati, si richiede una formale "*approvazione*" dei trattamenti "*da parte dei*

(18) Articolo aggiunto dall'art. 28, comma 1, lettera b) della legge 20 novembre 2017, n. 167, recante "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2017" e poi novellato, mentre l'art. 44 del recentissimo decreto-legge 2.3.2024, n. 19, convertito dalla legge 29.4.2024, n. 56, ha modificato anche il primo comma dell'art. 110 citato, attribuendo al Garante il compito di individuare le garanzie da osservare, in sostituzione dell'obbligo di consultarlo.

*comitati etici interessati*" e la loro "*comunicazione*" all'Autorità garante per la protezione dei dati personali, che potrebbe disporne il blocco entro trenta giorni, valendo altrimenti il silenzio-assenso.
Tuttavia, una tale disciplina appare censurabile, per la genericità dei *presupposti di legge* che consentono il superamento del diritto fondamentale al consenso informato in questo settore particolare di dati personali, che toccano l'identità psico-fisica della persona e la sua stessa storia, cui non può certo sopperire l'appesantimento burocratico "diffuso", ma inadeguato, che verrebbe introdotto, vista la possibilità di esiti difformi da comitato a comitato e la mancanza di specifiche competenze in materia. Nel contempo, appare insufficiente, oltre che difficile da realizzare in concreto, l'intervento del Garante della *privacy*, certamente ben più competente, che – scalzato dal ruolo ora assegnatogli dal Codice *privacy*, in forza delle norme sopra richiamate (par. 3.1.) – potrebbe solo residualmente "bloccare", nel termine molto stretto di trenta giorni, i trattamenti già approvati dai comitati etici, senza alcuna previsione della possibilità di dare prescrizioni o anche previe indicazioni per il superamento *ab origine* di criticità riscontrabili. Per cui si indebolirebbe l'attuale meccanismo di garanzia, già per vero notevolmente elastico.
È, quindi, auspicabile che nel corso dei lavori parlamentari la norma venga sostanzialmente riveduta, con una più chiara definizione normativa dei presupposti che legittimano siffatte modalità e condizioni dei trattamenti, mantenendosi il ruolo centrale della funzione e dell'azione del Garante, in quanto autorità politicamente indipendente, deputata proprio a salvaguardare i diritti e le libertà fondamentali che vengono in rilievo in tutti gli ambiti di trattamento dei dati personali, compreso in particolare quello sanitario.
Lo schema di disegno di legge governativo sull'intelligenza artificiale interviene anche sul trattamento dei dati acquisibili nel "Fascicolo sanitario elettronico" (già oggetto del comma 1-*bis* dell'art. 2-*sexies* del Codice *privacy*, introdotto dall'art. 9 del decreto legge 8.10.2021, n. 139, convertito dalla legge 3.12.2021, n. 205), in forza del quale "*I dati personali relativi alla salute, privi di elementi identificativi* diretti, *sono trattati, nel rispetto delle finalità istituzionali di ciascuno, dal Ministero della salute, dall'Istituto superiore di sanità, dall'Agenzia nazionale per i servizi sanitari regionali, dall'Agenzia italiana del farmaco, dall'Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle malattie della povertà e, relativamente ai propri assistiti, dalle Regioni anche mediante l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Servizio sanitario nazionale, ivi incluso il Fasciolo Sanitario Elettronico (FSE),* aventi finalità compatibili *con quelle sottese al trattamento, con le modalità e per le finalità fissate con* decreto del Ministro della salute, *ai sensi del comma 1, previo parere del Garante, nel rispetto di quanto previsto dal Regolamento, dal presente codice, dal codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e dalle linee guida dell'Agenzia per l'Italia digitale in materia di interoperabilità*" [evidenziazioni aggiunte].
Da siffatta norma emerge una gran quantità di enti legittimati a trattare "*dati personali relativi alla salute*", rispetto ai quali è garantita solo l'assenza di dati identificativi "*diretti*", mentre le regole del trattamento sono stabilite dal Ministero della salute, con proprio "*decreto*" sottoposto al mero parere del Garante (della *privacy*), da ritenere peraltro non vincolante, in mancanza di tale specificazione. Per cui appare violata sia la garanzia del suo "*controllo*", sia quella della riserva di "*legge*", che dovrebbe valere non solo ai fini penali, dato che tali regole costituiscono tecnicamente un'integrazione normativa del precetto di cui all'art. 167-*bis* Codice *privacy* (cfr. *infra* par. 3.1.2.), ma anche in materia di tutela dei diritti fondamentali della persona (19), tanto più esposti a rischio quando intervengano, nel trattamento, sistemi di intelligenza artificiale, che in quest'ambito, come detto, sono classificati dall'*AI Act* "*ad alto rischio*".
Al riguardo, il citato schema di disegno di legge governativo sull'intelligenza artificiale dedica il suo art. 9 anche ad una novella in materia di "Fascicolo sanitario elettronico", prevedendo l'introduzione dell'art. 12-*bis* (rubricato: "*intelligenza artificiale nel settore sanitario*") nel decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre, 2012, n. 221, in forza del quale verrebbe istituita una "*piattaforma di intelligenza artificiale*" per il supporto alle finalità di cura e per l'assistenza territoriale (comma 2), le cui "*soluzioni di intelligenza artificiale*" sono disciplinate da appositi decreti emanati ai sensi del comma 1, coinvolgendo sia l'Autorità "politica" per l'innovazione tecnologica e la transizione digitale, sia quella (altrettanto "politica") per la sicurezza della Repubblica e la cybersicurezza, non però l'Autorità garante per la protezione dei dati personali, che viceversa sarebbe non solo quella più specificamente competente in materia di trattamento di dati personali, ma anche quella indipendente (e non politica) deputata alla tutela dei diritti fondamentali delle persone, come impone il citato art. 8 CDFUE, di parti-

(19) Come noto, l'art. 8 CDFUE, che sancisce il diritto fondamentale alla "Protezione dei dati di carattere personale", di cui vale la pena di riportare il testo, richiama espressamente la garanzia della legge, quale fonte di disciplina del trattamento dei dati personali: "*1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un* altro fondamento legittimo previsto dalla legge. *Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*" [evidenziazioni aggiunte].

colare rilievo trattandosi di "*dati particolari*", quali sono quelli sanitari.
Anche sotto questo aspetto, appare dunque necessario un approfondito confronto sulle scelte di politica legislativa in materia, dovendosi auspicare un'attenta riformulazione delle disposizioni in questione, che devono allinearsi alle vincolanti Carte sovranazionali.
Se è necessario un ragionevole e chiaro bilanciamento fra interessi ed esigenze contrapposte, poiché esso coinvolge diritti fondamentali, deve essere definito dal legislatore europeo e nazionale, con la garanzia di un'Autorità indipendente, non certo a livello amministrativo con decreti o regolamenti, ed un controllo di organi sostanzialmente politici. Se i sistemi AI devono essere posti in grado di sfruttare l'enorme capacità di memoria e la velocità delle connessioni offerte oggi da tutta la rete e potenziare così nella misura massima possibile l'attendibilità delle valutazioni e previsioni probabilistiche, su cui si fondano le diagnosi e le analisi dei fattori o delle situazioni di rischio, per le quali è essenziale la disponibilità di ingenti quantità di dati (*big data*) e la *completezza* dei *data set*, che i singoli operatori o sistemi informatici tradizionali non potrebbero isolatamente raccogliere e trattare in pari misura, con indiscutibili vantaggi per le conoscenze tecnico-scientifiche nel campo medico e della ricerca, e nell'applicazione nei casi concreti, devono però sempre rispettarsi i diritti fondamentali della persona, in specie il diritto fondamentale alla *privacy*, pur ben lontano dall'ottocentesco diritto assoluto "a restare soli", ma da intendere quale diritto all'autodeterminazione informativa, in parallelo con quello all'autodeterminazione nei trattamenti sanitari.
Al riguardo emerge il fondamentale principio di *trasparenza* del trattamento, enunciato espressamente dall'art. 5 par. 1, lett. a), GDPR, che può entrare in conflitto con la menzionata "opacità" dell'AI. Per cui occorre garantirne comunque l'esplicabilità, tenendo conto non solo della menzionata disciplina che concerne la "governance dei dati", ma anche degli specifici obblighi che gravano sui fornitori di sistemi AI "*ad alto rischio*", ai quali spetta assicurare che il loro funzionamento sia "*sufficientemente trasparente da consentire ai deployer di interpretare l'output*" del sistema e "*utilizzarlo adeguatamente*" (art. 13 *AI Act*): trasparenza che dovrebbe logicamente rispecchiarsi, a valle, nel rapporto con gli interessati e gli utenti tutti, vale a dire con i pazienti oltre che con lo stesso personale sanitario.
La normativa interna, che deve comunque rispettare pienamente il diritto fondamentale alla "*protezione dei dati personali*", solennemente proclamato dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea (cfr. nota 19), dovrà adeguarsi anche al citato regolamento UE sullo "*spazio europeo dei dati sanitari*" (*EHDS*), di prossima entrata in vigore, che – tenendo conto dell'esperienza della pandemia (si pensi alla rilevanza delle app e dei sistemi di rilevazione dei contagi durante l'emergenza pandemica per il c.d. *contact tracing*), degli sviluppi del *machine learning* e dell'utilizzo e "riutilizzo" di dati personali su larga scala – pone attente regole al riguardo, in raccordo con la disciplina delineata dall'*AI Act*. (20).
Appare dunque prematuro e non del tutto coerente con tali principi, diritti e gerarchia delle fonti lo schema di disegno di legge governativo nei punti sopra richiamati.

### *3.1.2. Rilevanza penale delle violazioni in materia di trattamento di dati sanitari*

Venendo ora ad un rapido esame dei profili penali connessi alla violazione dell'illustrata disciplina concernente i dati personali di natura sanitaria, vengono in rilievo gli artt. 167 e 167-*bis* del nostro Codice *privacy*, nella formulazione portata dal d.lgs. 10.8. 2018, n. 101, che puniscono rispettivamente il "*Trattamento illecito di dati*" e la "*Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala*".
Si tratta di fattispecie delittuose strutturate quali norme sanzionatorie degli specifici precetti extrapenali sopra richiamati, fissati dal GDPR e dal Codice *privacy*, cui il legislatore rinvia per delineare il contenuto delle condotte consistenti nella loro violazione. Ma tali delitti richiedono due requisiti ulteriori, che ne condizionano la punibilità. Il primo è rappresentato dal "*fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato*": fine che deve essere perseguito dall'agente con le predette violazioni, ma che non è necessario che egli raggiunga oggettivamente, perché si abbia la consumazione del reato, come si verifica in tutte le fattispecie c.d. a dolo specifico (21).
Il secondo requisito selettivo è rappresentato dell'evento consumativo costituito invece dall'oggettivo "*nocumento*" che deve essere dolosamente causato dal reo con la propria condotta.
Tali due elementi sembrano sufficienti a distinguere gli illeciti penali in esame dagli illeciti di natura ammini-

(20) Il raccordo sistematico con il Regolamento generale sull'intelligenza artificiale è evidenziato nel Considerando (68) dell'*AI-Act*: dopo aver premesso che "Gli spazi comuni europei di dati istituiti dalla Commissione e l'agevolazione della condivisione dei dati tra imprese e con i governi, nell'interesse pubblico, saranno fondamentali per fornire un accesso affidabile, responsabile e non discriminatorio a dati di elevata qualità a fini di addestramento, convalida e prova dei sistemi di IA", si indica specificamente ad "esempio, per quanto riguarda la salute, lo spazio europeo di dati sanitari" che "agevolerà l'accesso non discriminatorio ai dati sanitari e l'addestramento di algoritmi di IA a partire da tali set di dati in modo sicuro, tempestivo, trasparente, affidabile e tale da tutelare la vita privata, nonché con un'adeguata governance istituzionale."

(21) Sulla struttura e sulle caratteristiche delle fattispecie c.d. a dolo specifico sia consentito rinviare a Picotti, *Il dolo specifico. Un'indagine sugli 'elementi finalistici' delle fattispecie penali*, Milano, 1993.

strativa, che sono invece previsti dal regolamento europeo, con sanzioni pecuniarie anche severissime (cfr. art. 99-101 *AI Act*) (22), senza violare il divieto di *bis in idem* (cfr. Considerando (168) *AI Act*), che notoriamente si applica anche a livello sovranazionale ed al concorso fra sanzioni penali e sanzioni amministrative che abbiano carattere punitivo (23).

Il delitto previsto dal comma 2 dell'art. 167 Codice *privacy* punisce dunque ("*salvo che il fatto costituisca più grave reato*") con la reclusione da uno a tre anni chi, al fine specifico sopraddetto, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento europeo (GDPR), "*in violazione* (...) *delle misure di garanzia di cui all'articolo* 2-septies" del Codice *privacy* – che riguardano il trattamento dei dati genetici, biometrici, relativi alla salute – "*arreca nocumento*" all'interessato. Mentre il comma 3 stabilisce che la stessa pena si applica altresì a chi, al medesimo fine ed arrecando nocumento, procede "*al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti*".

Senza approfondire in questa sede l'analisi ermeneutica di tali fattispecie, basti segnalare che il menzionato regolamento UE sullo "spazio europeo dei dati sanitari" potrebbe costituire la fonte che legittima anche il trasferimento di tali dati in altri Paesi dell'Unione, alle condizioni in esso previste. Per cui la loro violazione potrebbe integrare il delitto in esame, in quanto il trasferimento avverrebbe "*fuori dei casi consentiti*".

L'altro delitto, previsto dall'art. 167-*bis* Codice *privacy*, è stato introdotto dal citato d.lgs. 101/2018, e considera specificamente la nuova dimensione globale del *web* e la tematica dei *big data*. La fattispecie punisce infatti più gravemente, con la reclusione da uno a sei anni (salvo sempre che il fatto costituisca più grave reato), chi, al fine specifico richiesto anche per gli altri delitti sopra menzionati, "*comunica o diffonde un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento* su larga scala, *in violazione degli articoli* 2-ter, 2-sexies e 2-octies" [evidenziazioni aggiunte]; nonché, ai sensi del comma 2, chi "*comunica o diffonde, senza consenso*" un tale archivio automatizzato o una sua parte sostanziale, "*quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione*".

Diversi sono gli aspetti problematici che la norma presenta (24).

Innanzitutto, la nozione di "*trattamento su larga scala*" presenta un'estrema elasticità di contenuto, che per non confliggere con il principio di determinatezza che presiede alla materia penale, deve trovare una dimensione normativa extrapenale (e tecnologica), che consenta di circoscriverla in termini prevedibilmente accettabili.

In secondo luogo, occorre risalire al contenuto dell'art. 2-*sexies* (in disparte quello degli artt. 2-*ter* (25) e 2-*octies* (26)) Codice *privacy* ed alla complessa disciplina che può far escludere la necessità del consenso per il trattamento dei dati sanitari, di cui sopra si è detto (par. 3.1), perché si possano definire le violazioni che integrano le condotte costitutive della fattispecie penale esame, alle quali devono correlarsi anche gli altri due elementi menzionati (fine specifico di profitto per sé od altri o di danneggiare l'interessato, ed evento consumativo di nocumento).

Ebbene, la norma extrapenale oggetto del rinvio non individua, in realtà, dei contenuti specifici delle eventuali condotte da sanzionare, perché rimanda ad una molteplicità di fonti, fra cui anche regolamenti ed atti amministrativi di rango inferiore alla legge, delle quali non sono esplicitati gli ambiti di intervento ed i criteri direttivi, in violazione (ulteriore) del principio di legalità in materia penale, oltre che in materia di tutela dei dati personali (27).

La sua formulazione dà quindi adito a fondate censure di incostituzionalità, dato che l'articolata e stratificata base giuridica per il trattamento lecito dei dati sanitari digitalizzati, compresi quelli del "Fascicolo sanitario elettronico", anche da parte di sistemi AI, ben al di là del ristretto perimetro individuale dei singoli pazienti per cui siano raccolti e del loro esplicito consenso, non consente di determinare in modo preciso o, comunque, agevole il confine rispetto alle violazioni di rilevanza penale di tale disciplina, che è per di più in forte evoluzione, alla luce delle innovative fonti in materia, che vanno dai regolamenti europei di prossima entrata in vigore

(22) Come noto, le sanzioni amministrative del Codice privacy sono state abrogate, a seguito dell'entrata in vigore del GDPR, che le prevede unitariamente a livello europeo, restando solo disciplinato, a livello nazionale, il relativo procedimento di accertamento e applicazione (cfr. art. 166 Codice privacy, che rappresenta l'unica norma ancora in vigore dell'intero Capo I dedicato alle "Violazioni amministrative" nell'ambito del Titolo III, dedicato alle "Sanzioni", in cui si colloca il Capo II dedicato agli "illeciti penali" di fonte necessariamente nazionale).

(23) Sulla faticosa elaborazione delle Corti europee relative alla portata di tale principio, che costituisce un diritto fondamentale valevole anche in ambito comunitario, sia consentito rinviare, per ragioni di sintesi, a L. Picotti, *Doppio binario sanzionatorio e* ne bis in idem*: verso un accettabile epilogo del lungo dialogo fra le corti?*, in Cadoppi - Veneziani - Aldrovandi - Putinati (a cura di), *Legalità e diritto penale dell'economia. Studi in onore di Alessio Lanzi*, Roma, 2020, 512 s., ed ai richiami giurisprudenziali e bibliografici ivi contenuti.

(24) Per primi commenti si vedano Manes, Mazzacuva, *GDPR e nuove disposizioni penali del Codice privacy*, in *Dir. pen. proc.* 2/2019, 171 s.; De Bernardo, *Le sanzioni penali previste nel nuovo D. lgs. n. 101/2018*, in *giurisprudenza penale web*, 2, 2019, 1.s.

(25) La norma disciplina la "Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri".

(26) La norma contiene i "Principi relativi al trattamento di dati relativi a condanne penali e reati".

(27) Cfr. l'art. 8 CDFUE, riportato a nota 19.

(*AI Act* e *EHDS* sullo "*spazio europeo dei dati sanitari*") fino al recente schema di disegno di legge governativo sull'intelligenza artificiale.
Tuttavia, venendo in gioco diritti fondamentali (basti il rinvio ai citati artt. 3 ed 8 CDFUE), già e senz'altro ancora meritevoli di forte tutela penale, se da un lato non può rinunciarsi ad essa in nome dello sviluppo delle nuove tecnologie, dall'altro – perché il loro rispetto non rappresenti un ostacolo, ma una chiara indicazione per indirizzarne la necessaria regolamentazione giuridica – occorre che la relativa disciplina sia precisa e tassativa, e di fonte legale, convergendo in questo le esigenze di garanzia di tali diritti con i principi garantisti del diritto penale.
Spetta allora al legislatore nazionale non solo adeguare doverosamente l'ordinamento interno ai principi ed ai regolamenti europei richiamati, ma anche dettare una normazione interna precisa e tassativa di natura penale, che è di sua competenza, in modo che lungi dall'indebolirli o da sminuirne la portata, come avverrebbe se si lasciasse troppo spazio alla discrezionalità dell'amministrazione, o, peggio, della politica del momento, ne irrobustisca i presidi di garanzia per i diritti della persona, in conformità all'esigenza di certezza del diritto penale, così rafforzandone l'efficacia e nel contempo delimitandone il campo, in coerenza con la sua funzione di *extrema ratio*.
Una siffatta disciplina, con le debite distinzioni, dovrà comprendere anche i trattamenti dei dati oggetto delle "Cartelle sanitarie elettroniche", contenenti dati amministrativi su prestazioni, dispositivi sanitari, e quant'altro, in cui possono venire in rilievo anche le tematiche dell'*Internet of Things* (IoT), date le caratteristiche di moltissimi dispositivi sanitari.
Gli incroci fra quest'accresciuta molteplicità di dati, compresi quelli "*personali derivati*" o "*sintetici*", e pur dopo i doverosi procedimenti di anonimizzazione o pseudonimizzazione, non deve infatti portare alla possibilità di "re-identificazione" degli interessati.

### *3.2. Sulla* cybersecurity

Nell'ambito dei trattamenti dei dati sanitari digitalizzati, emerge in modo forte il tema della *cybersecurity*, richiamata da molteplici norme anche dell'*AI Act* (28), con relative ricadute penali (29).

Pur non essendo questa la sede per l'approfondimento di un così articolato argomento, va segnalata la ricorrente menzione dell'esigenza di sicurezza cibernetica quale oggetto di molteplici obblighi incombenti sui fornitori, sui *disployer* e più in generale sui titolari e responsabili dei sistemi, per prevenire i rischi non solo di attacchi informatici, ma anche di incidenti e perdite fortuite.
Sul piano penale, rispetto a fatti dolosi di terzi (intranei od estranei) si possono richiamare le fattispecie che a livello nazionale puniscono, innanzitutto, l'accesso abusivo ad un sistema informatico o telematico, che deve essere "*protetto da misure di sicurezza*" per meritare tutela penale (cfr. art. 615-*ter* c.p.), a fronte di condotte criminose che possono realizzarsi anche a distanza (si pensi in particolare ai rischi che sotto questo aspetto potrebbe altresì presentare la telemedicina, per connessioni non adeguatamente protette, anche da parte dell'utente stesso).
In secondo luogo vengono in rilievo i danneggiamenti informatici, che siano in pregiudizio di sistemi AI, e che possono riguardare sia singoli dati o componenti *software* (art. 635-*bis* e art. 635-*ter* c.p.) sia anche componenti *hardware* (art. 635-*quater* ed art. 635-*quinquies* c.p.), secondo una differente struttura e con gravità crescente di pene, a seconda che si tratti di dati e sistemi privati ovvero pubblici, o comunque di interesse pubblico, come sono certamente quelli che vengono in rilievo nell'ambito delle attività sanitarie.
Nell'ampia categoria dei "*sistemi informatici*" oggetto di protezione penale vanno compresi sia l'*hardware* che il *software* di sistemi AI. Ma per la rilevanza penale delle condotte incriminate, si richiede il dolo di chi agisce illecitamente, mentre comportamenti meramente colposi potrebbero avere rilievo solo sul piano delle sanzioni amministrative (fra cui quelle previste dal GDPR) o della responsabilità civile.
Tuttavia, la dimensione della cibersicurezza è oggi ben più estesa, perché la prevenzione di rischi anche di accadimenti accidentali, oltre che di attacchi informatici intenzionali, si compenetra con l'esigenza primaria di protezione e robustezza delle infrastrutture critiche, oltre che dei sistemi di AI "*ad alto rischio*", come quelli in esame.

(28) Senza pretesa di completezza, data la molteplicità di norme in cui compare la necessità di garantire un adeguato livello di cibersicurezza, si vedano ad es. l'art. 70, par. 4, sugli obblighi in materia che devono essere adempiuti dalle autorità nazionali; e l'Allegato IV, par. 5, lettera h) relativo alla "documentazione tecnica" che – ai sensi dell'art. 11, par. 1 - il fornitore dei sistemi AI deve fornire.

(29) In argomento sia consentito rinviare, per un sintetico inquadramento delle norme sul "Perimetro nazionale di sicurezza cibernetica" di cui al decreto-legge 21.9.2019, n. 105, conv. dalla legge 18.11.2020, n. 133, a Picotti, *Cybersecurity:* quid novi?, in questa ***Rivista***, 2020, n. 1, 11 s. Sugli ulteriori sviluppi a livello europeo e nazionale, dopo l'approvazione della c.d. NIS 2, cfr. Flor, *Cybersecurity for Artificial Intelligence e diritto penale: prime riflessioni nel prisma del diritto europeo*, in Luchtman et al. (eds.), *Of swords and shields: due process and crime control in times of globalization - Liber amicorum prof. dr. J.A.E. Vervaele*, Hague, 2023, 785 s.; con specifica attenzione agli aspetti tecnologici si veda Vigano, *Nuove frontiere della cybersecurity*, in Picotti (a cura di), *Automazione, Diritto e Responsabilità*, Napoli, 2023, 213 s. A livello normativo si segnala il più recente decreto-legge 10.8.2023, n. 105, conv. dalla legge 9.10.2023, n. 137, che all'art. 2-*bis* ha integrato i compiti dell'"Agenzia per la cybersicurezza nazionale", istituita con il decreto-legge 14.6.2021, n. 82, conv. dalla legge 4.8.2012, n. 109.

E a loro volta, questi possono e debbono rafforzare i sistemi di cybersicurezza, come espressamente enuncia anche l'art. 16 (rubricato: "*Utilizzo dell'intelligenza artificiale per il rafforzamento della cybersicurezza nazionale*") del citato schema di disegno di legge governativo in materia di intelligenza artificiale (30), in forza del quale all'art. 7, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, che riguarda le funzioni dell'"Agenzia per la cybersicurezza nazionale", dopo la lettera m-*ter*), va inserita la seguente: «m-*quater*) *promuove e sviluppa ogni iniziativa, anche di partenariato pubblico-privato, volta a valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della cybersicurezza nazionale*».

Si tratta ormai di un'esigenza cogente, che coinvolge non solo enti e soggetti pubblici, ma anche enti ed operatori privati, che prestino servizi pubblici essenziali, a partire dunque da quelli sanitari, o siano comunque coinvolti nella catena che va dalla produzione, alla fornitura, fino alla disposizione ed utilizzazione di detti sistemi. Tanto che nel richiamato Schema di disegno di legge governativo sono previsti, all'art. 21, anche specifici interventi di finanziamento per investimenti in questo ambito.

### *3.3. Sulle falsità informatiche*

Infine, un semplice cenno merita anche il tema delle falsità materiali ed ideologiche che riguardino dati e documenti informatici contenuti in specie nel "Fascicolo sanitario elettronico" od anche nelle "Cartelle sanitarie elettroniche", eventualmente imputabili anche all'impiego di sistemi AI.

Viene in questi casi in rilievo l'art. 491-*bis* c.p., che estende espressamente l'applicabilità di tutti i delitti di falsità in atti, offensivi della c.d. fede pubblica, anche alle falsità relative a "*documenti informatici pubblici*", quali sono certamente quelli in questione, essendo tali tutti quelli che, applicando la definizione del Codice dell'Amministrazione digitale, costituiscono "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*" (art. 1, lett. p) d.lgs. 82/2005 e succ. modifiche), redatti od anche ricevuti o conservati da un pubblico ufficiale nell'esercizio delle sue funzioni (31).

Qualche nuovo problema può suscitare però l'attribuzione di una falsità materiale od ideologica, rispettivamente *ex* artt. 476 o 479 segg. c.p., al soggetto umano che "stia dietro" l'impiego di un sistema AI, cui debba farsi risalire la "contraffazione" od "alterazione" del documento informatico, come pure la "difformità dal vero" dell'attestazione in esso contenuta, avente valore probatorio, di atti e fatti giuridicamente rilevanti.

Tali condotte potrebbero essere frutto dell'autonoma acquisizione di dati ovvero dell'autonomo trattamento realizzati dal o tramite un sistema AI. Nonostante l'oggettiva sussistenza di tali falsità, potrebbe non essere accertabile il dolo di un agente umano, richiesto quale condizione per la punizione di queste fattispecie delittuose. Lo spazio di autonomia decisionale, che connota l'operato di detti sistemi, può infatti far sfuggire l'*output* dall'ambito di concreta previsione dell'agente competente, per cui esso non sarebbe imputabile ad una sua volontà consapevole. Al riguardo, non può che farsi rinvio, in questa sede, ai criteri di possibile attribuzione della responsabilità penale, anche per fatti dolosi, elaborati dall'*Association Internationale de Droit Pénal*, nella risoluzione sopra richiamata (cfr. par. 1, in specie note 1 e 4).

## 4. Responsabilità medica per eventi avversi colposi

### *4.1. Premesse generali sulla tutela penale in materia*

Un tema assai rilevante, che si pone di fronte all'utilizzo di sistemi AI in medicina, sia in ambito diagnostico, che in ambito terapeutico ed assistenziale, specie se associati ad *hardware* (robotica), è quello della c.d. colpa medica per eventi avversi attribuibili (anche) all'operato di tali sistemi.

Vengono in rilievo, sotto il profilo penale, gli artt. 589 e 590 c.p., che puniscono rispettivamente l'omicidio colposo e le lesioni personali colpose, di cui l'art. 590-*sexies*, comma 2, c.p. (introdotto dall'art. 6 legge 6.3.2017, n. 24, c.d. legge Gelli-Bianco) limita l'ambito applicativo, nei casi di "*imperizia*", "*quando sono rispettate le raccomandazioni previste dalle linee guida* [...] *ovvero, in mancanza di queste, le buone pratiche clinico-assistenziali*" (32).

(30) Cfr. *supra*, par. 2.1.

(31) Per un inquadramento del tema ed il commento critico della prima formulazione di tale norma si veda, volendo, PICOTTI, *Commento Art. 3 legge 23 dicembre 1993, n. 547 (Art. 491-bis cod. pen.: Documenti informatici)*, in *Legislazione penale*, 1996, n. 1-2, 62 s.; sulla sua modifica cfr. ID., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2018, 700 s., in specie 701 s.; per attente osservazioni anche critiche cfr. GROTTO, *Regime giuridico del falso informatico e dubbi sulla funzione interpretativa dell'art. 491 bis c.p.*, in *Dir. inf. inf.*, 2006, 589 s.

(32) Sull'impatto dell'art. 590-*sexies* c.p. (introdotto dalla c.d. Leggi Gelli Bianco) sui limiti della responsabilità penale del sanitario, fra i numerosissimi contributi si veda RISICATO, *Il nuovo statuto della colpa medica: un discutibile progresso nella valutazione della responsabilità del personale sanitaria*, in *www.lalegislazionepenale.eu*, 5 giugno 2017; per un attento bilancio sintetico CANZIO, *Linee evolutive del sistema della responsabilità in ambito sanitario*, in *Responsabilità sanitaria, rischio clinico e valore della persona*, 2022, 3 s., con essenziali indicazioni bibliografiche e giurisprudenziali. Fra questi in specie si veda Cass. sez. un., 21 dicembre 2017, n. 8770/18, Mariotti, Rv. 272174-75-76, annotata da CUPELLI, *La legge Gelli-Bianco nell'interpretazione delle Sezioni Unite: torna la gradazione della colpa e si riaffaccia l'art. 2236 c.c.*, in *www.penalecontemporaneo.it*, 2017, 12, 135, con ulteriori ampi rinvii.

Si tratta di delitti di evento c.d. a forma libera, per cui qualsiasi azione od omissione, che sia causa o concausa della morte o delle lesioni personali del paziente, *ex* artt. 40, anche capoverso (secondo cui "*non impedire un evento che si ha l'obbligo giuridico di impedire equivale a cagionarlo*") e 41 c.p. (secondo cui il "*concorso di cause... non esclude il rapporto di causalità*", salvo che quelle "*sopravvenute*" siano "*state da sole sufficienti a determinare l'evento*"), può far sorgere la responsabilità dell'esercente la professione sanitaria, e/od eventualmente della struttura ed ente che abbia messo a disposizione il sistema (c.d. diployer), a condizione che – oltre al menzionato nesso oggettivo di causalità – si accerti anche la relativa colpa "personale".
È stato già autorevolmente affermato che non può accettarsi che, sol perché vi è stato l'utilizzo di sistemi AI (in queste ipotesi, ad es., nella diagnosi o nel trattamento sanitario), sia da escludersi la colpa penalmente rilevante, stanti le caratteristiche di (relativa) imprevedibilità degli *output* forniti e dei comportamenti posti in essere con scelte (in concreto) "autonome" da tali sistemi (33). Si creerebbe, altrimenti, uno spazio di impunità od irresponsabilità, rispetto ad offese a beni giuridici anche primari e diritti fondamentali della persona, quali la vita e l'incolumità personale, che richiedono e già ricevono, altrimenti, protezione penale.
Questa non può quindi venir meno, salvo adeguare in concreto i criteri di imputazione della causalità e della colpa alle peculiari caratteristiche di tali sistemi e della loro utilizzazione.
A tal fine si deve muovere dal rilievo che un sistema IA non è riducibile ad un mero strumento passivo nelle mani dell'uomo, come sembrerebbe far pensare il termine di "utilizzo" di un robot (nella chirurgia o nell'assistenza) o di un sistema diagnostico basato sull'IA, perché non resta nel pieno e costante dominio dell'agente umano, come potrebbe essere un bisturi o la lettura di dati clinici e della letteratura medica da parte dell'operatore.
Occorre preliminarmente distinguere fra l'automazione di singole funzioni, che possono restare sotto il diretto controllo umano, e la vera "autonomia" decisionale e operativa, che basandosi su tecniche di *machine learning*, per la ricerca e selezione di enormi quantità di dati ed informazioni (*big data*), non disponibili al singolo operatore, nonché su algoritmi anche adattivi, che si evolvono sulla base dell'esperienza acquisita, porta ad *output* e comportamenti anche immediatamente eseguiti, caratterizzati, come già detto, da "imprevedibilità" e possibile "opacità" del processo che vi è alla base, determinando un'interazione complessa fra uomo e macchina, alla quale il primo si affida.
Escluso il riconoscimento – almeno allo stato attuale dello sviluppo tecnologico – di una soggettività o capacità penale del sistema AI in quanto tale, che non possiede una libertà cosciente di autodeterminazione, invece richiesta a fondamento dell'imputabilità ai fini penali, per cui neppure possibili sanzioni (seppur *sui generis*) potrebbero perseguire, nei suoi confronti, le funzioni (retributiva, nonché di prevenzione generale e speciale) proprie della pena (34), nondimeno emerge un diaframma fra l'atto umano e l'offesa dei beni giuridici penalmente rilevanti, posta in essere da o tramite detti sistemi, cui l'agente umano ed, in particolare, il personale sanitario "delega" importanti attività, facendovi affidamento, data la superiore capacità cognitiva, decisionale ed operativa, sicura, precisa ed immediata, che tali sistemi possiedono. Tanto che può configurarsi, di converso, un obbligo, anche giuridicamente rilevante (ad es. sul piano della colpa, in caso di omissione), di ricorrere ad essi, per garantire il miglior trattamento che la scienza e la tecnologia rendono disponibile (35).
Ai fini della responsabilità penale per eventi avversi, che possano derivarne, occorre dunque risalire ai soggetti che "stanno dietro" ai sistemi AI, e che in effetti decidono di utilizzarli e li utilizzano nel proprio interesse o vantaggio, seppur non egoistico, ma riferibile alla miglior terapia o al più efficace trattamento che devono e così possono porre in essere.

### *4.2. Sul nesso causale*

Tale affidamento (o delega) rappresenta un sicuro *fattore causale*, all'origine della catena che può portare all'even-

(33) Si vedano le raccomandazioni (citate *supra* a nota 4) contenute nella risoluzione adottata a Siracusa il 15-16.9.2022 a conclusione dei lavori della prima sezione del Congresso internazionale dell'*Association Internationale de Droit Pénal*. In materia, nel dibattito penalistico si rinvia ai contributi di Bartoli, *La responsabilità medica tra individuale e collettivo: rischi, regole, centri di imputazione*, in Bianchi (a cura di), *Distribuzione del rischio sanitario tra responsabilità dell'organizzazione e responsabilità individuali*, Torino 2021, 80 s.; Cappellini, *L'"allocazione della colpa" nella responsabilità penale sanitaria*, ivi, 54 s.; Panattoni, *Profili penali dell'interazione uomo-macchina nell'ambito della responsabilità medica*, in Picotti (a cura di), *Automazione, Diritto e Responsabilità*, cit., 269 s. Da ultimo cfr. anche Amore - Rossero, *Robotica e intelligenza artificiale nell'attività medica*, cit., 185 s., Terrizzi, Medical devices *e diritto penale*, cit., 177 s. e, volendo, Picotti, *Robotica ed intelligenza artificiale in medicina: possibili aspetti di rilievo penale*, in Faccioli (a cura di), *Profili giuridici dell'utilizzo della robotica*, cit., 89 s.; nel più esplorato campo della responsabilità civile si veda, oltre all'interessante contributo comparatista di Guerra, *Profili di responsabilità del produttore del robot chirurgico nell'ordinamento americano*, ivi, 57 s., Rizzo, *Strutture della responsabilità civile e intelligenza artificiale: i problemi in medicina*, *ivi*, 1 s.; Faccioli, *Principi e categorie della responsabilità sanitaria alla prova della telemedicina*, in Picotti (a cura di), *Automazione, Diritto e Responsabilità*, cit., 245 s., con ampie indicazioni bibliografiche anche di carattere generale.

(34) Per riferimenti sia consentito rinviare per brevità a Picotti, *Intelligenza artificiale e diritto penale*, cit., 295 s.

(35) Su tali profili cfr. Pagallo, *Il dovere alla salute. Sul rischio di sottoutilizzo dell'intelligenza artificiale in ambito sanitario*, Milano, 2022.

to avverso. Data la menzionata struttura a forma libera dei reati in esame, dal punto di vista del rispetto del principio di legalità è sufficiente, come detto, qualsiasi contributo eziologico alla produzione dell'evento, anche di natura omissiva (*ex* art. 40 capoverso c.p.), ad es. per mancato controllo, essendo configurabile una posizione di garanzia del medico e del personale sanitario competente, rispetto alle fonti di pericolo per la vita, la salute, l'incolumità del paziente ad essi affidato, che costituiscano rischi specifici relativi alla patologia oggetto di cura e, quindi, ricadano nella sfera degli obblighi di vigilanza ed intervento che su di essi incombono (36).
Pertanto, anche di fronte alle c.d. *black box*, non essendo esimente l'*error in causa*, la scelta dell'operatore di ricorrere all'AI appare integrare quanto meno una condizione essenziale da cui dipende la causazione dell'evento, che può inserirsi od aggiungersi alla catena che va dall'ideatore al programmatore, dal produttore al fornitore, fino a chi dispone del ed utilizza concretamente il sistema, in conformità al c.d. principio di equivalenza dei contributi causali, ricavabile dal menzionato art. 41 c.p.
In altri termini, benché l'ultimo anello della catena sia determinato dal "comportamento" del sistema IA, e questo non sia assimilabile ad un mero strumento passivo, non può escludersi il nesso eziologico, in quanto con l'eliminazione mentale dell'antecedente o degli antecedenti in esame, verrebbe meno l'evento stesso.
La "autonomia" dell'AI non può considerarsi, infatti, un fattore del tutto "eccezionale" ed assolutamente imprevedibile, tale da interrompere (*ex* art. 41, capoverso, c.p.) il nesso causale, salvo che anomalie, che abbiano tali caratteristiche, possano esorbitare dal nesso di rischio e far risalire la responsabilità agli anelli anteriori della menzionata catena.
Nonostante la tracciabilità tecnica dell'*iter* che ha portato all'evento, può residuare una difficoltà di prova nella precisa ricostruzione ed individuazione delle caratteristiche e cause delle anomalie che lo abbiano determinato.
Per superare tali difficoltà, può sopperire la disciplina della responsabilità da prodotto difettoso, che la recente proposta di direttiva europea in materia estende espressamente anche a vizi del *software* (37), ferma la sussidiarietà della sanzione penale, rispetto alla tutela risarcitoria di natura civile. Anche la prima dovrebbe però potersi configurare, per l'esposizione a grave rischio di beni primari, se del caso con opportune scelte di politica criminale indirizzate ad un adattamento della disciplina positiva, che delimiti le condizioni e le garanzie di utilizzo dei predetti sistemi.
Inoltre, si potrebbero introdurre fattispecie che anticipino la soglia della tutela penale, per sanzionare quali "reati preparatori" la produzione, la fornitura e l'impiego di "dispositivi medici", in cui rientrano anche i sistemi AI, non autorizzati o pericolosi, od irregolarmente acquisiti tramite appalti non rispettosi della disciplina in materia, finalizzata a garantire anche elevati *standard* di sicurezza.

### *4.3. Sulla colpa "personale"*

Fondamentali principi di garanzia in materia di responsabilità penale richiedono che la sua attribuzione si basi, oltre che sull'elemento oggettivo sopra delineato, su di un rimprovero giuridico "*personale*", quantomeno di natura colposa, come si ricava dall'art. 27, commi 1 e 3, Cost., oltre che dagli artt. 42 e 43 c.p.
Colpa penale che diverge da quella civile, essendo esclusa ogni forma di responsabilità per fatto altrui, ad es. del dipendente, o di responsabilità c.d. per posizione, anziché per la propria azione od omissione, come pure qualsivoglia ricorso a presunzioni od anche inversioni dell'onere probatorio.
Come si è già sottolineato a proposito del ruolo del consenso al trattamento sanitario (*supra* par. 2), ci troviamo nel campo di attività lecite di base, dato che l'invasione anche materiale della sfera corporea del paziente non costituisce una "*lesione*" personale, ai sensi dell'art. 582 c.p., non essendo causa di una "*malattia*" ma, al contrario, essendo un intervento a favore del paziente stesso e della sua salute, data la funzione, più che la semplice "finalità" terapeutica della condotta stessa, diretta a curare la patologia preesistente (salvi i debiti adattamenti rispetto alla chirurgia estetica).
In tale contesto, l'impiego di sistemi AI offre la massima utilità, per l'entità e qualità di informazioni, ampie ed aggiornate, di cui possono e devono disporre, con limitazione della possibilità di errore ed incremento della precisione e rapidità di diagnosi ed intervento.
Il nodo problematico è quello dell'eventuale violazione delle c.d. regole cautelari che devono essere rispettate, anche nel ricorso ai sistemi AI, trattandosi comunque di attività pericolose.
Al riguardo, il modello di comportamento dell'*homo eiusdem conditionis et professionis* – dal quale si ricavano usualmente le regole di diligenza, prudenza e perizia la cui violazione configura la colpa ai fini penali – non appare applicabile ai sistemi AI in quanto tali, che non sono persone umane ed operano con proprie caratteristiche e modalità tecniche.

(36) Sull'ambito di rilevanza penale di tale sfera di obblighi cfr. CAPUTO, *Colpa penale del medico e sicurezza delle cure*, Torno 2017; sui fondamenti generali già FORTI, *Colpa ed evento nel diritto penale*, Milano, 1990, nonché GIUNTA, *Illiceità e colpevolezza nella responsabilità colposa*, Padova, 1993, con i necessari richiami ai molteplici autorevoli contributi precedenti.

(37) In tal senso si veda la proposta di nuova direttiva (2022/0302 (COD)) presentata dalla Commissione europea il 28.9.2022 sulla responsabilità da prodotto difettoso, che modifica la vigente direttiva 85/374/CEE.

Per cui il parametro di riferimento deve essere, piuttosto, quello assai ampio della "miglior scienza ed esperienza" del settore in cui intervengono.
Ma la negligenza, imprudenza ed imperizia punibili non possono imputarsi direttamente ai sistemi AI. Per cui occorre – come si è detto – risalire all'agente umano che "sta dietro", al quale potrebbe rimproverarsi, oltre che l'eventuale esito infausto o lesivo, anche di non aver fatto ricorso, potendolo, ai sistemi AI disponibili (38).
Una particolare questione pone al riguardo il tema cruciale della perizia, dato che, come si è ricordato, non è punibile l'imperizia quando si seguano le "*raccomandazioni previste dalle linee guida* [...] *ovvero, in mancanza di queste, le buone pratiche clinico-assistenziali*", sempre che siano "*adeguate alla specificità del caso concreto*" (art. 590-*sexies* c.p.).
È evidente che queste previsioni non sono dirette ai sistemi AI, ma al personale sanitario che "vi sta dietro", la cui osservanza fonda l'esonero da responsabilità (39).
Per cui occorrerà che le predette raccomandazioni ed, eventualmente, buone pratiche clinico-assistenziali da rispettare, siano integrate ed aggiornate con riferimento all'impiego delle tecnologie in questione, includendo i casi e modi in cui si debba o possa fare ricorso ai sistemi AI disponibili, nonché le caratteristiche che debbano possedere, da impostare e garantire già a monte del loro concreto utilizzo.
A tal fine, si dovrà implementare uno specifico sistema di autorizzazioni e di verifiche di "conformità" ad elevati *standard* di precisione ed accuratezza, di competenza dell'Autorità sanitaria, con obbligo di monitoraggio e segnalazione di eventi avversi anche a carico di chi li utilizza, compresi gli enti ospedalieri e sanitari in genere, secondo meccanismi già collaudati in altri settori (come ad es. quello della circolazione dei veicoli a guida autonoma, introdotto in Germania), ed in conformità all'approccio regolatorio evincibile dall'*AI Act* per i "*sistemi ad alto rischio*".
La violazione di una siffatta disciplina extrapenale potrebbe quindi essere fonte di responsabilità penale, pur di fronte a comportamenti "imprevisti" dei sistemi in questione, che sono quelli maggiormente temibili, non occorrendo, per l'imputazione a titolo di colpa, che questa sia "cosciente", vale a dire implichi la previsione *concreta* dell'evento causato, che costituisce infatti solo un'eventuale circostanza aggravante propria dei reati colposi (*ex* art. 61, n. 2 c.p.). In generale, è sufficiente la "possibilità di prevedere" vale a dire la c.d. prevedibilità non già del singolo evento concreto che si possa verificare, ma della tipologia di eventi cui esso appartenga e che le misure cautelari hanno per l'appunto la finalità di evitare.
Il modello più adeguato appare, in questo contesto, quello della c.d. colpa specifica, che presuppone la formulazione – in regole scritte di comportamento – di dette misure cautelari, aventi funzione di prevenzione o, quantomeno, riduzione dei rischi ad un livello accettabile (quello del c.d. rischio consentito), tenuto conto dei vantaggi che porta l'impiego dei sistemi AI: regole che possono o anzi debbono essere fornite già dai produttori e manutentori, anche privati, e da coloro che ne dispongono l'utilizzo (c.d. *disployer*, nella terminologia dell'*AI Act*), oltre che dalle Autorità competenti al rilascio delle autorizzazioni al loro uso ed al loro controllo.
Si tratta di una prospettiva che non esclude anche la responsabilità per negligenza ed imprudenza, rispetto a cui non opera l'esonero stabilito dal controverso art. 590 *sexies* c.p., e che pare integrarsi con il modello più generale della c.d. "colpa di organizzazione" basata su un previo *risk assessment*, come delineato dall'*AI Act* per qualsiasi utilizzazione lecita di sistemi AI "*ad alto rischio*".
I fornitori e coloro che dispongono dell'utilizzo di questi sistemi (dunque le stesse strutture sanitarie ed i loro responsabili, prima ancora degli operatori), in ogni ambito in cui agiscono, devono identificare e riconoscere previamente le tipologie ed i livelli dei rischi connessi all'utilizzazione dei sistemi AI nelle specifiche attività in cui vanno impiegati, e devono quindi "organizzare" l'attività in modo tale che siano stabilite ed efficacemente attuate e controllate – con una chiara attribuzione di competenze ed istituzione di appositi organismi interni, che ne garantiscano anche la "*sorveglianza umana*" (cfr. artt. 9 e 14 *AI Act*) – le più adeguate misure cautelari, in funzione specificamente preventiva, necessarie per ridurre e contenere i predetti rischi nell'ambito di quelli accettabili o "consentiti" nel bilanciamento con i vantaggi che offrono.
Su tali basi normative extrapenali, il concreto rimprovero di colpa alla persona umana od all'ente che "stanno

(38) Cfr. *supra*, nota 35.

(39) È stato prospettato ed enfatizzato in dottrina il cambio di paradigmi che comporterebbe il ricorso massivo ai sistemi AI in medicina, in quanto farebbe superare il modello dell'*Evidence-Based Medicine* (incentrata su una metodologia di ricerca scientifica condotta dall'uomo, al quale rimane poi la scelta e responsabilità nel singolo caso clinico), su cui si fondano anche le "Linee Guida", a favore di una *Data-Driven Medicine*, affidata invece agli algoritmi di apprendimento automatico, basata sui *Big Data* e capace addirittura di indicazioni terapeutiche sullo specifico caso clinico, alle quali il medico devolverebbe le decisioni e gli interventi, con conseguente spostamento anche della responsabilità dagli operatori – ridotti a meri esecutori delle indicazioni cogenti dei sistemi algoritmici – alle strutture che li implementano (cfr. Amore, Rossero, *Robotica e intelligenza artificiale nell'attività medica*, cit., 199 s., 215 s.). Pur suggestiva nella prospettiva avveniristica in cui si colloca, la tesi non appare convincente, perché estremizza una contrapposizione che va invece ricondotta ad un'interazione e sinergia fra uomo e macchina, da regolare e garantire anche tramite una chiara e vincolante disciplina giuridica, che si sta in effetti incontrovertibilmente delineando a livello interno e sovranazionale.

dietro" all'utilizzazione di questi sistemi da cui sia derivato un evento avverso, non potrebbe più considerarsi quale inammissibile "colpa per non aver previsto l'imprevedibile", come è stato detto (40), ma per la violazione di quelle cautele, anche organizzative, specificamente finalizzate ad evitare che si verifichino eventi della tipologia di quello realizzatosi: violazioni che quindi, in conformità all'essenza normativa della colpa, assorbono i requisiti della prevedibilità ed evitabilità in concreto da parte dell'agente, in quanto l'evento stesso realizzerebbe proprio lo specifico rischio che le predette norme extrapenali sono dirette a contrastare o ridurre, in conformità al loro scopo cautelare.

E questo non esclude, ma anzi consente che, a fondamento della responsabilità penale per colpa, si debba ravvisare anche quella "rimproverabilità giuridica" *soggettiva*, consistente nella disapprovazione dell'ordinamento per non aver agito diversamente da quanto sarebbe stato possibile e doveroso per la singola persona.

Tali considerazioni assumono una chiara rilevanza pratica, se si considera che questi sistemi AI vengono per lo più impiegati o resi disponibili, anche ai singoli operatori sanitari, da strutture organizzate e complesse, come le aziende ospedaliere od i presidi sanitari del territorio. Nel loro ambito è, quindi, possibile individuare sia le posizioni di garanzia assunte da chi è deputato a controllare le specifiche fonti di rischio, in base alle competenze attribuite, non necessariamente coincidenti con le sole posizioni apicali; sia le eventuali carenze che possano integrare quella "colpa di organizzazione" cui si è fatto riferimento, e che ne può fondare la responsabilità per i fatti colposi che si verifichino, per non aver valutato adeguatamente i rischi, e/o non aver preso le necessarie misure organizzative e cautelari, nonché di monitoraggio ed attenzione ai segnali d'allarme per eventi avversi, che devono essere oggetto di adeguati "modelli organizzativi" (c.d. MOG), cui fa riferimento paradigmatico il d.lgs. 231/2001, che prevede e regola la responsabilità "da reato" delle persone giuridiche e degli enti (41).

### *4.4. Prospettive* de jure condendo

*De jure condito*, il limite di applicazione della disciplina della responsabilità degli enti, correlata all'utilizzo di sistemi AI nel settore in esame, è però duplice.

Innanzitutto, sono ad essa sottratti espressamente gli enti pubblici, salvo che svolgano attività economiche (art. 1, comma 3, d.lgs. 231/2001), e tali non sono considerate le attività sanitarie, che non perseguono fini di lucro. Per cui potrebbe interessare solo le aziende ospedaliere private (42).

In secondo luogo, nell'elenco tassativo dei reati cui si applica la predetta disciplina, non sono inclusi gli omicidi colposi e le lesioni personali colpose, che non siano riferibili a violazione delle regole in materia di salute e sicurezza sui luoghi lavoro (art. 25-*septies* d.lgs. 231/2001). Per cui appare necessario ed urgente un intervento del legislatore, che ponga rimedio a tali carenze di disciplina, ed estenda quantomeno l'elenco degli enti responsabili e dei reati per cui può operare, data la vitale (e crescente) importanza dei sistemi AI in campo sanitario.

Tale intervento novellistico non è invero previsto nel recente schema di disegno di legge governativo in materia di intelligenza artificiale (43), che pur dedica l'art. 7 all' "*Uso dell'intelligenza artificiale in ambito sanitario e di disabilità*" (cfr. *supra*, par. 2.1). Dopo aver sottolineato che l'utilizzo di questi sistemi "*contribuisce al miglioramento del sistema sanitario e alla prevenzione e cura delle malattie, nel rispetto dei diritti, delle libertà e degli interessi della persona, anche in materia di protezione dei dati personali*" (comma 1), la norma richiama al comma 5 il principio antropocentrico, già proclamato all'art. 1, prevedendo che "*I sistemi di intelligenza artificiale nell'ambito sanitario costituiscono un supporto nei processi di prevenzione, diagnosi, cura e scelta terapeutica, lasciando impregiudicata* la decisione, *che* è sempre rimessa alla professione medica" [evidenziazioni aggiunte]. Ne dovrebbe discendere dunque la riaffermazione anche dell'eventuale responsabilità penale "personale", visto altresì che al comma successivo si stabilisce che "*I sistemi di intelligenza artificiale utilizzati nell'ambito sanitario e i relativi dati impiegati devono essere affidabili e periodicamente* verificati e aggiornati *al fine di minimizzare il rischio di errori*" [evidenziazioni aggiunte].

Ma fra le deleghe legislative al Governo previste dall'art. 22, al comma 3 si fa riferimento ad una disciplina soltanto per i "*casi di uso di sistemi di intelligenza* artificiale per finalità illecite", sulla base di criteri direttivi enunciati nel successivo comma 5, in cui contraddittoriamente si prevedono anche "*autonome fattispecie di reato, punite a titolo di dolo o* di colpa, *incentrate sulla omessa adozione o l'omesso adeguamento di misure di sicurezza per la produzione, la messa in circolazione e* l'utilizzo professionale *di sistemi*

(40) Piergallini, *Intelligenza artificiale: da "mezzo" ad "autore" del reato?*, in *Riv. it. dir. proc. pen.*, 2020, 1771 s.

(41) Nella sterminata letteratura in argomento, con specifica attenzione al tema della responsabilità penale connessa all'uso di sistemi AI, si veda Mongillo, *Corporate Criminal Liability for AI-Related Crimes: Possible Legal Techniques and Obstacles*. Special Report in Picotti, Panattoni (eds.) *Traditional Criminal Law Categories and AI: Crisis or Palingenesis?* (international Colloquium Section I, Siracusa, 15-16 September 2022), in *Revue Internationale de Droit Pénal*, Nr. 1, 2023, 77 s., cui si rinvia anche per l'ampia bibliografia, non solo nazionale.

(42) Per un caso di estensione a società non soltanto private, ma a partecipazione mista, si veda però – in sede cautelare – Cass., sez. II, 9-21.7.2010, n. 28699, con nota di Di Giovine, *Sanità ed ambito applicativo della disciplina sulla responsabilità degli enti: alcune riflessioni sui confini tra pubblico e privato*, in *Cass. pen.*, 2011, 1888 s.

(43) Cfr. *supra*, par. 2.1.

*di intelligenza artificiale*" [evidenziazioni aggiunte]: vale a dire reati che si possono anche commettere nell'ambito di un utilizzo per finalità in realtà *lecite*, quali quelle che si svolgono in ambito sanitario, ma che possono cagionare eventi avversi "per colpa". Per cui sarebbe auspicabile una maggior chiarezza e coerenza al riguardo.
Più che un'estensione a nuove fattispecie della sfera di responsabilità penale, od un generalizzato aggravamento di pene, tramite circostanze aggravanti *comuni* (*ex* art. 25, comma 1, lettera a) o *speciali* per singoli delitti peraltro dolosi (*ex* art. 25, comma 1, lettere da b) ad i), ivi compreso l'inserimento di un nuovo delitto doloso di "*Illecita diffusione di contenuti generati o manipolati con sistemi di intelligenza artificiale*" quale art. 612-*quater* c.p. – previsto con duplice formulazione alternativa alla lettera d) – sarebbe auspicabile un'attenta rielaborazione ed integrazione dei criteri di imputazione, anche a titolo di colpa, della responsabilità penale o punitiva nell'ambito delle complesse strutture che dispongono, quali *diployer*, dei sistemi AI e del loro utilizzo, estendendo ed adeguando perimetro di applicazione del d.lgs. 231/2001 all'intero ambito delle attività sanitarie oggetto d'esame.

## 5. Conclusioni: esigenze di tutela penale ed adeguamento delle categorie penalistiche

L'importanza della sanzione penale, compresa quella punitiva per la responsabilità "da reato" dell'ente, che può anche prescindere dalla concreta individuazione della singola persona fisica che nel suo ambito lo abbia realizzato (cfr. art. 8 d.lgs. 231/2001), ha un'essenziale funzione di monito e di guida al comportamento corretto conforme a diritto, e non pare rinunciabile, in coerenza con il criterio guida già richiamato, secondo cui quanto sarebbe penalmente rilevante, se il fatto fosse commesso da una persona umana, non può essere penalmente irrilevante, perché vi è l'intervento di un sistema AI. Infatti, i beni giuridici offesi, compresi i diritti fondamentali che vengono in rilievo, sono già dall'ordinamento vigente considerati meritevoli di siffatta tutela, che non appare "sostituibile" da altra tecnica sanzionatoria, per l'efficacia e l'incisività che la prima presenta, nel necessario giudizio di proporzione fra i beni che la pena sacrifica e quelli che vanno protetti tramite la sua minaccia ed applicazione.
Tanto più che, di fronte ai nuovi impetuosi sviluppi tecnologici ed all'estensione tumultuosa delle relative applicazioni nel campo medico-sanitario, si estenderebbero inaccettabili aree di impunità, che lascerebbero sforniti di adeguata tutela beni ed interessi giuridici, nonché diritti fondamentali, quali la vita, l'integrità personale, la libertà di autodeterminazione in campo sanitario, la *privacy*, la sicurezza cibernetica, la fede pubblica, che già sono oggetto di protezione penale, non solo per il loro rango primario, ma anche per l'inadeguatezza della protezione che – considerando altresì il profilo processuale dei mezzi di indagine ed acquisizione della prova – potrebbe essere offerta da altre tecniche di tutela, come quelle civilistica ed amministrativistica.
È dunque indispensabile un attento e calibrato adeguamento delle categorie penalistiche, sostenuto da un oculato intervento del legislatore, che dovrebbe a monte sopperire alle lacune riscontrabili, integrandosi con la nuova disciplina europea sopra menzionata, in modo che il ricorso allo strumento penale non sia un demagogico sostituto, ma davvero l'*ultima ratio* di una tutela che trovi solido fondamento nella disciplina organica del settore, innovato in modo così dirompente dall'avvento dell'intelligenza artificiale.
E per questo obiettivo la dottrina ed il confronto interdisciplinare possono dare il necessario contributo di analisi critica e di inquadramento sistematico.

# L'illiceità del trattamento per diffusione di dati personali riferiti alla diagnosi di HIV

Corte Europea dei Diritti dell'Uomo; 23 gennaio 2024; Affaire O.G. et Autres c. Grèce (requêtes nos 71555/12 et 48256/13).

*In tema di tutela di riservatezza di informazioni relative al virus dell'HIV, la sottoposizione a un trattamento sanitario in difetto di una libera espressione del consenso dell'assistito e di una completa informazione rilasciata al medesimo, così come invocato dall'art. 8 della CEDU, salvo che non sia prescritto dalla legge, sostanzia un'ingerenza nel diritto del paziente al rispetto della sua vita privata (1).*

*Atteso che i dati relativi alla sieropositività sono per loro natura meritevoli di stringenti meccanismi di protezione, è già illecita la diffusione sul web dei nomi e delle foto di interessate esercenti la professione della prostituzione, ulteriormente aggravata dall'ulteriore disvelazione dell'informazione relativa allo sviluppo dell'infezione da virus dell'immunodeficienza umana (2).*

**La sentenza è presente per esteso sul sito di questa *Rivista* < https://dirittodiinternet.it/>**

## IL COMMENTO

*di Filippo Lorè*

**Sommario:** 1. Il caso di specie e la disciplina rilevante. – 2. Le questioni giuridiche. Illegittimità del prelievo di sangue senza consenso. – 3. Profili di diritto della protezione dei dati personali. – 4. Conclusioni e parallelismi con l'ordinamento italiano.

Il presente contributo prende in esame la condotta posta in essere delle autorità inquirenti greche, le quali, all'esito di importanti operazioni di polizia, ordinavano che i dati identificativi e i rilievi fotografici di talune prostitute, tratte in arresto, venissero diffusi con la correlata notizia riferita alla loro sieropositività, provvedimento che veniva ulteriormente diffuso sui canali istituzionali dell'autorità di polizia. La Corte EDU, esaminato il caso di specie, ha ritenuto, all'unanimità, violato l'articolo 8 della Convenzione europea dei diritti dell'uomo nei confronti delle interessate ricorrenti, atteso che, in assenza di idonee garanzie, le stesse venivano sottoposte, altresì, ad esami ematoclinici, in difetto di idonee informazioni preventive e di una manifestazione positiva di volontà. L'autore, esaminata la decisione, esamina i profili afferenti la protezione dei dati personali e gli elementi di tutela delle libertà fondamentali delle persone fisiche.

*This contribution examines the conduct of the Greek investigating authorities, who, following important police operations, ordered that the identification data and photographic findings of certain prostitutes, arrested, be disseminated with the related news referring to their HIV positivity, a provision which was further disseminated on the institutional channels of the police authority. The ECHR, having examined the case in question, unanimously held that Article 8 of the European Convention on Human Rights had been violated in relation to the appellant interested parties, given that, in the absence of suitable guarantees, they were subjected, also, to haematoclinic tests, in the absence of suitable information and a positive expression of will. The author, having examined the decision, examines the profiles relating to the protection of personal data and the elements of protection of the fundamental freedoms of natural persons.*

### 1. Il caso di specie e la disciplina rilevante

Ai fini di una migliore comprensione della pronuncia della Corte Europea dei Diritti Umani (di seguito semplicemente "Corte" e "CEDU") è opportuno ripercorrere le tappe salienti del contenzioso *de quo*. I ricorsi riguardano la decisione, delle autorità greche, riguardante, da un lato, la diffusione di dati relativi alla salute delle ricorrenti, vale a dire di certune prostitute sieropositive (tranne una che non lo era) e, d'altro canto, l'imposizione, alle medesime, di un trattamento sanitario. Il 30 aprile 2012, infatti, nell'ambito di un'operazione di polizia, effettuata nel centro di Atene, venivano dichiarate in stato di fermo novantasei individui, comprese le ricorrenti, le quali, sospettate di aver commesso il reato previsto dall'art. 5 della L. n. 2734/1999, ovvero l'esercizio della prostituzione senza il permesso e in assenza

dell'apposito libretto sanitario, alla richiesta degli agenti di attestare la loro identità, riferivano di non disporre di documenti di riconoscimento. A seguito di visita medica sostenuta e sottoposte al *test* rapido, utile a misurare la presenza di anticorpi del virus HIV, sarebbe emerso che undici delle interessate, arrestate, risultavano positive. Le ricorrenti, in merito, riferivano che tali esami medici venivano compiuti in difetto di idonea e preventiva informazione, in più in carenza di una manifestazione positiva di volontà. In appresso, il pubblico ministero presso il Tribunale di Atene disponeva l'avvio di un procedimento penale contro le ricorrenti per il reato tentato di lesioni personali gravi e per la pratica della prostituzione, intrapresa senza autorizzazione ufficiale, il tutto in assenza di una licenza utile a gestire una casa di appuntamenti e, ancora più, del possesso di una cartella clinica speciale. Contestualmente, il pubblico ministero, muovendo dalle disposizioni di cui agli artt. 2, lettere a) e b), e 3 § 2, lettera b), della normativa greca sulla tutela delle persone fisiche in relazione al trattamento dei dati personali, L. 10 novembre 1997, n. 2472, aveva, inoltre, disposto, con l'ordinanza n. 23/2012, la divulgazione delle foto e dei dati identificativi delle ricorrenti, accompagnata dal motivo per il quale era stato avviato un procedimento penale contro le stesse e, ancora, dall'indicazione del loro *status* di sieropositive. L'ordine, invero, veniva caricato sul sito *web* dell'autorità di polizia e, successivamente, diffuso attraverso i *media*, comportando, tale azione, una rilevantissima disvelazione dei dati personali delle ricorrenti e una inevitabile copertura mediatica. Successivamente, il 4 maggio 2012 le ricorrenti avanzavano istanza di revoca della predetta ordinanza al direttore della Procura presso il Tribunale penale di Atene, ritenendo che la divulgazione di dati personali, "sensibilissimi", fosse contraria agli artt. 2, 5, 9, 9 A e 25 della Costituzione e agli artt. 3 e 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, dunque sproporzionata rispetto allo scopo perseguito. Orbene, a parere delle ricorrenti, che versavano in stato di detenzione, tale domanda veniva respinta senza una formale e motivata decisione. In seguito, il procedimento relativo ad alcune ricorrenti, a causa del loro decesso, veniva dichiarato concluso, diversamente, altre interessate venivano assolte e, l'ordinanza n. 23/2012, oggetto di abrogazione. Con riferimento ai profili penalistici relativi alla circostanza che l'esame del sangue era stato eseguito senza consenso e che, comunque, in alcuni casi, non poteva essere effettuato, poiché alcune interessate presentavano sintomi di patologie gravi, le autorità greche ricavavano che la base giuridica per l'intervento dei medici fosse rinvenibile nell'ordinanza n. 39A /2012 del ministro della Sanità (la quale prevede il test dell'HIV sui tossicodipendenti e sulle prostitute per rispondere alle esigenza di salute pubblica e della propria salute individuale). Di conseguenza, alla luce delle argomentazioni addotte, la denuncia presentata contro i suddetti agenti di polizia e avverso il personale medico coinvolto, per attentato alla dignità umana, violenza illegale e violazione dei doveri, non trovava accoglimento. In ordine, invece, ai profili attinenti alla protezione dei dati personali, il 9 agosto 2012 talune delle imputate arrestate, lamentando la diffusione dei propri rilievi fotografici sulle principali testate giornalistiche, presentavano ricorso dinanzi all'autorità di controllo nazionale, che, tuttavia, procedeva all'archiviazione del caso, senza alcuna possibilità di esaminare il ricorso, sulla base dell'accertamento di incompetenza, già formulato, nei suoi confronti, con la decisione n. 128/2012. In linea continua con le modalità appena rappresentate, il 5 maggio 2012 venivano effettuati pattugliamenti simili a quelli avvenuti il 30 aprile 2012 e, al termine dell'operazione, gli agenti di polizia conducevano diciannove interessate alla direzione degli stranieri dell'Attica (nel convincimento che fossero prostitute) e sottoponevano, le stesse, a visita medica ai fini dello *screening* dell'HIV, all'esito della quale veniva accertata la positività di talune di esse, che, pertanto, venivano tratte in arresto. Le medesime, in seguito, riferivano di essersi sottoposte agli esami del sangue in difetto di una manifestazione libera di volontà, in assenza di un idoneo chiarimento circa le procedure avviate dall'autorità di polizia e, ad ogni modo, negando di tenere legami con il fenomeno della prostituzione, tanto meno di essere a conoscenza di aver contratto l'infezione da *virus* dell'immunodeficienza umana. Con l'ordinanza n. 27/2012 del 5 maggio 2012, il pubblico ministero, similmente all'ordinanza summenzionata, disponeva la pubblicazione delle fotografie delle ricorrenti accompagnate dai dati identificativi, nonché il presupposto legittimante il procedimento penale contro le stesse e la notizia relativa alla loro sieropositività. Sicché, l'11 maggio 2012 le ricorrenti venivano trasferite nel carcere di Korydallos, mentre il 20 luglio 2012, con decisione n. 2749/2012, la sezione d'accusa del Tribunale penale di Atene rinviava a giudizio le ricorrenti. La Corte d'Assise di Atene assolveva le ricorrenti, con sentenza n° 8 del 7 gennaio 2013, assunto che non si evinceva, sotto il profilo probatorio, che le interessate fossero prostitute e che avessero deciso, scientemente, di infliggere gravi lesioni personali a terzi. Gli eventi di cui si è dato conto possono essere inquadrati, in punto di diritto, nel dettato dell'art. 8 della CEDU, secondo cui, "ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza", e "non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria

alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui". Tali assiomi sembrano essere messi in pericolo, nella vicenda che ha portato all'approdo in commento, da un lato, con riguardo agli esami clinici comandati alle meretrici, quale interferenza non prevista dalla legislazione, e, d'altro canto, dalla decisione del pubblico ministero di rendere pubblici, mediante i *media*, i dati sanitari delle interessate sieropositive, per di più associati ai dati identificativi delle stesse e al motivo del procedimento penale avviato nei loro confronti. Senza poter qui affrontare, per ragioni di spazio, l'evoluzione del quadro giuridico-normativo penale e civile, europeo e greco, in materia di sanità (per i temi che afferiscono alla prostituzione, alla tossicodipendenza e all'HIV), né operare considerazioni sulle norme rilevanti in merito alla ricevibilità del ricorso, ci si soffermerà in particolare sui profili riguardanti la tutela dei dati personali (1). Prima di fare questo, è opportuno, tuttavia, accennare che, nella sentenza in commento, la Corte ha dato conto di una serie di normative su cui ha basato la propria decisione. Anzitutto la Corte si rifà al caso Mitkus c. Lettonia, n. 7259 /03, §§ 59 e 60, del 2 ottobre 2012. Viene in evidenza, ovviamente, anche la disciplina della Convenzione di Oviedo sulla biomedicina, in vigore in Grecia dal 1° dicembre 1999. In particolare, la suddetta Convenzione introduce la "Regola generale" secondo la quale "un intervento nel campo della salute non può essere effettuato se non dopo che la persona interessata abbia dato consenso libero e informato" e senza che la stessa abbia ricevuto "una informazione adeguata sullo scopo e sulla natura dell'intervento e sulle sue conseguenze e i suoi rischi" (2). Emblematica, per il caso *de quo*, risulta essere anche la disposizione seguente che, riservando protezione alle persone fisiche, stabilisce il divieto di attuare un intervento sanitario su di un interessato che non ha capacità di manifestare il consenso, se non per un diretto beneficio dello stesso (3). Per quanto attiene, invece, alle patologie connesse all'HIV, in una Raccomandazione dell'Assemblea Parlamentare del Consiglio d'Europa ("PACE"), si rimarca la stringente esigenza di "adottare tutte le misure atte a garantire il rispetto della riservatezza e/o l'anonimato delle persone che vivono con l'HIV o l'AIDS" (4). Ancor più pregnante, per la sentenza in commento, appare quanto statuito in ulteriore Raccomandazione della PACE, laddove si cristallizza che "[i] test HIV, compresi i test prenatali, devono essere riservati, richiedono il consenso informato e devono essere accompagnati da consigli e informazioni sulle opzioni terapeutiche" (5). Da ultimo, la Corte ha sollevato la rilevanza, per il caso di specie, della normativa europea in materia di protezione dei dati personali, in particolare della Direttiva 95/46/CE (6), in vigore all'epoca dei fatti, nonché del Regolamento UE 2016/679, noto ai più come *General Data Protection Regulation ("GDPR")* (7), direttamente applicabile negli Stati membri dal 25 maggio 2018, che ha provveduto a innovare la disciplina, abrogando la medesima Direttiva (8). I profili inerenti gli obblighi dettati dal GDPR verranno trattati nel prosieguo della presente nota a sentenza. Senonché, decisiva, nel caso oggetto di commento, risulta la disciplina tratteggiata dalla CEDU, laddove prescrive che «[n]on può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute e della morale, o alla protezione dei diritti e delle libertà altrui" (9).

(1) D'Orazio, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in *I dati personali nel diritto europeo*, a cura di Cuffaro - D'Orazio et al., Torino, 2019, 61 ss.

(2) Consiglio d'Europa, Convenzione per la protezione dei Diritti dell'Uomo e della dignità dell'essere umano nei confronti dell'applicazioni della biologia e della medicina: Convenzione sui Diritti dell'Uomo e la biomedicina, 4 aprile 1997, articolo 5.

(3) Consiglio d'Europa, Convenzione per la protezione dei Diritti dell'Uomo e della dignità dell'essere umano nei confronti dell'applicazioni della biologia e della medicina: Convenzione sui Diritti dell'Uomo e la biomedicina, 4 aprile 1997, articolo 6.

(4) Assemblea Parlamentare del Consiglio d'Europa ("PACE"), Raccomandazione 1116 (1989) sull'AIDS e i diritti umani, punto 8.4.1.

(5) Assemblea Parlamentare del Consiglio d'Europa ("PACE"), Raccomandazione 1785 (2007) sulla diffusione dell'HIV/AIDS tra le donne e le ragazze in Europa, punto 6.

(6) Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché sulla libera circolazione di tali dati.

(7) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, sul carattere personale e sulla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), di seguito "GDPR".

(8) D'Orazio - Finocchiaro et al., *Codice della privacy e data protection*, Milano, 2021; Bifulco - D'Acquisto, *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, 2021; Locoratolo, *Il trattamento dei dati personali e la Privacy*, Bari, 2021; Resta, *Il Codice della Privacy. Commento al D.Lgs. n. 30 giugno 2003, n. 196 e al D.Lgs 10 agosto 2018, n. 101 alla luce del Regolamento (UE) 2016/679 (GDPR)*, Pisa, 2019, 243 ss.

(9) Art. 8, Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

## 2. Le questioni giuridiche. Illegittimità del prelievo di sangue senza consenso

Come riferito, le ricorrenti lamentavano come la mancata raccolta del consenso all'esame ematoclinico, prima che questo venisse effettuato, integrasse la violazione della CEDU, non soltanto nella disposizione di cui all'art. 8, bensì all'art. 3, nella parte in cui si definisce che "nessuno può essere sottoposto a tortura né a pene o trattamenti inumani o degradanti", mentre la Corte riteneva non perfezionata tale ultima violazione. Come accennato, dall'analisi delle memorie difensive prodotte, le interessate, i cui diritti erano stati oggetto di violazione, sostenevano, anzitutto, che l'HIV non rientrava tra i *virus* per i quali la legge greca fissava la visita medica obbligatoria e, pertanto, l'imposizione di un trattamento sanitario può trovare applicazione solamente in adesione a una disposizione normativa, non certo in forza di un decreto ministeriale, che, nel caso di specie, avrebbe "abusato" dell'autorizzazione legislativa del Parlamento, senza alcuna giustificazione scientifica, trasgredendo i principi della Costituzione. Inoltre, l'intervento medico sarebbe avvenuto, oltre che senza la raccolta del consenso, "in assenza di qualsiasi riservatezza, assistenza medica e psicologica" e in difetto di annotazione degli eventi nel registro delle prestazioni sanitarie. Ancora, le ricorrenti attestavano l'assoluta illegittimità della divulgazione dei dati sanitari, a cura delle figure professionali coinvolte (10). Di contro, il Governo greco confutava tali affermazioni, avanzando motivate significazioni, mediante le quali sunteggiava che per le esercenti la professione richiamata corre l'obbligo di sottoporsi ad accertamenti medici e, invero, che l'esame del sangue era stato compiuto contro la volontà delle interessate, poiché finalizzato alla valutazione sia del loro stato di salute, sia degli eventuali danni eventualmente arrecati a terzi (11). La Corte, in merito, ha riscontrato, nella decisione in esame, che un trattamento sanitario in carenza di una libera espressione del consenso dell'assistito e di una completa informazione rilasciata al medesimo, così come invocato dall'art. 8 della CEDU, sostanzia un'ingerenza nel diritto del paziente al rispetto della sua vita privata (12), salvo che non sia "prescritto dalla legge", come perseguimento di uno o più scopi legittimi, e, come tale, necessario "in una società democratica" per raggiungere le finalità perseguite (13). In particolare, la Corte richiama la propria costante giurisprudenza secondo cui la locuzione "previsto dalla legge" deve essere intesa nel senso che "il provvedimento impugnato deve avere fondamento in diritto interno ed essere compatibile con lo Stato di diritto, espressamente menzionato nel preambolo della Convenzione e inerente all'oggetto e allo scopo dell'articolo 8". In altre parole, la norma di legge deve essere accessibile e prevedibile, vale a dire enunciata con sufficiente precisione, così da consentire all'individuo di regolare la propria condotta. La medesima disposizione deve, dunque, prevedere "un'adeguata tutela contro l'arbitrarietà e, conseguentemente, definire con sufficiente chiarezza la portata e le modalità di esercizio del potere conferito alle autorità competenti" (14). Pertanto, l'applicazione di tali principi al caso *de quo*, ha portato la Corte a ritenere, correttamente, violato l'art. 8 della CEDU. La tesi avanzata dal Governo delineava come l'intervento medico vantasse molteplici condizioni di liceità, vale a dire, in primo luogo, la L. n. 2734 /1999, la cui funzione è quella di segnare gli obblighi delle persone autorizzate a esercitare la prostituzione, tra cui il vincolo a sostenere cicliche visite mediche (ogni due settimane per lo *screening* di alcune malattie, compresa l'HIV). In secondo luogo, espresso risultava il rimando alle decisioni n. 660 e 661 del Ministro della Salute, dalla cui lettura se ne deduce che le meretrici debbano sottoporsi a esami di *screening* (per l'HIV) ogni tre mesi e che, nel caso in cui si accerti l'infezione da virus dell'immunodeficienza umana, non possano più esercitare la professione, così come il richiamo all'art. 1 § 4 dell'ordinanza n. 39A/2012 del Ministro della Salute. Tuttavia, la Corte ha statuito che l'articolo 1, comma 2, del citato decreto ministeriale, enumera molteplici patologie considerate potenzialmente pericolose per la salute pubblica, come l'influenza pandemica o la SARS, mentre, tra queste, non figura l'HIV. Senonché, il comma 4 del medesimo articolo prevede che sia previsto uno specifico monitoraggio per il test HIV sulle interessate che esercitano la prostituzione, senza la necessaria autorizzazione (15). Più in generale, giova ricordare che, sebbene tutte le disposizioni giuridiche menzionate dal Governo riguardino l'obbligo per le interessate legate al fenomeno della prostituzione di sottoporsi a test di *screening* per la rispondenza di patologie, compresa l'HIV, nessuna di esse fotografa, in maniera puntuale, quali siano i protocolli da seguire, né tanto meno contempla le modalità operative dei controlli (con o senza il consenso informato delle persone interessate) effettuati

(10) Sentenza in commento, punto 107.

(11) Sentenza in commento, punto 108.

(12) Sentenza in commento, punto 109.

(13) Sentenza in commento, punto 110, in cui si rinvia a Corte Europea dei Diritti dell'Uomo, sentenza 27 giugno 2013, V sez., 7841/08, Vassis e altri c. Francia.

(14) Sentenza in commento, punto 111, in cui si rinvia a Corte Europea dei Diritti dell'Uomo, sentenza 2 agosto 1984, II sez., § § 66-68, Serie A n° 82, sentenza 4 maggio 2000, Grande Camera, 28341/95, § 55, Rotaru c. Romania, e sentenza 16 febbraio 2000, Grande Camera, 27798/95, Amann c. Svizzera, § 56.

(15) Sentenza in commento, punto 116.

dagli organi di polizia o dalle autorità giudiziarie. Per quanto attiene, invece, alle disposizioni del Codice di procedura penale greco, la Corte ha rilevato che esse postulano un ordine del pubblico ministero, affinché il giudice istruttore o gli agenti di polizia possano compiere atti investigativi, e soltanto in caso di pericolo immediato, fattispecie che, evidentemente, il Governo non ha in alcun modo invocato e che, ad ogni modo, non ha trovato applicazione nel caso in commento (16). Né si può ritenere sussistente la stringente esigenza di dover ottenere elementi di prova, in fase di indagine preliminare, della partecipazione delle ricorrenti a un reato, nel caso di specie, attesa la mancanza di un'ordinanza che autorizzasse il prelievo di sangue, a favore della polizia e del personale medico del Centro di controllo e di prevenzione delle malattie (KEELPNO), e accertata, altresì, che non è stata applicata una specifica procedura per i trattamenti sanitari avvenuti nei locali della polizia (17) (come invece era avvenuto, ricorda la Corte, in altri casi simili sottoposti al Suo vaglio (18)). In conclusione, la Corte ha ritenuto che l'ingerenza nel diritto delle ricorrenti al rispetto della loro vita privata non fosse configurabile, nel caso concreto, come "prevista dalla legge", circostanza sufficiente per esonerare lo stesso Organo dall'esaminare se l'atto costitutivo della suddetta ingerenza perseguisse uno "scopo legittimo" e se fosse "necessario in una società democratica" (19). Volendo esercitare un parallelismo con la normativa vigente in Italia, è opportuno segnalare come le argomentazioni addotte dalla Corte trovano soddisfazione in molteplici arresti della Corte di Cassazione, dai cui orientamenti viene riconosciuto come l'art. 5, comma 3, L. 5 giugno 1990 n. 135 – secondo cui "nessuno può essere sottoposto al test anti HIV senza il suo consenso, se non per motivi di necessità clinica, nel suo interesse" – deve essere interpretato alla luce dell'art. 32, comma 2, della Costituzione, nel senso che, anche nei casi di necessità clinica, l'assistito deve essere informato del trattamento a cui lo si vuole sottoporre e, allo stesso tempo, l'interessato conserva il diritto di conferire o diniegare il consenso, in tutti i casi in cui sia in grado di autodeterminarsi, salvo i casi di "obiettiva e indifferibile urgenza del trattamento sanitario, o per specifiche esigenze di interesse pubblico (rischi di contagio per i terzi, od altro): circostanze che il giudice deve indicare nella motivazione" (20). In altre parole, verrebbe vanificato il diritto del paziente di accettare o rifiutare le cure se, alla personale valutazione dell'interessato sulla necessità di essere sottoposto al test HIV, si sostituisse quella del personale sanitario.

## 3. Profili di diritto della protezione dei dati personali

L'art. 8 della CEDU è finalizzato fondamentalmente a difendere la persona fisica dalle arbitrarie ingerenze del pubblico potere nella sua "vita privata", concetto che include anche le informazioni personali che un individuo può legittimamente aspettarsi non vengano pubblicate senza il suo consenso (21). I profili dell'identità di un individuo attengono, infatti, oltre che al nome, agli elementi che si riferiscono al diritto all'immagine (22). In riferimento agli aspetti più prettamente legati alla tutela della riservatezza, nel caso in commento, per la diffusione dei dati personali dei ricorrenti, condotta posta in essere a seguito delle ordinanze adottate dal pubblico ministero, la Corte ha contestato la violazione dell'art. 8 della CEDU, nella parte relativa al secondo paragrafo di tale disposizione, laddove stabilisce che "non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla dife-

(16) Sentenza in commento, punto 118.

(17) Sentenza in commento, punto 119.

(18) Corte Europea dei Diritti dell'Uomo, sentenza 18 luglio 2023, n. 44033/17, Manole c. Modavia, § 52; Corte Europea dei Diritti dell'Uomo, sentenza 9 luglio 1985, n. 10670/83, Schmidt c. Austria, § 33, in cui gli interventi medici contestati erano stati disposti sulla base di un articolo del codice penale e seguendo la procedura ivi descritta, vale a dire a seguito di un ordine adottato rispettivamente da un pubblico ministero, da un giudice e da un tribunale. Nel caso di specie, nessuna delle disposizioni citate dal Governo era idonea a giustificare un intervento medico effettuato da agenti di polizia o da medici della KEELPNO come quello effettuato nei confronti dei ricorrenti; Corte Europea dei Diritti dell'Uomo, sentenza 7 ottobre 2008, 35228/03, Vallauri c. Italia, in *Riv. it. dir. proc. pen.*, 2009, 325, nella quale la Corte ha affermato che non integra una violazione dell'art. 8, CEDU, il trattamento medico effettuato senza consenso, laddove lo stesso sia dettato esclusivamente da esigenze terapeutiche. Nel caso di specie il ricorrente era stato fermato all'aeroporto di Lisbona dall'autorità dogale e trovato in possesso di numerosi sacchetti di cocaina. Una volta arrestato, aveva confessato agli agenti di aver ingerito uno dei sacchetti: dato che, a sessantadue ore dall'ingestione, l'uomo non era ancora riuscito a espellere naturalmente il sacchetto, i medici decidevano di estrarlo chirurgicamente per impedire che la sostanza in esso contenuta fosse assorbita dall'organismo. La Corte, pur riconoscendo che qualsiasi trattamento medico praticato senza il consenso dell'interessato costituisce un'interferenza nel diritto all'integrità fisica e morale della persona, ha ritenuto giustificata tale interferenza perché il trattamento nel caso di specie era stato eseguito al fine esclusivo di tutelare la salute del paziente e nel rispetto delle regole dell'*ars* medica, così da porre nel giusto equilibrio l'interesse pubblico alla tutela della salute, da un lato, e il diritto all'integrità fisica e morale della persona, dall'altro.

(19) Sentenza in commento, punti 120-122.

(20) Cass., 14 novembre 2008, n. 2468.

(21) Corte Europea dei Diritti dell'Uomo, sentenza 6 aprile 2010, IV sez., Causa 25576/04, CGIL e Cofferati c. Italia, §75.

(22) Corte Europea dei Diritti dell'Uomo, sentenza 5 dicembre 2013, V sez., Causa 32265/10, Henry Kismoun c. Francia.

sa dell'ordine e alla prevenzione dei reati, alla protezione della salute e della morale, o alla protezione dei diritti e delle libertà altrui" (23). Invero, secondo il medesimo Organo, se è vero che l'ingerenza in questione si può ritenere come "prevista dalla legge" – poiché la misura impugnata trova la sua base giuridica negli artt. 2, lettere a) e b) e 3 § 2, lettera b) della L. n. 2472/1997 – e che l'esecuzione è conforme al diritto interno, ovvero finalizzata a "proteggere i diritti e le libertà altrui", vieppiù "idonea a contribuire alla scoperta di atti simili commessi dagli imputati a danno dei loro clienti, nonché mirata a garantire la sottoposizione al test di *screening* per l'HIV" (24), tuttavia, i giudici di Strasburgo hanno ritenuto sussistente il *vulnus*, all'art. 8 CEDU, sotto il profilo della «necessità, in una società democratica» della divulgazione dell'identità e delle fotografie delle ricorrenti, rispetto agli interessi citati nella disposizione violata. Ciò, sulla scia della decisione assunta nella causa *Margari (25),* caso simile (ma non identico) e comunque meno grave, atteso che i dati relativi alla sieropositività sono "per loro natura estremamente sensibili" e che, in merito al caricamento sul *web* dei nomi e delle foto delle ricorrenti, insieme alla patologia, "misure di questo tipo adottate senza il consenso dell'interessato richiedono l'esame più rigoroso da parte della Corte" (26). Il pubblico ministero, in sostanza, aveva ordinato la pubblicazione senza averne valutato gli effetti sui diritti fondamentali degli interessati e, al contempo, non aveva ulteriormente ponderato se, per raggiungere lo scopo perseguito, potesse essere opportuno diffondere un diverso annuncio generale, che menzionasse, più semplicemente, la notizia dell'arresto di prostitute sieropositive. Inoltre, non è stato preso in considerazione il fatto che una eventuale opposizione delle ricorrenti, necessariamente successiva alla pubblicazione dei loro dati personali, non avrebbe potuto far ritornare la situazione al punto in cui era *ex ante*, rimediando alla loro identificazione, con "conseguenze devastanti sulla loro vita privata e familiare nonché sulla loro situazione sociale e professionale, potendo mettere in luce il disprezzo e il rischio di esclusione" (27). Tali rilevantissime considerazioni, per la Corte, sono state ritenute adeguate per concludere, all'unanimità, che "l'ingerenza nel diritto dei ricorrenti designati ai numeri 1, 2, 6 e 7 del ricorso n. 71555/12 al rispetto della loro vita privata causato dall'ordine del pubblico ministero non era sufficientemente giustificata nelle particolari circostanze del caso ed era sproporzionata rispetto agli scopi legittimi perseguiti" (28), con la conseguente violazione dell'art. 8 della CEDU e la condanna, per lo Stato greco, al risarcimento delle ricorrenti per il danno morale subito (29). È opportuno segnalare che in tema di riservatezza di informazioni relative al *virus* dell'HIV, la Corte era in passato intervenuta più volte, ribadendo come la divulgazione di un tale patrimonio informativo comporti conseguenze devastanti per la vita privata e familiare, nonché per la sfera sociale e professionale degli interessati, esponendoli allo stigma e al rischio di esclusione dalle dinamiche relazionali di una comunità, con l'ulteriore effetto che il *right to confidentiality* di tali informazioni risulta essere il metro tramite il quale stimare se l'ingerenza sia stata proporzionata rispetto al legittimo fine perseguito. Tale ingerenza, per essere compatibile con l'art. 8 della CEDU, deve essere giustificata da un'imperativa esigenza di interesse pubblico, dall'interesse del ricorrente stesso, o, ancora, dall'interesse della sicurezza del personale ospedaliero (30). Come accennato in precedenza, emergono, altresì, profili di violazione anche della normativa europea in materia di protezione dei dati personali, di cui al citato GDPR, sebbene tale disciplina sia divenuta applicabile negli Stati membri soltanto nel 2018, dunque, alcuni anni dopo i fatti contestati dalla CEDU, nella sentenza in commento. Sono rilevanti, difatti, alcuni Considerando alla medesima disciplina euronitaria, ove, da un lato, con riferimento alla definizione di dati genetici, il legislatore europeo puntualizza che in essa vanno ricompresi i dati "che risultino dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti" (31), e, d'altro canto, in merito alla liceità di un trattamento di dati personali, sebbene possa con-

(23) Art. 8, c. 2, CEDU.

(24) Sentenza in commento, punti 148-149.

(25) Corte Europea dei Diritti dell'Uomo, sentenza 20 giugno 2023, I sez., Causa 36705/16, Margari c. Grecia, §§ 46-49 e 56.

(26) Sentenza in commento, punti 150-154.

(27) Sentenza in commento, punti 155-157.

(28) Sentenza in commento, punti 158-159.

(29) Con riferimento al danno *"da illecito trattamento dei dati personali"*, si rinvia a Crescentini, *Risarcimento del danno non patrimoniale da illecito trattamento dei dati personali. Spunti di dibattito alla luce del GDPR*, in questa ***Rivista***, 2022, 665; Avitabile, *Il risarcimento del danno a seguito dell'illecito trattamento di dati personali: un nuovo impulso dal Reg. UE 27 aprile 2016 n. 679? Corte di Cassazione; sezione VI civile; ordinanza 20 agosto 2020, n. 17383*, in questa ***Rivista***, 2020, 619; Russo, CGUE, *Danno morale e data breach: il timore da utilizzo illecito dei dati personali. Corte di giustizia dell'Unione europea; sentenza 14 dicembre 2023, n. c-340/2021*, in questa ***Rivista***, 2024, 49.

(30) Corte Europea dei Diritti dell'Uomo, sentenza 25 febbraio 1997, Grande Camera, n. 22009/93, sentenza 6 ottobre 2009, III Sez., n. 1425/06, sentenza 19 marzo 2015, II sez., n. 648/10.

(31) Considerando n. 35, GDPR.

siderarsi, quale idonea condizione un atto legislativo come base per svolgere più operazioni conformemente a un obbligo legale cui è soggetto il titolare del trattamento (o se il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri), nondimeno, il legislatore europeo ha disposto che tale atto legislativo potrebbe assicurare la previsione dei "soggetti cui possono essere comunicati i dati personali, le limitazioni della finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto" (32). Come è noto, il GDPR dedica alla liceità del trattamento dei dati personali l'articolo 6, elencando in esso sei motivi che possono essere posti quali basi giuridiche. Orbene, la disciplina europea riserva condizioni di maggior tutela nei casi in cui i dati trattati siano più – per utilizzare il linguaggio del nostro vecchio Codice privacy (33) – "sensibili", ossia meritevoli di maggiore protezione. A sancire, infatti, la logica da seguire nei trattamenti di dati personali relativi alla salute è l'art. 9 del GDPR, laddove è posto un generale divieto di trattare "dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" (34). Chiaramente, tale divieto cede in presenza di alcune condizioni, elencate nel secondo paragrafo della medesima disposizione, tra cui, in particolare, rilevano, per la sentenza in commento, la lettera a) ("l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche") e la lettera g) ("il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato") (35). Rivolgendo lo sguardo all'ordinamento italiano, la norma di riferimento è rappresentata dall'art. 5, comma 1, della L. n. 135/1990, laddove prescrive che è onere del personale sanitario dimostrare di avere adottato tutte le misure occorrenti per assicurare il diritto alla riservatezza dell'assistito e, contestualmente, ogni tecnica utile a ridurre il rischio che (all'esito del *test*) i dati relativi alle condizioni di salute dell'interessato possano addivenire nella disponibilità di terzi (36). Ben si combina, tale disposizione, con il principio generale di *accountability* che il legislatore europeo ha codificato nell'art. 24 del GDPR, ove impone al titolare del trattamento dei dati personali, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, di mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente alla normativa rilevante in materia di protezione dati (37). La dottrina, al tal proposito, ricava come l'accertamento *contra voluntatem* della sieropositività possa essere correlato alla compressione del "*right to privacy*" del paziente e alla violazione sia del rapporto empatico medico-paziente, sia del segreto professionale, integrando la fattispecie a memoria dell'art. 622 del codice penale (38). Ma vi è di più, la medesima dottrina, nel commentare la sentenza degli Ermellini – scaturita dall'inaccortezza di un medico che aveva lasciato incustodita la cartella contenente i risultati del trattamento diagnostico sostenuto dal paziente, facendo sì che la madre venisse a conoscenza della sieropositività del figlio – ha riconosciuto come la circostanza che l'assistito abbia espresso il suo consenso al compimento del test HIV non elide "l'antigiuridicità" della condotta di rivelazione dell'esito dell'esame anche a terzi (39).

## 4. Conclusioni e parallelismi con l'ordinamento italiano

A parere di chi scrive, la sentenza in commento opera un giusto bilanciamento degli interessi delle parti, in

(32) Considerando n. 45, GDPR. Cfr. anche Shabani - Marelli, *Re-identifiability of genomic data and the GDPR: Assessing the reidentifiability of genomic data in light of the EU General Data Protection Regulation*, in *Embo Reports*, 2019.

(33) Decreto legislativo 30 giugno 2003, n.196, recante il "Codice in materia di protezione dei dati personali".

(34) Saari, *GDPR Data Categorisation: Article 9 Special Category Data*, in *Helda University of Helsinki Open Repository*, 2021.

(35) Art. 9, par. 2, GDPR.

(36) Cass., 14 novembre 2008, n. 2468, cit. Per il tema della privacy in sanità cfr. Colangelo, *App mediche e protezione dei dati personali. Alcuni spunti giuridici tra Gdpr, codice privacy novellato e chiarimenti del Garante*, in *Autonomie locali e servizi sociali*, 2019, 275 ss.; Corso - Thiene, *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, Napoli, 2023.

(37) Faillace, *La natura e la disciplina delle obbligazioni di cui all'art. 25 del GDPR espressione dei principi di privacy by design e di privacy by default*, in *Contratto e impresa*, 2022, 1123 ss.; Borrillo, *La tutela della "privacy" e le nuove tecnologie: il principio di "accountability" e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*, in *dirittifondamentali.it*, 2020, 326 ss.; Celella, *Il principio di responsabilizzazione: la novità del GDPR*, in *Ciberspazio e Diritto*, 2018, 211 ss.

(38) Passalacqua, *Il rispetto del consenso informato nell'accertamento della Sieropositività. Note a Sentenza Cassazione Civile, sezione III, 14.11.2008 - 30.01.2009 n. 2468*, in *Diritto.it*, 2010.

(39) Passalacqua, op. cit.

relazione alle condotte poste in essere dall'apparato governativo greco. È importante rilevare, tuttavia, come, nell'ordinamento italiano, la tutela per i pazienti positivi all'HIV è prevista fin dal 1990. Si è fatto cenno alla volontà, del legislatore europeo, di configurare, nel GDPR, una tutela rafforzata per i dati genetici (nel caso di specie, i risultati del test per l'HIV), nonché per i dati relativi alla salute degli interessati, come risulta essere la notizia della positività a tale test. In tal senso, appare opportuno ricordare che il Garante per la protezione dei dati personali, autorità di controllo che vigila sulla corretta applicazione della disciplina rilevante in Italia (40), si era occupata, nel 1999, di un caso molto simile a quello della sentenza in commento. Sugli organi di informazione, infatti, erano apparsi fotografie e generalità di una prostituta affetta dal virus dell'HIV, informazioni comunicate ai *media* dalla polizia giudiziaria. L'Autorità aveva rimarcato la necessità, nell'informare le persone che avevano intrattenuto con la prostituta dei rapporti a rischio, di mettere in atto "procedure più selettive, basate, ad esempio, sulla notizia della sieropositività di una persona che pratichi abitualmente la prostituzione in una determinata zona, accompagnata dall'istituzione di un servizio di informazione ed assistenza (es.: un numero verde) cui gli interessati potessero rivolgersi" (41), affinché l'attività di raccolta, utilizzazione e divulgazione dei dati avvenisse con modalità tali da non recare agli interessati un pregiudizio ingiustificato rispetto alle finalità perseguite, nel rispetto "dei principi di pertinenza e non eccedenza nel trattamento dei dati personali sanciti dall'art. 9 della legge n. 675/1996". In realtà, il Garante italiano aveva iniziato molti anni orsono a occuparsi della questione inerente la tutela della riservatezza dei dati relativi all'HIV. Non ci si può esimere, in merito, dal citare Stefano Rodotà, il quale aveva pubblicato degli scritti in materia ben prima dell'istituzione dell'Authority *de qua*, affermando, più volte, che riservatezza e rispetto della dignità del paziente sono sempre dei fattori centrali nel rispetto della privacy, pertanto, quando si trattano informazioni delicate come quelle correlate all'infezione da HIV, il trattamento dev'essere ancora più accurato rispetto a quanto prescritto per i dati "sensibili", perché dalla loro circolazione può derivare un gravissimo pregiudizio per la vita privata e la dignità personale degli interessati. Nella proposta di legge presentata dallo stesso Rodotà, nel 1987, per la "riservatezza delle persone affette da HIV" (42), la garanzia di anonimato dei pazienti e la loro protezione da rischi di stigmatizzazioni sociali (e, dunque, la protezione dei dati personali di tali assistiti) mirava a evitare l'esposizione dell'interessato a discriminazioni, realizzando quel binomio dignità personale-interesse collettivo, sotteso, nell'art. 32 della Costituzione, al diritto alla salute (43). In tale direzione, il Garante aveva riconosciuto, in una sua decisione, l'obbligo di garantire, per gli interessati positivi all'HIV, la massima tutela della riservatezza e della propria dignità personale, stabilendo il divieto, per le commissioni mediche che svolgono gli accertamenti sanitari sui lavoratori, di divulgare la diagnosi (relativa anche alla patologia di AIDS) riscontrata in sede di verifica sanitaria, e ribadendo quanto disposto dalla L. 135/1990, secondo cui i risultati dei controlli diagnostici devono essere comunicati dagli operatori sanitari esclusivamente all'interessato, salvo suo consenso espresso (44). L'art. 5, comma 4, della L. n. 135/1990 stabilisce, difatti, che "la comunicazione di risultati di accertamenti diagnostici diretti o indiretti per infezione da HIV può essere data esclusivamente alla persona cui tali esami sono riferiti". Pochi mesi dopo, il Garante –

(40) Califano, *Il ruolo di vigilanza del Garante per la protezione dei dati personali*, in *federalismi.it*, 2020, 1 ss.; Califano, *La protezione dei dati personali e il ruolo del Garante in ambito pubblico*, in *Rivista di diritto dei media*, 2018, 8 ss.

(41) Garante per la protezione dei dati personali, *Dati sensibili: divulgazione da parte della polizia giudiziaria*, 13 aprile 1999, doc. web n. 39077, all'indirizzo <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39077>.

(42) IX Legislatura della Repubblica italiana, Proposta di legge a firma dell'On. Stefano Rodotà, *Norme sulla riservatezza delle persone affette da sindrome da immunodeficienza acquisita (AIDS) e dei sieropositivi*, Atto C.4580 del 6 aprile 1987, all'indirizzo <http://www.camera.it/_dati/leg09/lavori/stampati/pdf/45800001.pdf >.

(43) Soro, *Incontro "Verso una nuova privacy?" In ricordo di Stefano Rodotà - Intervento del Presidente del Garante*, 6 ottobre 2017, all'indirizzo <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/6937167>.

(44) Garante per la protezione dei dati personali, *Privacy: la diagnosi di AIDS non si può divulgare*, 31 luglio 1998, doc. web n. 48865, all'indirizzo <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/48865#:~:text=31%20luglio%201998-,Privacy%3A%20la%20diagnosi%20di%20AIDS%20non,pu%C3%B2%20divulgare%20%2D%2031%20luglio%201998&text=Il%20Garante%20per%20la%20protezione,nel%20settore%20pubblico%20e%20privato.>; Garante per la protezione dei dati personali, *Pubblica amministrazione - Infermità da causa di servizio, pensioni privilegiate ed equo indennizzo*, 3 maggio 2001, doc. web n. 1076053, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1076053; Garante per la protezione dei dati personali, 7 gennaio 1999, doc. web n. 38989. Per i profili penalistici, Garante per la protezione dei dati personali, *Relazione Annuale 2018*, 7 maggio 2019, doc. web n. 9109075l, all'indirizzo <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9109075>, laddove afferma che "sotto il profilo penale, possono essere tenute parimenti in considerazione le riflessioni in ambito giuridico e scientifico circa i presupposti per l'eventuale applicazione dell'esimente dello stato di necessità (art. 54 c.p.) o della "giusta causa" – richiamata anche dalle norme di deontologia medica – che legittimerebbe la rivelazione di informazioni eventualmente coperte da segreto professionale (art. 622 c.p., nonché codice di deontologia medica 2014, artt. 10, 12 e 34) nel caso in cui la sieropositività sia resa nota dal medico senza il consenso dell'interessato a un suo familiare, allorché vi sia l'urgenza di salvaguardare l'integrità psico-fisica del familiare medesimo, laddove sia in grave (e altrimenti non evitabile) pericolo la salute o la vita di questi".

in riferimento a una richiesta avanzata dal primario di una divisione di malattie infettive, in ordine alla richiesta di trasmissione di dati nominali e di indicazioni terapeutiche relative ai pazienti affetti da AIDS pervenuta dal direttore generale della stessa U.L.S.S. – aveva sancito che la comunicazione dei sopracitati dati personali, sensibili, alla direzione sanitaria, motivata da stringente necessità di rilevamento di informazioni concernenti il consumo dei farmaci, non fosse conforme al dettato normativo della L. n. 135/1990, considerate le finalità di tipo statistico-contabile perseguite dalla direzione, non preordinate, quindi, ad esigenze di cura delle persone affette da AIDS. Le rilevazioni e i controlli sul numero delle presenze, sulla durata dei periodi di degenza, nonché sul tipo di farmaci somministrati dovrebbero avvenire attraverso sistemi di monitoraggio in grado di preservare l'anonimato dei soggetti interessati (45). Analogamente, nel 2000, l'Autorità aveva rappresentato, in un parere pronunciato su richiesta della Lega italiana per la lotta all'AIDS, riguardo all'applicazione delle norme che disciplinano la tutela della privacy rispetto alla sorveglianza epidemiologica dei casi di infezione da HIV (e al correlato obbligo di denuncia dei casi di AIDS conclamati), l'importanza di conservare i dati anagrafici, relativi a persone sieropositive o affette dall'Aids, separatamente da quelli sanitari, come pure, se questi ultimi risiedono in elenchi, registri e banche dati, di applicare ad essi tecniche di cifratura o misure che consentano di identificare gli interessati solo in caso di effettiva e stringente necessità (46). Più recentemente, il Garante ha inflitto una sanzione, nell'ordine di ventimila euro, nei confronti di un odontoiatra che domandava, nell'ambito delle prestazioni eseguite, ai propri pazienti, se fossero positivi all'infezione da HIV. L'Autorità ha chiarito come tale richiesta risulti legittima nella fase di avvio della relazione medica, in vista della corretta programmazione del piano di cura più adeguato al singolo caso, se ritenuta dal professionista sanitario necessaria in funzione del tipo di intervento sanitario da eseguire sull'assistito, "ferma restando la volontà del paziente di decidere, in modo consapevole (e quindi informato) e responsabile, di non comunicare al medico alcuni eventi sanitari che lo riguardano" (47). Più in generale, gli assiomi pocanzi elencati oggi si traducono anche nella corretta implementazione degli strumenti di sanità digitale, quali la refertazione *online*, la cartella clinica elettronica, il Dossier Sanitario Elettronico (DSE) e il Fascicolo Sanitario Elettronico (FSE) (48). Come è noto, nel nostro ordinamento, la disciplina vigente in ambito sanitario consente di consultare i referti mediante modalità digitali, quali l'accesso al proprio FSE, la ricezione di un messaggio di posta elettronica, tanto più l'accesso a un portale *web* istituzionale. Con riferimento alla refertazione *online*, il Garante privacy, nel 2009, aveva prescritto che i referti riguardanti accertamenti relativi ad indagini genetiche o all'HIV non possono essere oggetto di comunicazione all'interessato tramite modalità digitali. Nell'aggiornamento approntato nel 2020, la stessa Autorità ha ulteriormente puntualizzato che, anche qualora l'interessato propenda per l'adesione ai servizi di refertazione *online*, deve essergli concesso, in relazione ai singoli esami clinici a cui si sottoporrà di volta in volta, di manifestare una volontà contraria, ribadendo che gli accertamenti relativi ad indagini genetiche o all'HIV non possono essere comunicate all'interessato tramite modalità digitali (49). Inoltre, anche ove sussista una base giuridica per il trattamento di tali dati personali, l'Autorità ha corroborato l'assunto secondo il quale il referto digitale va protetto con specifiche misure (50), quali, ad esempio, *policies* sui tempi di cancellazione dei dati, protocolli crittografici per i siti *web* e sistemi di *strong authentication* per le piattaforme in uso *(51)*. Analogamente, il Garante, nelle FAQ relative al FSE, ha chiarito che spetta "alla struttura sanitaria individuare le modalità più corrette per assicurare la prevista intermediazione tra medico e paziente in merito al significa-

(45) Garante per la protezione dei dati personali, *Parere in ordine al trattamento di dati personali relativi ad ammalati di AIDS*, 7 gennaio 1999, doc. web n. 38989, all'indirizzo <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/38989>. Cfr. anche Garante per la protezione dei dati personali, *Parere in ordine all'applicazione della legge 5 giugno 1990, n. 135*, 16 febbraio 2000, doc. web n. 30907, all'indirizzo <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/30907>.

(46) Garante per la protezione dei dati personali, *Aids: vanno rafforzate garanzie e misure di sicurezza sui dati sanitari*, 21 febbraio 2000, doc. web n. 47040, all'indirizzo <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/47040>.

(47) Garante per la protezione dei dati personali, *Ordinanza ingiunzione,* 10 giugno 2021, doc. web n. 9677521, all'indirizzo <https://gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9677521>.

(48) Guarda - Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, Milano, 2023, 302 ss.; Pietroletti - Nicotra, *Tutela della salute, sistemi digitali e privacy*, in *Rivista italiana di informatica e diritto*, 2022, 283 ss.; Escurolle, *Le novità sul Fascicolo Sanitario Elettronico (FSE)*, in *Ciberspazio e diritto: rivista internazionale di informatica giuridica*, 2020, 427 ss.

(49) Garante per la protezione dei dati personali, *Linee guida in tema di referti on-line*, 25 giugno 2009, doc. web n. 1630271, all'indirizzo <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1630271>, come aggiornate nel 2020.

(50) Garante per la protezione dei dati personali, *Relazione annuale sull'attività 2022*, 6 luglio 2023, doc. web n. 9905999, all'indirizzo <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9905999>.

(51) Garante per la protezione dei dati personali, *Ordinanza ingiunzione nei confronti di Servizio Idrico Integrato S.c.p.a.*, 6 ottobre 2022, n. 328, doc. web n. 9817058, all'indirizzo <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9817058>.

to diagnostico di questi referti, così come richiesta dalla disciplina di settore". Ne deriva che, una volta soddisfatta tale intermediazione, il referto vertente sull'HIV, al pari di ogni altro referto, può essere reso disponibile all'assistito tramite il FSE. Resta fermo, inoltre, che il risultato del test HIV può essere reso accessibile al personale che ha in cura l'interessato, solo previo rilascio del consenso informato a cura dell'assistito (52). Di conseguenza, le strutture sanitarie sono tenute a "bloccare" il flusso di dati all'interno del FSE, e, solamente dopo interlocuzione diretta tra medico e paziente, il cui fine è quello di consentire a chi abbia effettuato un test un'adeguata assistenza psicologica e una consulenza specialistica sul significato del risultato, il referto potrà entrare nel Fascicolo, sempre previo e libero consenso espresso dal paziente. Infine, rileva l'applicazione, da parte delle strutture sanitarie, del principio di *accountability*, cui si è fatto cenno nel paragrafo precedente del presente commento, nell'alimentazione della cartella clinica. La diagnosi di HIV fornita direttamente dal paziente come dato anamnestico, infatti, può essere acclusa in cartella clinica, una volta registrata la manifestazione positiva di volontà dell'interessato (53). Vieppiù, sotto il profilo della custodia della cartella clinica, il principio di responsabilizzazione impone al titolare del trattamento di inibire accessi non autorizzati alle informazioni sulla salute dell'assistito, considerato che la struttura sanitaria è tenuta a risarcire il danno sofferto dal paziente in conseguenza della mancata tutela di dati personali contenuti nella cartella, ove non riesca a comprovare di avere adottato tutte le misure necessarie utili a garantire il "*right to privacy*". Appare evidente, dunque, la necessità di dotarsi di misure di sicurezza tecniche e organizzative, come prescritto dal GDPR (54), anche nella gestione del dato personale nell'ambito degli archivi sanitari (55). Di tale principio, la giurisprudenza italiana si era fatta portatrice prima ancora che il GDPR trovasse applicazione, stabilendo che "la mera conservazione della cartella in tale locale non è di per sé sufficiente a garantire la riservatezza dei dati personali del paziente anche se tale locale è riservato al personale sanitario, in mancanza di dimostrazione che a detta sala viene effettivamente impedito l'accesso a terzi" (56). L'Autorità garante, recentemente, in un suo Provvedimento relativo a una violazione dei dati personali (*data breach*), avvenuta a mezzo posta elettronica, ha rammentato come il titolare del trattamento, in ogni caso, sia tenuto a rispettare i principi in materia di *data protection*, fra i quali quello di "integrità e riservatezza", secondo il quale i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza, tale da scongiurare trattamenti non autorizzati o illeciti, così come la perdita, la distruzione o il danno accidentale (57). In tal senso, il personale sanitario dell'Azienda Ospedaliero-Universitaria di Modena, mediante l'inserimento, nel campo destinatari, di novantotto indirizzi *e-mail*, trasmetteva formale comunicazione ai pazienti affetti da HIV, seguiti dall'ambulatorio di Malattie Infettive, tramite la quale gli stessi venivano invitati a compilare un questionario sul loro stato di salute, consentendo, mediante la consultazione del campo denominato "copia conoscenza", che tutti i destinatari potessero conoscere i dati di contatto di altri soggetti, affetti da HIV, in cura presso il medesimo ambulatorio (58). Pertanto, la condotta posta in essere dall'Azienda ha configurato "una comunicazione di dati relativi alla salute e, in particolare, di infezione da HIV, di novantotto pazienti ad altrettanti pazienti, in assenza di un idoneo presupposto giuridico" (59) e, quindi, la violazione dei principi di base del trattamento di cui agli artt. 5, par. 1, lett. f), e 9 del GDPR, nonché dell'art. 75 del Codice, disposizione recante "Specifiche condizioni in ambito sanitario", laddove specifica che "il trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere h) ed i), e 3 del regolamento, dell'articolo 2-*septies* del presente codice, nonché nel rispetto delle specifiche disposizioni di settore". In tema di (illecita) comunicazione (60) della positività all'HIV,

(52) Garante per la protezione dei dati personali, *FAQ - Fascicolo sanitario elettronico (FSE)*, <https://www.garanteprivacy.it/temi/fse>.

(53) In materia di consenso, va ricordato che secondo il Garante privacy le Direzioni Sanitarie devono individuare adeguate procedure affinché vi sia traccia del consenso a inserire il dato in cartella, cfr. in tal senso Garante per la protezione dei dati personali, *Illiceità nel trattamento di dati personali e sensibili presso una struttura ospedaliera*, 18 dicembre 2014, doc. web n. 3725976, all'indirizzo <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3725976>.

(54) Art. 32, GDPR.

(55) Ciclosi, *La gestione degli archivi sanitari e la protezione dei dati personali, tra pseudonimizzazione e anonimizzazione*, in *Officina della storia*, 2020, 50 ss.

(56) Cass., II Sez., 30 gennaio 2009, n. 2468, sentenza citata in Garante per la protezione dei dati personali, *Relazione sull'attività 2014*, 23 giugno 2015, doc. web n. 4056414, all'indirizzo <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4056414>.

(57) Art. 5, par. 1, lett. f), GDPR.

(58) Garante per la protezione dei dati personali, *Ordinanza ingiunzione nei confronti di Azienda Ospedaliero-Universitaria di Modena*, 16 settembre 2021, doc. web n. 9722297, all'indirizzo <https://gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9722297>.

(59) Garante per la protezione dei dati personali, *Ordinanza ingiunzione nei confronti di Azienda Ospedaliero-Universitaria di Modena*, 16 settembre 2021, cit.

(60) Ai sensi dell'art. 2-*ter*, comma 4, del Codice Privacy, per comunicazione di dati personali si intende il darne conoscenza a uno o più soggetti

infine, non può tacersi il *dictum* della Corte di Cassazione in merito alla trasmissione, da parte di un Circolo didattico ad altro Circolo, del verbale (nella sua versione integrale) relativo all'accertamento sanitario effettuato dalla Commissione medica di verifica di Grosseto, in relazione alla richiesta dell'interessata (che aveva proposto reclamo presso il Garante privacy, impugnato dal Circolo) volta ad ottenere la pensione di inabilità, documento contenente, oltre alla valutazione medico-legale circa l'inidoneità all'impiego, altri dati personali e informazioni anamnestiche, tra cui quella relativa all'infezione da HIV(61). La Corte ha rigettato il ricorso del Circolo didattico, poiché "avrebbe potuto conseguire ugualmente la prosecuzione del procedimento trasmettendo una copia parziale della documentazione pervenutagli da cui fosse omessa la visibilità di dati sanitari riferiti all'interessata ultronei rispetto a quello dell'accertata inabilità al lavoro e riguardanti la diagnosi accertata, gli esami obiettivi e gli accertamenti clinici e strumentali effettuati, nonché l'anamnesi da cui emerge anche l'informazione relativa all'HIV, in maniera tale da rendere nota all'istituzione scolastica competente ad emettere il provvedimento finale soltanto l'informazione relativa al giudizio medico-legale di inidoneità all'impiego" (62).

determinati, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione.

(61) Cass., I Sez., 29 maggio 2015, n. 11223.

(62) Cass., I Sez., 29 maggio 2015, n. 11223.

# Pubblicità personalizzata e formalismo degli interpreti

Corte di Giustizia dell'Unione Europea; Grande Sezione; sentenza 4 luglio 2023, n. 252/21; Pres. K. Lenaerts; Rel. L.S. Rossi.

*Fermo restando il rispetto del suo obbligo di leale cooperazione con le autorità di controllo, un'Autorità Garante della Concorrenza di uno Stato membro può constatare, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa, che le condizioni generali d'uso di tale impresa relative al trattamento dei dati personali, e la loro applicazione, non sono conformi al GDPR, qualora tale constatazione sia necessaria per accertare l'esistenza di un tale abuso.*

*La circostanza che l'operatore di un social network online occupi una posizione dominante sul mercato dei social network online non osta, di per sé, a che gli utenti di tale social network possano validamente acconsentire al trattamento dei loro dati personali effettuato da tale operatore.*

*Malgrado la gratuità dei servizi online di Facebook, l'utente di quest'ultimo non può ragionevolmente attendersi che, senza il suo consenso, l'operatore di tale social network tratti i suoi dati personali a fini di personalizzazione della pubblicità.*

*...Omissis...*

**Svolgimento del processo - Motivi della decisione**

1 La domanda di pronuncia pregiudiziale verte sull'interpretazione dell'articolo 4, paragrafo 3, TUE nonché dell'articolo 6, paragrafo 1, dell'articolo 9, paragrafi 1 e 2, dell'articolo 51, paragrafo 1, e dell'articolo 56, paragrafo 1, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU 2016, L 119, pag. 1, e rettifiche in GU 2016, L 314, pag. 72, GU 2018, L 127, pag. 3 e GU 2021, L 74, pag. 35; in prosieguo: il "RGPD").

2 Tale domanda è stata presentata nell'ambito di una controversia tra M.P. Inc., già F. Inc., M.P.I. Ltd, già F.I. Ltd, e F.D. GmbH, da un lato, e il Bundeskartellamt (autorità federale garante della concorrenza, Germania), dall'altro, in merito alla decisione di quest'ultimo di vietare a tali società di procedere al trattamento di taluni dati personali previsto dalle condizioni generali di utilizzo del social network F. (in prosieguo: le "condizioni generali").

Contesto normativo

Diritto dell'Unione

Regolamento (CE) n. 1/2003

3 L'articolo 5 del regolamento (CE) n. 1/2003 del Consiglio, del 16 dicembre 2002, concernente l'applicazione delle regole di concorrenza di cui agli articoli [101 e 102 del TFUE] (GU 2003, L 1, pag. 1),), rubricato "Competenze delle autorità garanti della concorrenza degli Stati membri", prevede quanto segue:

"Le autorità garanti della concorrenza degli Stati membri sono competenti ad applicare gli articoli [101 et 102 TFUE] in casi individuali. A tal fine, agendo d'ufficio o in seguito a denuncia, possono adottare le seguenti decisioni:

- ordinare la cessazione di un'infrazione,
- disporre misure cautelari,
- accettare impegni,
- comminare ammende, penalità di mora o qualunque altra sanzione prevista dal diritto nazionale.

Qualora, in base alle informazioni di cui dispongono, non sussist[a]no le condizioni per un divieto, possono anche decidere di non avere motivo di intervenire"

RGPD

4 I considerando 1, 4, 38, 42, 43, 46, 47, 49 e 51 del RGPD enunciano:

"(1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea ("Carta") e l'articolo 16, paragrafo 1, [TFUE] stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

(...)

(4) Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei

dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.
(...)
(38) I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore.
(...)
(42) Per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. (...) Ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. Il consenso non dovrebbe essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio.
(43) Per assicurare la libertà di prestare il consenso, è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente in tutte le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.
(...)
(46) Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana.
(47) I legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. (...) In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali. (...) Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto.
(...)
(49) Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi (...).
(...)
(51) Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica, essendo inteso che l'utilizzo dei termini "origine razziale" nel presente regolamento non implica l'accettazione da parte dell'Unione [europea] di teorie che tentano di dimostrare l'esistenza di razze umane distinte. Il trattamento di fotografie non dovrebbe co-

stituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica. Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito nei casi specifici di cui al presente regolamento, tenendo conto del fatto che il diritto degli Stati membri può stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del presente regolamento ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Oltre ai requisiti specifici per tale trattamento, dovrebbero applicarsi i principi generali e altre norme del presente regolamento, in particolare per quanto riguarda le condizioni per il trattamento lecito. È opportuno prevedere espressamente deroghe al divieto generale di trattare tali categorie particolari di dati personali, tra l'altro se l'interessato esprime un consenso esplicito o in relazione a esigenze specifiche, in particolare se il trattamento è eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali".

5 L'articolo 4 di tale regolamento così dispone:

"Ai fini del presente regolamento s'intende per:

1) "dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); (...)

2) "trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

(...)

7) "titolare del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

(...)

11) "consenso dell'interessato": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, [a] che i dati personali che lo riguardano siano oggetto di trattamento;

(...)

23) "trattamento transfrontaliero",

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

(...)".

6 L'articolo 5 di detto regolamento, rubricato "Principi applicabili al trattamento di dati personali", dispone, ai paragrafi 1 e 2, quanto segue:

"1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; (...)

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");

(...)

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ("responsabilizzazione")".

7 L'articolo 6 del medesimo regolamento, rubricato "Liceità del trattamento", è così formulato:

"1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore;
La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.
(...)
3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:
a) dal diritto dell'Unione; o
b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento.
(...)
(...) Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito".
8 Ai sensi dell'articolo 7 del RGPD, rubricato "Condizioni per il consenso":
"1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
(...)
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto".
9 L'articolo 9 di detto regolamento, rubricato "Trattamento di categorie particolari di dati personali", dispone quanto segue:
"1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:
a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
(...)
e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
(...)".
10 L'articolo 13 del regolamento in parola, relativo alle "[i]nformazioni da fornire qualora i dati personali siano raccolti presso l'interessato", prevede, al suo paragrafo 1, quanto segue:
"In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
(...)
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
(...)".
11 Il capo VI del RGPD, relativo alle "[a]utorità di controllo indipendenti", comprende gli articoli da 51 a 59 di tale regolamento.
12 L'articolo 51 del regolamento succitato, rubricato "Autorità di controllo", ai paragrafi 1 e 2 così prevede:
"1. Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di controllare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (...).
2. Ogni autorità di controllo contribuisce alla coerente applicazione del presente regolamento in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione [europea], conformemente al capo VII".
13 Ai sensi dell'articolo 55 del medesimo regolamento, rubricato "Competenza":
"1. Ogni autorità di controllo è competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del presente regolamento nel territorio del rispettivo Stato membro.
2. Se il trattamento è effettuato da autorità pubbliche o organismi privati che agiscono sulla base dell'articolo 6, paragrafo 1, lettera c) o e), è competente l'autorità di controllo dello Stato membro interessato. In tal caso, non si applica l'articolo 56".
14 L'articolo 56 del RGPD, rubricato "Competenza dell'autorità di controllo capofila", al suo paragrafo 1 enuncia:
"Fatto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal

suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60".
15 L'articolo 57 di detto regolamento, rubricato "Compiti", al suo paragrafo 1 così dispone:
"Fatti salvi gli altri compiti indicati nel presente regolamento, sul proprio territorio ogni autorità di controllo:
a) sorveglia e assicura l'applicazione del presente regolamento;
(...)
g) collabora, anche tramite scambi di informazioni, con le altre autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del presente regolamento;
(...)".
16 L'articolo 58 di detto regolamento stabilisce, al suo paragrafo 1, l'elenco dei poteri di indagine di cui dispone ogni autorità di controllo e precisa, al suo paragrafo 5, che "[o]gni Stato membro dispone per legge che la sua autorità di controllo abbia il potere di intentare un'azione o di agire in sede giudiziale o, ove del caso, stragiudiziale in caso di violazione del presente regolamento per far rispettare le disposizioni dello stesso".
17 La sezione 1, rubricata "Cooperazione", del capo VII del RGPD, a sua volta rubricato "Cooperazione e coerenza", comprende gli articoli da 60 a 62 di tale regolamento. L'articolo 60, relativo alla "[c]ooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate", al paragrafo 1 prevede quanto segue:
"L'autorità di controllo capofila coopera con le altre autorità di controllo interessate conformemente al presente articolo nell'adoperarsi per raggiungere un consenso. L'autorità di controllo capofila e le autorità di controllo interessate si scambiano tutte le informazioni utili".
18 L'articolo 61 di detto regolamento, rubricato "Assistenza reciproca", al suo paragrafo 1, così recita:
"Le autorità di controllo si scambiano le informazioni utili e si prestano assistenza reciproca al fine di attuare e applicare il presente regolamento in maniera coerente, e mettono in atto misure per cooperare efficacemente tra loro. L'assistenza reciproca comprende, in particolare, le richieste di informazioni e le misure di controllo, quali le richieste di autorizzazioni e consultazioni preventive e le richieste di effettuare ispezioni e indagini".
19 L'articolo 62 del medesimo regolamento, rubricato "Operazioni congiunte delle autorità di controllo", ai paragrafi 1 e 2 prevede quanto segue:
"1. Se del caso, le autorità di controllo conducono operazioni congiunte, incluse indagini congiunte e misure di contrasto congiunte, cui partecipano membri o personale di autorità di controllo di altri Stati membri.
2. Qualora il titolare del trattamento o responsabile del trattamento abbia stabilimenti in vari Stati membri o qualora esista la probabilità che il trattamento abbia su un numero significativo di interessati in più di uno Stato membro un impatto negativo sostanziale, un'autorità di controllo di ogni Stato membro in questione ha il diritto di partecipare alle operazioni congiunte. (...)".
20 La sezione 2 del capo VII del RGPD, rubricata "Coerenza", comprende gli articoli da 63 a 67 di detto regolamento. Ai sensi dell'articolo 63, rubricato "Meccanismo di coerenza":
"Al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il meccanismo di coerenza stabilito nella presente sezione".
21 A termini dell'articolo 64, paragrafo 2, di tale regolamento:
"Qualsiasi autorità di controllo, il presidente del comitato [europeo per la protezione dei dati] o la Commissione può richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro siano esaminate dal comitato [europeo per la protezione dei dati] al fine di ottenere un parere, in particolare se un'autorità di controllo competente non si conforma agli obblighi relativi all'assistenza reciproca ai sensi dell'articolo 61 o alle operazioni congiunte ai sensi dell'articolo 62".
22 L'articolo 65 di detto regolamento, rubricato "Composizione delle controversie da parte del comitato", al paragrafo 1 così dispone:
"Al fine di assicurare l'applicazione corretta e coerente del presente regolamento nei singoli casi, il comitato [europeo per la protezione dei dati] adotta una decisione vincolante nei seguenti casi:
a) se, in un caso di cui all'articolo 60, paragrafo 4, un'autorità di controllo interessata ha sollevato un'obiezione pertinente e motivata a un progetto di decisione dell'autorità di controllo capofila e l'autorità capofila di controllo non abbia dato seguito all'obiezione o abbia rigettato tale obiezione in quanto non pertinente o non motivata. La decisione vincolante riguarda tutte le questioni oggetto dell'obiezione pertinente e motivata, in particolare se sussista una violazione del presente regolamento;
b) se vi sono opinioni contrastanti in merito alla competenza delle autorità di controllo interessate per lo stabilimento principale;
(...)".
Diritto tedesco
23 L'articolo 19, paragrafo 1, del Gesetz gegen Wettbewerbsbeschränkungen (legge contro le restrizioni della concorrenza), nella sua versione pubblicata il 26 giugno 2013 (BGBl. 2013 I, pag. 1750, 3245), modificata da ultimo dall'articolo 2 della L. del 16 luglio 2021 (BGBl. 2021 I, pag. 2959) (in prosieguo: il "GWB") così dispone:

"È vietato lo sfruttamento abusivo di una posizione dominante sul mercato tramite una o più imprese".
24 Ai sensi dell'articolo 32, paragrafo 1, del GWB:
"L'autorità garante della concorrenza può obbligare le imprese o associazioni di imprese a porre fine a un'infrazione alle disposizioni della presente parte o agli articoli 101 o 102 del Trattato sul funzionamento dell'Unione europea".
25 L'articolo 50f del GWB prevede, al suo paragrafo 1, quanto segue:
"Le autorità garanti della concorrenza, le autorità di regolamentazione, il responsabile federale della protezione dei dati e della libertà di informazione, i responsabili regionali della protezione dei dati e le autorità competenti ai sensi dell'articolo 2 dell'EU-Verbraucherschutzdurchführungsgesetz [(legge per l'attuazione del diritto dell'Unione europea in materia di tutela dei consumatori)] possono, indipendentemente dalla procedura scelta, scambiarsi informazioni, compresi dati personali e segreti tecnici e commerciali, nella misura necessaria per l'assolvimento dei rispettivi compiti e utilizzare tali informazioni nell'ambito delle loro procedure. (...)".
Procedimento principale e questioni pregiudiziali
26 M.P.I. gestisce l'offerta del social network online Facebook nell'Unione e promuove, in particolare all'indirizzo www.facebook.com, servizi gratuiti per gli utenti privati. Altre società del gruppo M. offrono, nell'Unione, altri servizi online tra cui Instagram, WhatsApp, Oculus e - fino al 13 marzo 2020 - Masquerade.
27 Il modello economico del social network online Facebook si fonda sul finanziamento tramite la pubblicità online, che viene creata su misura per i singoli utenti del social network in funzione, in particolare, del loro comportamento di consumo, dei loro interessi, del loro potere d'acquisto e della loro situazione personale. Il presupposto tecnico per questo tipo di pubblicità è la creazione automatizzata di profili dettagliati degli utenti del network e dei servizi online offerti a livello del gruppo M. A tal fine, oltre ai dati che gli utenti forniscono direttamente al momento della loro iscrizione ai servizi online di cui trattasi, vengono raccolti, all'interno e all'esterno di detto social network e dei servizi online forniti dal gruppo M., e messi in relazione ai loro diversi account di utenza anche altri dati relativi ai tali utenti e ai loro dispositivi. Il quadro generale di tali dati consente di trarre conclusioni dettagliate sulle preferenze e sugli interessi dei medesimi utenti.
28 Per il trattamento di tali dati, M.P.I. si basa sul contratto d'uso a cui gli utenti del social network Facebook aderiscono tramite l'attivazione del pulsante "Iscriviti" e con il quale essi accettano le condizioni generali stabilite da detta società. L'accettazione di queste condizioni è necessaria per poter utilizzare il social network Facebook. Per quanto riguarda il trattamento dei dati personali, le condizioni generali rinviano alle regole sull'uso dei dati e dei marcatori (cookies) adottate dalla suddetta società. In forza di queste ultime, M.P.I. raccoglie dati riferiti agli utenti e ai loro dispositivi, relativi alle loro attività all'interno e all'esterno del social network, e li mette in relazione con gli account Facebook degli utenti interessati. Per quanto riguarda questi ultimi dati, relativi alle attività al di fuori del social network (in prosieguo anche: i "dati off Facebook"), si tratta, da un lato, dei dati concernenti la consultazione di pagine Internet e di applicazioni di terzi che sono collegate a Facebook attraverso interfacce di programmazione – gli "Strumenti business di Facebook" – e, dall'altro, dei dati riguardanti l'utilizzo degli altri servizi online appartenenti al gruppo M., tra i quali Instagram, WhatsApp, Oculus e – fino al 13 marzo 2020 – Masquerade.
29 L'autorità federale garante della concorrenza ha avviato nei confronti di M.P., M.P.I. e F.D. un procedimento in esito al quale, con decisione del 6 febbraio 2019, fondata sull'articolo 19, paragrafo 1, e sull'articolo 32 del GWB, essa ha sostanzialmente vietato loro di subordinare, nelle condizioni generali, l'uso del social network Facebook da parte di utenti privati residenti in Germania al trattamento dei loro dati off Facebook e di procedere, senza il consenso di detti utenti, al trattamento di tali dati sulla base delle condizioni generali allora vigenti. Inoltre, essa ha ordinato loro di adeguare dette condizioni generali in modo che da esse risultasse chiaramente che tali dati non sarebbero stati né raccolti, né messi in relazione con gli account degli utenti Facebook, né utilizzati senza il consenso dell'utente interessato, e ha chiarito che tale consenso non è valido qualora costituisca una condizione per l'utilizzo del social network.
30 L'autorità federale garante della concorrenza ha motivato la sua decisione con il fatto che il trattamento dei dati degli utenti interessati, quale previsto dalle condizioni generali e attuato da M.P.I., costituiva uno sfruttamento abusivo della posizione dominante di tale società sul mercato dei sociali network online per gli utenti privati in Germania, ai sensi dell'articolo 19, paragrafo 1, del GWB. Precisamente, secondo l'autorità federale garante della concorrenza, tali condizioni generali, in quanto emanazione di tale posizione dominante, sarebbero abusive perché il trattamento dei dati off Facebook da esse previsto non sarebbe conforme ai valori sottesi al RGPD e, in particolare, non potrebbe essere giustificato alla luce dell'articolo 6, paragrafo 1, e dell'articolo 9, paragrafo 2, del medesimo regolamento.
31 L'11 febbraio 2019 M.P., M.P.I. e F.D. hanno presentato un ricorso avverso la decisione dell'autorità federale garante della concorrenza dinanzi all'Oberlandesgericht Düsseldorf (Tribunale superiore del Land, Düsseldorf, Germania).

32 Il 31 luglio 2019 M.P.I. ha introdotto nuove condizioni generali, le quali indicano espressamente che l'utente, invece di pagare per l'uso dei prodotti Facebook, dichiara di acconsentire alle inserzioni pubblicitarie.
33 Inoltre, dal 28 gennaio 2020 M.P. offre in tutto il mondo, l'"Off-Facebook-Activity", la quale consente agli utenti del social network Facebook di visualizzare un riepilogo delle informazioni che li riguardano, che le società del gruppo M. ottengono in relazione alle loro attività su altri siti Internet e applicazioni, e di scollegare, se lo desiderano, tali dati dal loro account Facebook.com, tanto per il passato quanto per il futuro.
34 L'Oberlandesgericht Düsseldorf (Tribunale superiore del Land, Düsseldorf) nutre dubbi, in primo luogo, in merito alla possibilità per le autorità nazionali garanti della concorrenza di controllare, nell'ambito dell'esercizio delle loro competenze, la conformità di un trattamento di dati personali alle condizioni stabilite nel RGPD; in secondo luogo, in merito alla possibilità per un operatore di un social network online di trattare i dati personali sensibili della persona interessata, ai sensi dell'articolo 9, paragrafi 1 e 2, di tale regolamento; in terzo luogo, in merito alla liceità del trattamento dei dati personali dell'utente interessato da parte di un siffatto operatore, conformemente all'articolo 6, paragrafo 1, di detto regolamento, e, in quarto luogo, in merito alla validità – alla luce dell'articolo 6, paragrafo 1, primo comma, lettera a), e dell'articolo 9, paragrafo 2, lettera a), del medesimo regolamento – del consenso prestato a un'impresa che detiene una posizione dominante sul mercato nazionale dei social network online, ai fini di un trattamento di questo tipo.
35 In tale contesto, ritenendo che la soluzione della controversia principale dipenda dalla risposta da dare a tali questioni, l'Oberlandesgericht Düsseldorf (Tribunale superiore del Land, Düsseldorf) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:
"1) a) Se sia compatibile con gli articoli 51 e seguenti del RGPD il fatto che un'autorità garante della concorrenza di uno Stato membro, quale l'autorità federale garante della concorrenza, che non sia un'autorità di controllo ai sensi degli articoli 51 e seguenti del RGPD e nel cui Stato membro un'impresa stabilita al di fuori dell'Unione europea disponga di una filiale di supporto alla filiale principale nel settore della pubblicità, della comunicazione e delle relazioni pubbliche – mentre la filiale principale di tale impresa è situata in un altro Stato membro e ha la responsabilità esclusiva per il trattamento dei dati personali per l'intero territorio dell'Unione europea –, constati, nell'ambito dell'esercizio di un controllo degli abusi di posizione dominante ai sensi del diritto della concorrenza, che le condizioni contrattuali operate dalla filiale principale relativamente al trattamento dei dati e la relativa attuazione violano il RGPD, e disponga di porre fine a tale violazione.
b) In caso affermativo, se ciò sia compatibile con l'articolo 4, paragrafo 3, TUE se, nel contempo, l'autorità di controllo capofila nello Stato membro in cui si trova la filiale principale ai sensi dell'articolo 56, paragrafo 1, del RGPD sottopone a un procedimento di indagine le condizioni contrattuali per il trattamento dei dati operate da quest'ultima.
In caso di risposta affermativa alla prima questione:
2) a) Se, nel caso di un utente di Internet che si limiti a visitare siti Internet o applicazioni ("app") che fanno riferimento ai criteri di cui all'articolo 9, paragrafo 1, del RGPD – come app di incontri, siti per incontri omosessuali, siti di partiti politici, siti relativi alla salute – o vi immetta dati al fine di registrarvisi o di effettuare degli ordini, e di una (...) società, come [M.P.I.], che raccolga i dati relativi all'accesso ai siti e alle app e alle informazioni ivi immesse da parte dell'utente – tramite interfacce integrate nei siti e nelle app, come "Strumenti di Facebook Business", o tramite marcatori temporanei ("cookies") o simili tecnologie di memorizzazione utilizzati sul computer o sul dispositivo terminale mobile dell'utente –, li colleghi ai dati dell'account Facebook.com dell'utente e li utilizzi, la raccolta e/o il collegamento e/o l'utilizzo configurino un trattamento di dati sensibili ai sensi di detto articolo.
b) In caso affermativo: se l'accesso a tali siti e app e/o l'inserimento di dati e/o l'attivazione di pulsanti ("plug-in social" come "Mi piace", "Condividi" o "Facebook Login" o "Account Kit") integrati in tali siti o app da un fornitore come [M.P.I.] costituiscano una modalità di rendere manifestamente pubblici i dati relativi all'accesso di per sé e/o i dati immessi da parte dell'utente, ai sensi dell'articolo 9, paragrafo 2, lettera e), del RGPD.
3) Se un'impresa come [M.P.I.], che gestisce un social network digitale finanziato dalla pubblicità e che offre, nelle sue condizioni d'uso, la personalizzazione dei contenuti e della pubblicità, la sicurezza del network, il miglioramento dei prodotti e l'utilizzo coerente e senza interruzioni di tutti i prodotti del gruppo, possa invocare la giustificazione della necessità per l'esecuzione di un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b), del RGPD, o la giustificazione della tutela dei legittimi interessi di cui all'articolo 6, paragrafo 1, lettera f), del RGPD, quando a tali fini essa raccoglie dati generati da altri servizi propri del gruppo e da siti e app di terzi tramite interfacce in essi integrate, come "Strumenti di Facebook Business", oppure tramite cookies o simili tecnologie di memorizzazione utilizzati sul computer o sul dispositivo terminale mobile dell'utente, li collega all'account Facebook.com dell'utente e li utilizza.

4) Se, in tal caso, possano essere considerati legittimi interessi ai sensi dell'articolo 6, paragrafo 1, lettera f), del RGPD anche
- la minore età dell'utente, ai fini della personalizzazione dei contenuti e della pubblicità, del miglioramento dei prodotti, della sicurezza del network e delle comunicazioni non commerciali destinate all'utente,
- la fornitura di misurazioni, dati statistici e altri servizi per le aziende a inserzionisti, sviluppatori e altri partner, affinché questi possano valutare e migliorare le proprie prestazioni,
- l'offerta di comunicazioni di marketing destinate all'utente affinché l'impresa possa migliorare i suoi prodotti e condurre marketing diretto,
- ricerca e innovazione per il bene della società per far progredire lo stato dell'arte o la comprensione scientifica relativamente a importanti temi sociali e per avere un impatto positivo sulla società e sul mondo,
- informazioni alle autorità preposte all'applicazione e all'esecuzione della legge e la risposta a richieste legali, al fine di prevenire, di individuare e di perseguire illeciti penali, usi non autorizzati, violazioni delle condizioni d'uso e delle regole aziendali ed altri comportamenti dannosi,
quando a tali fini l'impresa raccoglie dati generati da altri servizi propri del gruppo e da siti e app di terzi tramite interfacce in essi integrate, come "Strumenti di Facebook Business", o tramite cookies o simili tecnologie di memorizzazione utilizzati sul computer o sul dispositivo terminale mobile dell'utente, li collega all'account Facebook.com dell'utente e li utilizza.
5) Se, in tal caso, la raccolta di dati provenienti da altri servizi propri del gruppo e da siti internet e app di terzi tramite interfacce in essi integrate, come "Strumenti di Facebook Business", oppure tramite cookies o simili tecnologie di memorizzazione utilizzati sul computer o sul dispositivo terminale mobile dell'utente, il collegamento con l'account Facebook.com dell'utente e l'utilizzo di tali dati, oppure l'utilizzo di dati già altrimenti e legittimamente raccolti e collegati possano essere giustificati, caso per caso, anche ai sensi dell'articolo 6, paragrafo 1, lettere c), d) ed e) del RGPD, ad esempio per rispondere ad una legittima richiesta di dati specifici [lettera c)], per contrastare comportamenti dannosi e promuovere la sicurezza [lettera d)], per ricerche a beneficio della società e per promuovere protezione, integrità e sicurezza [lettera e)].
6) Se nei confronti di un'impresa in posizione dominante sul mercato come [M.P.I.] sia possibile esprimere un consenso valido, e in particolare libero ai sensi dell'articolo 4, punto 11, del RGPD, in conformità con gli articoli 6, paragrafo 1, lettera a), e 9, paragrafo 2, lettera a), del RGPD.
In caso di risposta negativa alla prima questione:
7) a) Se un'autorità nazionale garante della concorrenza di uno Stato membro, quale l'autorità federale garante della concorrenza, che non sia un'autorità di controllo ai sensi degli articoli 51 e seguenti del RGPD e che esamini una violazione del divieto di abuso di posizione dominante, ai sensi del diritto della concorrenza, da parte di un'impresa in posizione dominante, che non consista in una violazione del RGPD da parte delle sue condizioni per il trattamento dei dati e della loro attuazione, possa effettuare accertamenti, ad esempio nell'ambito del bilanciamento degli interessi, in merito alla conformità al RGPD delle condizioni per il trattamento dei dati di tale impresa e della loro attuazione.
b) In caso affermativo: se, ai sensi dell'articolo 4, paragrafo 3, TUE, ciò valga anche qualora, nel contempo, l'autorità di controllo capofila competente ai sensi dell'articolo 56, paragrafo 1, del RGPD sottoponga le condizioni per il trattamento dei dati di tale impresa ad un procedimento di indagine.
Se la risposta alla settima questione è affermativa, occorre rispondere alle questioni dalla terza alla quinta per quanto riguarda i dati generati dall'utilizzo del servizio Instagram, appartenente al gruppo".
Sulle questioni pregiudiziali
Sulle questioni prima e settima
36 Con la prima e la settima questione, che è opportuno trattare congiuntamente, il giudice del rinvio chiede, in sostanza, se gli articoli 51 e seguenti del RGPD debbano essere interpretati nel senso che un'autorità garante della concorrenza di uno Stato membro può constatare, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa, ai sensi dell'articolo 102 TFUE, che le condizioni generali d'uso di tale impresa relative al trattamento dei dati personali e la loro applicazione non sono conformi al RGPD e, in caso affermativo, se l'articolo 4, paragrafo 3, TUE debba essere interpretato nel senso che una simile constatazione, di natura incidentale, da parte dell'autorità garante della concorrenza è possibile anche nel caso in cui tali condizioni siano sottoposte, al contempo, a una procedura d'esame da parte dell'autorità di controllo capofila competente ai sensi dell'articolo 56, paragrafo 1, del RGPD.
37 Per rispondere a tale questione, si deve anzitutto ricordare che l'articolo 55, paragrafo 1, del RGPD stabilisce la competenza di principio di ogni autorità di controllo ad eseguire i compiti ed esercitare i poteri a essa conferiti, a norma di tale regolamento, nel territorio del rispettivo Stato membro (sentenza del 15 giugno 2021, F.I. e a., C-645/19, EU:C:2021:483, punto 47 e giurisprudenza ivi citata).
38 Tra i compiti assegnati a tali autorità di controllo si annovera quello di controllare l'applicazione del RGPD e di vigilare sul rispetto di quest'ultimo, previsto all'articolo 51, paragrafo 1, e all'articolo 57, paragrafo 1, let-

tera a), del medesimo regolamento, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei loro dati personali nonché di agevolare la libera circolazione di tali dati all'interno dell'Unione. Inoltre, conformemente all'articolo 51, paragrafo 2, e all'articolo 57, paragrafo 1, lettera g), di tale regolamento, tali autorità di controllo cooperano tra loro, anche tramite scambi di informazioni, e si prestano assistenza reciproca in tale ambito al fine di garantire la coerente applicazione del medesimo regolamento e delle misure adottate per assicurarne il rispetto.

39 Al fine di assolvere tali compiti, l'articolo 58 del RGPD conferisce a dette autorità di controllo, al suo paragrafo 1, poteri di indagine, al suo paragrafo 2, poteri correttivi e al suo paragrafo 5, il potere di intentare un'azione o di agire in sede giudiziale o, se del caso, stragiudiziale in caso di violazione di tale regolamento per far rispettare le disposizioni dello stesso.

40 Fatta salva la norma sulla competenza di cui all'articolo 55, paragrafo 1, del RGPD, l'articolo 56, paragrafo 1, di tale regolamento prevede, per i trattamenti transfrontalieri ai sensi del suo articolo 4, punto 23, un meccanismo di "sportello unico", basato su una ripartizione delle competenze tra un'"autorità di controllo capofila" e le altre autorità di controllo interessate, nonché su una cooperazione tra tutte queste autorità secondo la procedura di cooperazione di cui all'articolo 60 di detto regolamento.

41 Inoltre, l'articolo 61, paragrafo 1, del RGPD obbliga segnatamente le autorità di controllo a comunicarsi le informazioni utili nonché a prestarsi reciproca assistenza al fine di attuare ed applicare tale regolamento in modo coerente in tutta l'Unione. L'articolo 63 di detto regolamento precisa che proprio a tal fine è previsto il meccanismo di coerenza, stabilito agli articoli 64 e 65 di quest'ultimo (sentenza del 15 giugno 2021, F.I. e a., C-645/19, EU:C:2021:483, punto 52 e giurisprudenza ivi citata).

42 Ciò premesso, occorre rilevare che le norme di cooperazione previste nel RGPD non si rivolgono alle autorità nazionali garanti della concorrenza ma disciplinano la cooperazione tra le autorità nazionali di controllo interessate e l'autorità di controllo capofila nonché, se del caso, la cooperazione di tali autorità con il comitato europeo per la protezione dei dati e la Commissione.

43 Infatti, né il RGPD né altri strumenti del diritto dell'Unione stabiliscono norme specifiche sulla cooperazione tra un'autorità nazionale garante della concorrenza e le autorità nazionali di controllo interessate o l'autorità di controllo capofila. Inoltre, nessuna disposizione di detto regolamento vieta alle autorità nazionali garanti della concorrenza di constatare, nell'ambito dell'esercizio delle loro funzioni, la non conformità a tale regolamento di un trattamento di dati effettuato da un'impresa in posizione dominante e tale da costituire un abuso di tale posizione.

44 A tal riguardo, occorre precisare, in primo luogo, che le autorità di controllo, da un lato, e le autorità nazionali garanti della concorrenza, dall'altro, esercitano funzioni diverse e perseguono obiettivi e compiti ad esse propri.

45 Infatti, da un lato, come indicato al punto 38 della presente sentenza, in forza dell'articolo 51, paragrafi 1 e 2, nonché dell'articolo 57, paragrafo 1, lettere a) e g), del RGPD, il compito principale dell'autorità di controllo è quello di controllare l'applicazione di detto regolamento e di vigilare sul suo rispetto, contribuendo al contempo alla sua coerente applicazione nell'ambito dell'Unione, e ciò al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei loro dati personali nonché di agevolare la libera circolazione di tali dati all'interno dell'Unione. A tal fine, come ricordato al punto 39 della presente sentenza, l'autorità di controllo dispone dei diversi poteri che le sono conferiti in forza dell'articolo 58 del RGPD.

46 Dal canto loro, ai sensi dell'articolo 5 del regolamento n. 1/2003, le autorità nazionali garanti della concorrenza sono segnatamente competenti ad adottare decisioni che constatino un abuso di posizione dominante da parte di un'impresa, ai sensi dell'articolo 102 TFUE, il cui obiettivo consiste nell'istituire un regime atto a garantire che la concorrenza non sia falsata nel mercato interno, tenuto conto anche delle conseguenze di un tale abuso per i consumatori di tale mercato.

47 Come rilevato in sostanza dall'avvocato generale al paragrafo 23 delle sue conclusioni, nell'ambito dell'adozione di una decisione di questo tipo, un'autorità garante della concorrenza deve valutare, sulla base di tutte le circostanze del caso di specie, se il comportamento dell'impresa in posizione dominante abbia l'effetto di ostacolare, ricorrendo a mezzi diversi da quelli su cui si impernia la concorrenza normale tra prodotti o servizi, la conservazione del grado di concorrenza esistente sul mercato o lo sviluppo di detta concorrenza (v., in tal senso, sentenza del 25 marzo 2021, D.T./Commissione, C-152/19 P, EU:C:2021:238, punti 41 e 42). A tal riguardo, la conformità o non conformità di detto comportamento alle disposizioni del RGPD può costituire, se del caso, un importante indizio fra le circostanze rilevanti del caso di specie per stabilire se siffatto comportamento costituisca un ricorso a mezzi su cui s'impernia la concorrenza normale nonché per valutare le conseguenze di una determinata pratica sul mercato o per i consumatori.

48 Ne consegue che, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa su un dato mercato, può risultare necessario che l'autorità garante della concorrenza dello Stato membro interessato

esamini anche la conformità del comportamento di tale impresa a norme diverse da quelle rientranti nel diritto della concorrenza, quali le norme in materia di protezione dei dati personali previste dal RGPD.

49 Orbene, tenuto conto dei diversi obiettivi perseguiti dalle norme stabilite in materia di concorrenza, in particolare dall'articolo 102 TFUE, da un lato, e da quelle previste in materia di protezione dei dati personali in forza del RGPD, dall'altro, occorre constatare che, quando un'autorità nazionale garante della concorrenza rileva una violazione di questo regolamento nell'ambito della constatazione di un abuso di posizione dominante, essa non si sostituisce alle autorità di controllo. In particolare, l'autorità nazionale garante della concorrenza non controlla l'applicazione né assicura il rispetto di tale regolamento per le finalità di cui all'articolo 51, paragrafo 1, di quest'ultimo, vale a dire al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali e di facilitare la libera circolazione di questi ultimi all'interno dell'Unione. Inoltre, limitandosi a rilevare la non conformità al RGPD di un trattamento di dati al solo scopo di constatare un abuso di posizione dominante ed imponendo misure volte a far cessare tale abuso sul fondamento di una base giuridica derivante dal diritto della concorrenza, detta autorità non esercita alcuno dei compiti di cui all'articolo 57 di tale regolamento, né fa uso dei poteri riservati all'autorità di controllo in forza dell'articolo 58 del medesimo regolamento.

50 Si deve peraltro constatare che l'accesso ai dati personali nonché il loro sfruttamento rivestono un'importanza fondamentale nell'ambito dell'economia digitale. Tale importanza è illustrata, nell'ambito della controversia di cui al procedimento principale, dal modello economico su cui si fonda il social network Facebook, il quale prevede, come ricordato al punto 27 della presente sentenza, il finanziamento mediante la commercializzazione di messaggi pubblicitari personalizzati in funzione di profili di utente configurati sulla base di dati personali raccolti da M.P.I.

51 Come sottolineato in particolare dalla Commissione, l'accesso ai dati personali e la possibilità di trattamento di tali dati sono diventati un parametro significativo della concorrenza fra imprese dell'economia digitale. Pertanto, escludere le norme in materia di protezione dei dati personali dal contesto giuridico che le autorità garanti della concorrenza devono prendere in considerazione in sede di esame di un abuso di posizione dominante ignorerebbe la realtà di tale evoluzione economica e potrebbe pregiudicare l'effettività del diritto della concorrenza all'interno dell'Unione.

52 Occorre tuttavia rilevare, in secondo luogo, che, nel caso in cui un'autorità nazionale garante della concorrenza ritenga necessario pronunciarsi, nell'ambito di una decisione relativa ad un abuso di posizione dominante, sulla conformità o sulla non conformità al RGPD di un trattamento di dati personali effettuato dall'impresa in questione, tale autorità e l'autorità di controllo interessata o, se del caso, l'autorità di controllo capofila competente ai sensi di tale regolamento devono cooperare tra loro al fine di garantire un'applicazione coerente di tale regolamento.

53 Infatti, se è vero che, come rilevato ai punti 42 e 43 della presente sentenza, né il RGPD né alcun altro strumento del diritto dell'Unione prevedono norme specifiche a tal riguardo, ciò non toglie che, come sostanzialmente rilevato dall'avvocato generale al paragrafo 28 delle sue conclusioni, quando applicano il RGPD, le diverse autorità nazionali coinvolte sono tutte vincolate dal principio di leale cooperazione sancito all'articolo 4, paragrafo 3, TUE. Secondo una giurisprudenza costante, in forza di tale principio, nelle materie rientranti nel diritto dell'Unione, gli Stati membri, ivi incluse le loro autorità amministrative, devono rispettarsi ed assistersi reciprocamente nell'adempimento dei compiti derivanti dai Trattati, adottare ogni misura atta ad assicurare l'esecuzione degli obblighi conseguenti, in particolare, agli atti delle istituzioni dell'Unione, nonché astenersi da qualsiasi misura che rischi di mettere in pericolo la realizzazione degli obiettivi dell'Unione (v., in tal senso, sentenze del 7 novembre 2013, U.N., C-518/11, EU:C:2013:709, punto 59, nonché del 1° agosto 2022, S.W., C-14/21 e C-15/21, EU:C:2022:604, punto 156).

54 Pertanto, alla luce di tale principio, quando le autorità nazionali garanti della concorrenza sono chiamate, nell'esercizio delle loro competenze, ad esaminare la conformità di un comportamento di un'impresa alle disposizioni del RGPD, esse devono concertarsi e cooperare lealmente con le autorità nazionali di controllo interessate oppure con l'autorità di controllo capofila; tutte queste autorità sono quindi tenute, in tale contesto, a rispettare i loro rispettivi poteri e competenze, così da rispettare gli obblighi derivanti dal RGPD nonché gli obiettivi di tale regolamento e da preservare il loro effetto utile.

55 L'esame, da parte di un'autorità garante della concorrenza, di un comportamento di un'impresa alla luce delle norme del RGPD può comportare, infatti, il rischio di divergenze fra tale autorità garante della concorrenza e le autorità di controllo in merito all'interpretazione di tale regolamento.

56 Ne consegue che, qualora, nell'ambito dell'esame diretto a constatare un abuso di posizione dominante ai sensi dell'articolo 102 TFUE da parte di un'impresa, un'autorità nazionale garante della concorrenza ritenga che sia necessario esaminare la conformità di un comportamento di tale impresa alle disposizioni del RGPD, detta autorità deve verificare se tale comportamento o

un comportamento simile sia già stato oggetto di una decisione da parte dell'autorità nazionale di controllo competente o dell'autorità di controllo capofila o, ancora, della Corte. Se così fosse, l'autorità nazionale garante della concorrenza non potrebbe discostarsene, pur restando libera di trarne le proprie conclusioni sotto il profilo dell'applicazione del diritto della concorrenza.

57 Laddove nutra dubbi sulla portata della valutazione effettuata dall'autorità nazionale di controllo competente o dall'autorità di controllo capofila, laddove il comportamento di cui trattasi o un comportamento simile sia, al contempo, oggetto di esame da parte di tali autorità, o, ancora, laddove, in assenza di un'indagine di dette autorità, ritenga che un comportamento di un'impresa non sia conforme alle disposizioni del RGPD, l'autorità nazionale garante della concorrenza deve consultare tali autorità e chiederne la cooperazione, al fine di fugare i propri dubbi o di determinare se si debba attendere l'adozione di una decisione da parte dell'autorità di controllo interessata prima di iniziare la propria valutazione.

58 Dal canto suo, l'autorità di controllo, quando riceve una richiesta di informazioni o di cooperazione da parte di un'autorità nazionale garante della concorrenza, deve rispondere a tale richiesta entro un termine ragionevole, comunicando a quest'ultima le informazioni di cui dispone che possano consentire di fugare i dubbi di tale autorità sulla portata della valutazione effettuata dall'autorità di controllo o, se del caso, informando l'autorità nazionale garante della concorrenza se intende avviare il procedimento di cooperazione con le altre autorità di controllo interessate o con l'autorità di controllo capofila, conformemente agli articoli 60 e seguenti del RGPD, al fine di giungere a una decisione volta a constatare la conformità o la non conformità della condotta in questione a tale regolamento.

59 In assenza di risposta da parte dell'autorità di controllo interpellata entro un termine ragionevole, l'autorità nazionale garante della concorrenza può proseguire la propria indagine. Ciò vale anche nel caso in cui l'autorità nazionale di controllo competente e l'autorità di controllo capofila non sollevino obiezioni a che si prosegua tale indagine senza attendere l'adozione di una loro decisione.

60 Nel caso di specie, dal fascicolo agli atti della Corte risulta che, nel corso dei mesi di ottobre e novembre 2018, ossia prima dell'adozione della decisione del 6 febbraio 2019, l'autorità federale garante della concorrenza ha contattato il Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) (commissario federale per la protezione dei dati e la libertà d'informazione, Germania), lo Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (commissario per la protezione dei dati e la libertà d'informazione di Amburgo, Germania), competente riguardo a F.D., nonché la Data Protection Commission (DPC) (autorità per la protezione dei dati, Irlanda), per informare tali autorità del suo intervento. Inoltre, consta che l'autorità federale garante della concorrenza ha ottenuto la conferma che dette autorità non stavano conducendo alcuna indagine riguardo a fatti simili a quelli in causa nel procedimento principale, ed esse non hanno sollevato alcuna obiezione riguardo al suo intervento. Infine, ai punti 555 e 556 della sua decisione del 6 febbraio 2019, l'autorità federale garante della concorrenza ha fatto espressamente riferimento a tale cooperazione.

61 Date tali circostanze, e ferme restando le verifiche che spetta al giudice del rinvio effettuare, l'autorità federale garante della concorrenza sembra aver ottemperato ai suoi obblighi di leale cooperazione con le autorità di controllo nazionali interessate nonché con l'autorità di controllo capofila.

62 In considerazione di quanto precede, occorre rispondere alle questioni prima e settima dichiarando che gli articoli 51 e seguenti del RGPD nonché l'articolo 4, paragrafo 3, TUE devono essere interpretati nel senso che, fermo restando il rispetto del suo obbligo di leale cooperazione con le autorità di controllo, un'autorità garante della concorrenza di uno Stato membro può constatare, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa, ai sensi dell'articolo 102 TFUE, che le condizioni generali d'uso di tale impresa relative al trattamento dei dati personali e la loro applicazione non sono conformi a detto regolamento, qualora tale constatazione sia necessaria per accertare l'esistenza di un tale abuso.

63 Alla luce di tale obbligo di leale cooperazione, l'autorità nazionale garante della concorrenza non può discostarsi da una decisione dell'autorità nazionale di controllo competente o dell'autorità di controllo capofila competente riguardante tali condizioni generali o condizioni generali analoghe. Laddove nutra dubbi sulla portata di tale decisione, laddove dette condizioni o condizioni analoghe siano, al contempo, oggetto di esame da parte di tali autorità, o, ancora, laddove, in assenza di un'indagine o di una decisione di dette autorità, ritenga che le condizioni in questione non siano conformi al RGPD, l'autorità nazionale garante della concorrenza deve consultare dette autorità di controllo e chiederne la cooperazione, al fine di fugare i propri dubbi o di determinare se si debba attendere l'adozione di una decisione da parte di tali autorità prima di iniziare la propria valutazione. In assenza di obiezioni o di risposta di queste ultime entro un termine ragionevole, l'autorità nazionale garante della concorrenza può proseguire la propria indagine.

Sulla seconda questione

64 Con la sua seconda questione, lettera a), il giudice del rinvio chiede, in sostanza, se l'articolo 9, paragrafo 1, del RGPD debba essere interpretato nel senso che, nel caso in cui un utente di un social network online consulti siti Internet o applicazioni attinenti a una o più delle categorie indicate in tale disposizione e, se del caso, vi inserisca dati iscrivendosi o effettuando ordini online, il trattamento di dati personali da parte dell'operatore di tale social network online, consistente nel raccogliere, tramite interfacce integrate, cookie o simili tecnologie di registrazione, i dati risultanti dalla consultazione di tali siti e di tali applicazioni nonché i dati inseriti dall'utente, nel mettere in relazione l'insieme di tali dati con l'account del social network di quest'ultimo e nell'utilizzare detti dati, deve essere considerato un "trattamento di categorie particolari di dati personali" ai sensi di detta disposizione, il quale è vietato in linea di principio, fatte salve le deroghe previste dal paragrafo 2 di tale articolo 9.

65 In caso di risposta affermativa, il giudice del rinvio chiede, in sostanza, con la sua seconda questione, lettera b), se l'articolo 9, paragrafo 2, lettera e), del RGPD debba essere interpretato nel senso che, qualora un utente di un social network online consulti siti Internet o applicazioni collegate alle categorie indicate all'articolo 9, paragrafo 1, del RGPD, inserisca dati su tali siti o applicazioni, o attivi pulsanti di selezione integrati in questi ultimi, quali i pulsanti "Mi piace" o "Condividi" o i pulsanti che consentono all'utente di identificarsi su tali siti o tali applicazioni utilizzando gli identificativi di connessione legati al suo account di utente del social network online, il suo numero di telefono o il suo indirizzo di posta elettronica, si ritiene che egli abbia manifestamente reso pubblici, ai sensi della prima di tali disposizioni, i dati raccolti in tale occasione dall'operatore di tale social network online mediante cookie o simili tecnologie di registrazione.

Sulla seconda questione, lettera a)

66 Il considerando 51 del RGPD enuncia che i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali meritano una specifica protezione, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per tali diritti e tali libertà fondamentali. Tale considerando precisa che dati personali di questo tipo non dovrebbero essere oggetto di trattamento, a meno che quest'ultimo non sia consentito nei casi specifici previsti dal medesimo regolamento.

67 In tale contesto, l'articolo 9, paragrafo 1, del RGPD sancisce il principio del divieto di trattamento riguardante talune categorie particolari di dati personali da esso menzionati. Si tratta, in particolare, di dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose nonché di dati relativi alla salute, alla vita sessuale o all'orientamento sessuale di una persona fisica.

68 Ai fini dell'applicazione dell'articolo 9, paragrafo 1, del RGPD, occorre verificare, nel caso di un trattamento di dati personali effettuato dall'operatore di un social network online, se questi dati siano tali da rivelare informazioni rientranti in una delle categorie menzionate da tale disposizione, a prescindere dal fatto che tali informazioni riguardino un utente di tale social network o qualsiasi altra persona fisica. In caso affermativo, un siffatto trattamento di dati personali sarebbe dunque vietato, fatte salve le deroghe previste all'articolo 9, paragrafo 2, del RGPD.

69 Come sostanzialmente rilevato dall'avvocato generale ai paragrafi 40 e 41 delle sue conclusioni, tale divieto di principio, previsto all'articolo 9, paragrafo 1, del RGPD, è indipendente dalla questione se l'informazione rivelata dal trattamento di cui trattasi sia esatta o meno e se il titolare del trattamento agisca allo scopo di ottenere informazioni rientranti in una delle categorie particolari previste da tale disposizione.

70 Infatti, tenuto conto dei rischi significativi per le libertà fondamentali e i diritti fondamentali degli interessati, generati da qualsiasi trattamento di dati personali rientranti nelle categorie di cui all'articolo 9, paragrafo 1, del RGPD, quest'ultimo ha lo scopo di vietare tali trattamenti, a prescindere da quale sia la loro finalità dichiarata.

71 Nel caso di specie, il trattamento in causa nel procedimento principale effettuato da M.P.I. consiste nel raccogliere dati personali degli utenti del social network Facebook quando essi consultano siti Internet o applicazioni – ivi inclusi quelli che possano rivelare informazioni rientranti in una o più delle categorie di cui all'articolo 9, paragrafo 1, del RGPD – e, se del caso, vi inseriscono informazioni iscrivendosi o effettuando ordini online, nel mettere in relazione tali dati con l'account del social network di tali utenti e, infine, nell'utilizzare detti dati.

72 A tal riguardo, spetterà al giudice del rinvio stabilire se i dati in tal modo raccolti, di per sé oppure mediante la loro messa in relazione con gli account Facebook degli utenti interessati, consentano effettivamente di rivelare informazioni di questo tipo, a prescindere dal fatto che tali informazioni riguardino un utente di tale social network oppure qualsiasi altra persona fisica. Tuttavia, tenuto conto degli interrogativi sollevati da tale giudice, occorre precisare che, fatte salve le verifiche che quest'ultimo è tenuto ad effettuare, pare che il trattamento dei dati relativi alla consultazione dei siti Internet o delle applicazioni di cui trattasi possa, in determinati casi, rivelare siffatte informazioni, senza che sia necessario che detti utenti vi inseriscano informazioni iscrivendosi oppure effettuando ordini online.

73 Alla luce di quanto precede, occorre rispondere alla seconda questione, lettera a), dichiarando che l'articolo 9, paragrafo 1, del RGPD deve essere interpretato nel senso che, nel caso in cui un utente di un social network online consulti siti Internet oppure applicazioni correlati a una o più delle categorie menzionate da tale disposizione e, se del caso, inserisca in essi dati, iscrivendosi oppure effettuando ordini online, il trattamento di dati personali da parte dell'operatore di tale social network online – consistente nel raccogliere, tramite interfacce integrate, cookie o simili tecnologie di registrazione, dati risultanti dalla consultazione di tali siti e di tali applicazioni nonché i dati inseriti dall'utente, nel mettere in relazione l'insieme di tali dati con l'account del social network di quest'ultimo e nell'utilizzare detti dati – deve essere considerato un "trattamento di categorie particolari di dati personali" ai sensi di detta disposizione, il quale è in linea di principio vietato, fatte salve le deroghe previste da detto articolo 9, paragrafo 2, qualora tale trattamento di dati sia tale da rivelare informazioni rientranti in una di dette categorie, a prescindere dal fatto che tali informazioni riguardino un utente di tale social network o qualsiasi altra persona fisica.

Sulla seconda questione, lettera b)

74 Per quanto riguarda la seconda questione, lettera b), come riformulata al punto 65 della presente sentenza e relativa alla deroga prevista all'articolo 9, paragrafo 2, lettera e), del RGPD, va ricordato che, in forza di tale disposizione, il divieto di qualsiasi trattamento riguardante categorie particolari di dati personali, sancito in via di principio da detto articolo 9, paragrafo 1, non si applica nel caso in cui il trattamento riguardi dati personali "resi manifestamente pubblici dall'interessato".

75 In via preliminare, occorre rilevare, da un lato, che tale deroga si applica ai soli dati manifestamente resi pubblici "dall'interessato". Pertanto, essa non è applicabile ai dati riguardanti persone diverse da quella che ha reso pubblici detti dati.

76 Dall'altro lato, poiché prevede un'eccezione al principio del divieto di trattamento di categorie particolari di dati personali, l'articolo 9, paragrafo 2, del RGPD deve essere interpretato restrittivamente (v., in tal senso, sentenza del 17 settembre 2014, B.A., C-3/13, EU:C:2014:2227, punto 24 e giurisprudenza ivi citata, nonché del 6 giugno 2019, W., C-361/18, EU:C:2019:473, punto 43 e giurisprudenza ivi citata).

77 Ne consegue che, ai fini dell'applicazione dell'eccezione prevista all'articolo 9, paragrafo 2, lettera e), del RGPD, si deve verificare se l'interessato abbia inteso, in modo esplicito e con un atto positivo chiaro, rendere accessibili al pubblico i dati personali in questione.

78 Sotto tale profilo, per quanto riguarda, da un lato, la consultazione di siti Internet o di applicazioni correlati ad una o più delle categorie di cui all'articolo 9, paragrafo 1, del RGPD, si deve constatare che, con essa, l'utente interessato non intende in alcun modo rendere pubblico il fatto di aver consultato tali siti o tali applicazioni e i dati relativi a tale consultazione che possono essere ricollegati alla sua persona. Infatti, tale utente può tutt'al più attendersi che il gestore del sito o dell'applicazione abbia accesso a tali dati e che li condivida, se del caso e fermo restando il consenso esplicito prestato da tale utente, con taluni terzi e non con il pubblico.

79 Pertanto, dalla mera consultazione di tali siti Internet o applicazioni da parte di un utente non si può dedurre che detti dati personali siano stati manifestamente resi pubblici da tale utente, ai sensi dell'articolo 9, paragrafo 2, lettera e), del RGPD.

80 Dall'altro lato, per quanto riguarda le attività consistenti nell'inserire dati in tali siti Internet o applicazioni nonché nell'attivare pulsanti di selezione in essi integrati, quali i pulsanti "Mi piace" o "Condividi" o i pulsanti che consentono all'utente di identificarsi su un sito Internet o su un'applicazione utilizzando gli identificativi di connessione collegati al suo account utente Facebook, il suo numero di telefono o il suo indirizzo di posta elettronica, occorre rilevare che tali attività comportano un'interazione fra tale utente e il sito Internet o l'applicazione in questione e, se del caso, il sito Internet del social network online, interazione le cui forme di pubblicità possono variare in quanto possono essere oggetto di una impostazione individuale di parametri da parte di detto utente.

81 In tali circostanze, è compito del giudice del rinvio verificare se gli utenti interessati abbiano la possibilità di decidere, sulla base di un'impostazione di parametri effettuata con cognizione di causa, di rendere i dati inseriti nei siti Internet o nelle applicazioni in questione, nonché i dati risultanti dall'attivazione dei pulsanti di selezione in essi integrati, accessibili al pubblico o, invece, a un numero più o meno limitato di persone selezionate.

82 Qualora dispongano effettivamente di una tale scelta, si può ritenere che gli utenti interessati, quando inseriscono volontariamente dati in un sito Internet o in un'applicazione o quando attivano pulsanti di selezione integrati in questi ultimi, rendano manifestamente pubblici dati che li riguardano, ai sensi dell'articolo 9, paragrafo 2, lettera e), del RGPD, soltanto se, sulla base di un'impostazione individuale di parametri effettuata con piena cognizione di causa, tali utenti abbiano chiaramente espresso la loro scelta che tali dati siano resi accessibili a un numero illimitato di persone, circostanza che spetta al giudice del rinvio verificare.

83 Per contro, nel caso in cui non venga proposta un'impostazione individuale di parametri di questo tipo, si deve considerare, alla luce di quanto esposto al punto 77 della presente sentenza, che, per poter ritenere che

gli utenti abbiano manifestamente reso pubblici dati allorché inseriscono volontariamente dati in un sito Internet oppure in un'applicazione o attivano pulsanti di selezione in questi ultimi integrati, essi devono aver esplicitamente acconsentito, sulla base di un'informazione espressa fornita da tale sito o da tale applicazione prima di tale inserimento o attivazione, a che i suddetti dati possano essere visualizzati da chiunque abbia accesso a detto sito o a detta applicazione.

84 Alla luce di quanto precede, occorre rispondere alla seconda questione, lettera b), dichiarando che l'articolo 9, paragrafo 2, lettera e), del RGPD deve essere interpretato nel senso che un utente di un social network online, allorché consulta siti Internet oppure applicazioni correlati ad una o più delle categorie menzionate all'articolo 9, paragrafo 1, del RGPD, non rende manifestamente pubbliche, ai sensi della prima di tali disposizioni, i dati relativi a tale consultazione, raccolti dall'operatore di detto social network online mediante cookie o simili tecnologie di registrazione.

85 Quando inserisce dati in tali siti Internet o applicazioni nonché quando attiva pulsanti di selezione integrati in questi ultimi, come i pulsanti "Mi piace" o "Condividi" o i pulsanti che consentono all'utente di identificarsi su un sito Internet o su un'applicazione utilizzando gli identificativi di connessione collegati al suo account di utente del social network, il suo numero di telefono o il suo indirizzo di posta elettronica, tale utente rende manifestamente pubblici, ai sensi di detto articolo 9, paragrafo 2, lettera e), del RGPD, i dati così inseriti o risultanti dall'attivazione di tali pulsanti soltanto se abbia esplicitamente espresso preliminarmente, se del caso sulla base di un'impostazione individuale di parametri effettuata con piena cognizione di causa, la sua scelta di rendere i dati che lo riguardano pubblicamente accessibili a un numero illimitato di persone.

Sulle questioni dalla terza alla quinta

86 Con la sua terza e quarta questione, che è opportuno esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se, e a quali condizioni, l'articolo 6, paragrafo 1, primo comma, lettere b) e f), del RGPD debba essere interpretato nel senso che il trattamento di dati personali effettuato da un operatore di un social network online - consistente nel raccogliere dati degli utenti di tale social network provenienti da altri servizi del gruppo al quale appartiene tale operatore oppure derivanti dalla consultazione, da parte di tali utenti, di siti Internet o di applicazioni di terzi, nel mettere in relazione tali dati con l'account del social network di detti utenti e nell'utilizzare detti dati - può essere considerato necessario per l'esecuzione di un contratto del quale gli interessati sono parti, ai sensi della lettera b), oppure per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, ai sensi della lettera f). Detto giudice si chiede in particolare se, a tal fine, alcuni interessi da esso esplicitamente menzionati costituiscano un "legittimo interesse" ai sensi di quest'ultima disposizione.

87 Con la quinta questione, il giudice del rinvio chiede, in sostanza, se l'articolo 6, paragrafo 1, primo comma, lettere da c) a e), del RGPD debba essere interpretato nel senso che un simile trattamento di dati personali può essere considerato necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento, ai sensi della lettera c), per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, ai sensi della lettera d), o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ai sensi della lettera e), qualora il trattamento sia effettuato, rispettivamente, per rispondere a una legittima richiesta di determinati dati, per contrastare comportamenti dannosi e promuovere la sicurezza e per ricerche a beneficio della società e per promuovere protezione, integrità e sicurezza.

Osservazioni preliminari

88 In via preliminare, occorre osservare, in primo luogo, che le questioni dalla terza alla quinta sono sollevate in ragione del fatto che, secondo le constatazioni dell'autorità federale garante della concorrenza nella sua decisione del 6 febbraio 2019, non si può ritenere che gli utenti del social network Facebook abbiano prestato il loro consenso al trattamento dei loro dati in causa nel procedimento principale, ai sensi dell'articolo 6, paragrafo 1, primo comma, lettera a), e dell'articolo 9, paragrafo 2, lettera a), del RGPD. È dunque in tale contesto che il giudice del rinvio, pur interrogando la Corte con la sua sesta questione rispetto a tale premessa, ritiene di dover verificare se tale trattamento corrisponda a una delle altre condizioni di liceità di cui a detto articolo 6, paragrafo 1, primo comma, lettere da b) a f), di tale regolamento.

89 In tale contesto, occorre rilevare che le operazioni di raccolta, di collegamento e di utilizzo dei dati, prese in considerazione nelle questioni dalla terza alla quinta, sono tali da includere al contempo dati sensibili ai sensi dell'articolo 9, paragrafo 1, del RGPD e dati non sensibili. Orbene, occorre precisare che, nel caso in cui un insieme di dati contenente al contempo dati sensibili e dati non sensibili sia oggetto di siffatte operazioni e segnatamente sia raccolto in blocco senza che i dati possano essere dissociati gli uni dagli altri al momento di tale raccolta, il trattamento di tale insieme di dati deve essere considerato vietato, ai sensi dell'articolo 9, paragrafo 1, del RGPD, nella misura in cui contenga almeno un dato sensibile e non sia applicabile nessuna delle deroghe di cui all'articolo 9, paragrafo 2, del medesimo regolamento.

90 In secondo luogo, al fine di rispondere alle questioni dalla terza alla quinta, occorre ricordare che l'articolo 6, paragrafo 1, primo comma, del RGPD prevede un elenco esaustivo e tassativo dei casi nei quali un trattamento di dati personali può essere considerato lecito. Pertanto, per poter essere considerato lecito, un trattamento deve rientrare in uno dei casi previsti da tale disposizione [sentenza del 22 giugno 2021, L.R.S. (Punti di penalità), C-439/19, EU:C:2021:504, punto 99 e giurisprudenza ivi citata].
91 Ai sensi dell'articolo 6, paragrafo 1, primo comma, lettera a), di tale regolamento, il trattamento di dati personali è lecito se, e nella misura in cui, l'interessato vi ha acconsentito per una o più finalità specifiche.
92 In mancanza di un siffatto consenso, o qualora tale consenso non sia stato espresso in modo libero, specifico, informato e inequivocabile, ai sensi dell'articolo 4, punto 11, del RGPD, un trattamento di questo tipo è nondimeno giustificato qualora soddisfi uno dei requisiti di necessità menzionati all'articolo 6, paragrafo 1, primo comma, lettere da b) ad f), di detto regolamento.
93 In tale contesto, nella misura in cui consentono di rendere lecito un trattamento di dati personali effettuato in assenza del consenso dell'interessato, le giustificazioni previste da quest'ultima disposizione devono essere interpretate restrittivamente [v., in tal senso, sentenza del 24 febbraio 2022, Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali), C-175/20, EU:C:2022:124, punto 73 e giurisprudenza ivi citata].
94 Inoltre, la Corte ha considerato che, qualora si possa constatare che un trattamento di dati personali è necessario alla luce di una delle giustificazioni previste all'articolo 6, paragrafo 1, primo comma, lettere da b) a f), del RGPD, non occorre stabilire se tale trattamento rientri anche in un'altra di tali giustificazioni (v., in tal senso, sentenza del 1° agosto 2022, Vyriausioji tarnybinės etikos komisija, C-184/20, EU:C:2022:601, punto 71).
95 Occorre infine precisare che, conformemente all'articolo 5 del RGPD, è al titolare del trattamento che incombe l'onere di dimostrare che tali dati sono segnatamente raccolti per finalità determinate, esplicite e legittime e che essi sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Inoltre, in forza dell'articolo 13, paragrafo 1, lettera c), di tale regolamento, in caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento è tenuto ad informare quest'ultimo delle finalità del trattamento al quale sono destinati tali dati nonché della base giuridica di questo trattamento.
96 Anche se spetta al giudice del rinvio stabilire se i diversi elementi del trattamento in causa nel procedimento principale siano giustificati dall'uno o l'altro dei requisiti di cui all'articolo 6, paragrafo 1, primo comma, lettere da b) a f), del RGPD, la Corte può nondimeno fornirgli indicazioni utili al fine di consentirgli di dirimere la controversia di cui è investito.
Sulla terza e quarta questione
97 Per quanto riguarda, sotto un primo profilo, l'articolo 6, paragrafo 1, primo comma, lettera b), del RGPD, esso prevede che un trattamento di dati personali è lecito se è "necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso".
98 A tal riguardo, affinché un trattamento di dati personali sia considerato necessario all'esecuzione di un contratto, ai sensi di tale disposizione, esso deve essere oggettivamente indispensabile per realizzare una finalità che è parte integrante della prestazione contrattuale destinata all'interessato. Il responsabile del trattamento deve, quindi, essere in grado di dimostrare in che modo l'oggetto principale del contratto non potrebbe essere conseguito in assenza del trattamento di cui è causa.
99 La circostanza che un siffatto trattamento sia menzionato nel contratto oppure che esso sia soltanto utile per l'esecuzione di quest'ultimo è, di per sé, irrilevante al riguardo. Infatti, l'elemento determinante ai fini dell'applicazione della giustificazione di cui all'articolo 6, paragrafo 1, primo comma, lettera b), del RGPD è che il trattamento di dati personali effettuato dal titolare del trattamento sia essenziale per consentire la corretta esecuzione del contratto stipulato tra quest'ultimo e l'interessato e, pertanto, che non esistano altre soluzioni percorribili e meno invasive.
100 A tal riguardo, come rilevato dall'avvocato generale al paragrafo 54 delle sue conclusioni, se il contratto consiste in più servizi o in più elementi distinti di uno stesso servizio che possono essere prestati indipendentemente gli uni dagli altri, l'applicabilità dell'articolo 6, paragrafo 1, primo comma, lettera b), del RGPD deve essere valutata separatamente nel contesto di ciascuno di tali servizi.
101 Nel caso di specie, quanto alle giustificazioni idonee a rientrare nell'ambito di applicazione di tale disposizione, il giudice del rinvio fa riferimento – quali elementi diretti a garantire l'esecuzione adeguata del contratto concluso tra M.P.I. e i suoi utenti – alla personalizzazione dei contenuti nonché all'utilizzo omogeneo e fluido dei servizi propri del gruppo M.
102 Per quanto riguarda, in primo luogo, la giustificazione relativa alla personalizzazione dei contenuti, occorre rilevare che, sebbene tale personalizzazione sia utile per l'utente, in quanto gli consente in particolare di visualizzare un contenuto in larga misura corrispondente ai suoi interessi, resta il fatto che, salvo verifica del giudice del rinvio, la personalizzazione dei contenuti non appare necessaria per offrire a tale utente i servizi del social network online. Tali servizi possono, eventualmente, essergli forniti sotto forma di un'alternativa equivalente

che non implichi tale personalizzazione, che non è dunque oggettivamente indispensabile per una finalità che faccia parte integrante di detti servizi.
103 Per quanto riguarda, in secondo luogo, la giustificazione relativa all'utilizzo omogeneo e fluido dei servizi propri del gruppo M., dal fascicolo agli atti della Corte risulta che una persona non è tenuta a sottoscrivere i diversi servizi proposti dal gruppo M. per poter creare un account utente nel social network Facebook. Infatti, i diversi prodotti e servizi proposti da detto gruppo possono essere utilizzati indipendentemente gli uni dagli altri e l'utilizzo di ciascun prodotto o servizio si basa sulla sottoscrizione di un contratto d'uso distinto.
104 Pertanto, e salvo verifica del giudice del rinvio, un trattamento di dati personali provenienti da servizi diversi da quello del social network online, proposti dal gruppo M., non sembra essere necessario per consentire la fornitura di quest'ultimo servizio.
105 Per quanto riguarda, sotto un secondo profilo, l'articolo 6, paragrafo 1, primo comma, lettera f), del RGPD, esso prevede che un trattamento di dati personali è lecito se è "necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore".
106 Come già giudicato dalla Corte, detta disposizione prevede tre condizioni cumulative affinché i trattamenti di dati personali da essa considerati siano leciti, vale a dire, in primo luogo, il perseguimento di un legittimo interesse del titolare del trattamento o di terzi, in secondo luogo, la necessità del trattamento dei dati personali per la realizzazione del legittimo interesse perseguito e, in terzo luogo, la condizione che gli interessi o i diritti e le libertà fondamentali dell'interessato dalla tutela dei dati non prevalgano sul legittimo interesse del responsabile del trattamento o di terzi (sentenza del 17 giugno 2021, M.I.C.M., C-597/19, EU:C:2021:492, punto 106 e giurisprudenza ivi citata).
107 Per quanto riguarda, in primo luogo, la condizione relativa al perseguimento di un legittimo interesse, occorre precisare che, ai sensi dell'articolo 13, paragrafo 1, lettera d), del RGPD, spetta al titolare del trattamento, all'atto della raccolta presso l'interessato di dati che lo riguardano, indicargli i legittimi interessi perseguiti, qualora tale trattamento si basi sull'articolo 6, paragrafo 1, primo comma, lettera f), di tale regolamento.
108 Per quanto riguarda, in secondo luogo, la condizione relativa alla necessità del trattamento dei dati personali per la realizzazione del legittimo interesse perseguito, essa impone al giudice del rinvio di verificare che il legittimo interesse al trattamento dei dati perseguito non possa ragionevolmente essere raggiunto in modo altrettanto efficace mediante altri mezzi meno pregiudizievoli per i diritti fondamentali degli interessati, in particolare per i diritti al rispetto della vita privata e alla protezione dei dati personali garantiti agli articoli 7 e 8 della Carta [v., in tal senso, sentenza del 22 giugno 2021, L.R.S. (Punti di penalità), C-439/19, EU:C:2021:504, punto 110 e giurisprudenza ivi citata].
109 In tale contesto, occorre altresì ricordare che la condizione attinente alla necessità del trattamento deve essere esaminata unitamente al principio cosiddetto della "minimizzazione dei dati" sancito all'articolo 5, paragrafo 1, lettera c), del RGPD, secondo il quale i dati personali devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (v., in tal senso, sentenza dell'11 dicembre 2019, A.D.P. bloc M.S., C-708/18, EU:C:2019:1064, punto 48).
110 Per quanto riguarda, in terzo luogo, la condizione secondo cui gli interessi o i diritti e le libertà fondamentali dell'interessato non devono prevalere sul legittimo interesse del responsabile del trattamento o di terzi, la Corte ha già giudicato che ciò implica una ponderazione dei diritti e degli interessi contrapposti che dipende, in linea di principio, dalle circostanze del caso concreto e che, di conseguenza, spetta al giudice del rinvio effettuare tenendo conto di tali circostanze specifiche (sentenza del 17 giugno 2021, M.I.C.M., C-597/19, EU:C:2021:492, punto 111 e giurisprudenza ivi citata).
111 A tal riguardo, dal testo dell'articolo 6, paragrafo 1, primo comma, lettera f), del RGPD, risulta che, nell'ambito di siffatta ponderazione, è necessario prestare particolare attenzione alla situazione in cui l'interessato è un minore. Infatti, conformemente al considerando 38 di tale regolamento, i minori meritano una specifica protezione relativamente al trattamento dei loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione a un simile trattamento dei dati personali. Tale protezione particolare deve pertanto applicarsi, segnatamente, al trattamento di dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente o ancora di proposta di servizi direttamente riguardanti minori.
112 Inoltre, come risulta dal considerando 47 del RGPD, gli interessi e i diritti fondamentali dell'interessato possono in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un siffatto trattamento.
113 Nel caso di specie, quanto alle giustificazioni che possono rientrare nell'ambito di applicazione dell'articolo 6, paragrafo 1, primo comma, lettera f), del RGPD, il giudice del rinvio fa riferimento alla personalizzazione della pubblicità, alla sicurezza del network, al miglio-

ramento del prodotto, all'informazione delle autorità competenti per l'esercizio dell'azione penale e per l'esecuzione di pene, al fatto che l'utente sia un minorenne, alla ricerca e all'innovazione per finalità sociali nonché all'offerta, destinata agli inserzionisti e ad altri partner professionali, di servizi di comunicazione commerciale destinati all'utente e di strumenti di analisi che consentano a questi ultimi di valutare le loro prestazioni.

114 A tal riguardo, occorre anzitutto rilevare che la domanda di pronuncia pregiudiziale non contiene elementi esplicativi che permettano di comprendere in che modo la ricerca e l'innovazione per finalità sociali o il fatto che l'utente sia un minorenne possano giustificare, in quanto legittimi interessi ai sensi dell'articolo 6, paragrafo 1, primo comma, lettera f), del RGPD, la raccolta e l'utilizzo dei dati in questione. Pertanto, la Corte non è in grado di pronunciarsi su tale punto.

115 Per quanto concerne, in primo luogo, la personalizzazione della pubblicità, va rilevato che, secondo il considerando 47 di tale regolamento, il trattamento di dati personali per finalità di marketing diretto può essere considerato come effettuato per soddisfare un legittimo interesse del responsabile del trattamento.

116 Tuttavia, occorre altresì che un siffatto trattamento sia necessario per la realizzazione di tale interesse e che gli interessi o le libertà e i diritti fondamentali della persona interessata non prevalgano su di esso. Nell'ambito di siffatta ponderazione dei contrapposti diritti e interessi in gioco, vale a dire quelli del titolare del trattamento, da un lato, e quelli dell'interessato, dall'altro, si deve segnatamente tener conto, come rilevato al punto 112 della presente sentenza, delle ragionevoli aspettative dell'interessato, nonché della portata del trattamento in questione e dell'impatto di quest'ultimo su tale persona.

117 A tal riguardo, occorre rilevare che, malgrado la gratuità dei servizi di un social network online quale Facebook, l'utente di quest'ultimo non può ragionevolmente attendersi che, senza il suo consenso, l'operatore di tale social network tratti i suoi dati personali a fini di personalizzazione della pubblicità. In tali circostanze, si deve ritenere che i diritti fondamentali e gli interessi di tale utente prevalgano sull'interesse dell'operatore a tale personalizzazione della pubblicità mediante la quale egli finanzia la sua attività, cosicché il trattamento da quest'ultimo effettuato a tali fini non può rientrare nell'ambito di applicazione dell'articolo 6, paragrafo 1, primo comma, lettera f), del RGPD.

118 Inoltre, il trattamento in causa nel procedimento principale è particolarmente esteso, giacché verte su dati potenzialmente illimitati e ha un notevole impatto sull'utente, di cui M.P.I. controlla gran parte, se non la quasi totalità, delle attività online, il che può suscitare in quest'ultimo la sensazione di una continua sorveglianza della sua vita privata.

119 In secondo luogo, per quanto riguarda l'obiettivo di garantire la sicurezza del network, esso costituisce, come enunciato dal considerando 49 del RGPD, un legittimo interesse di M.P.I., idoneo a giustificare il trattamento di cui trattasi nel procedimento principale.

120 Tuttavia, in merito alla necessità di questo trattamento per la realizzazione di tale legittimo interesse, il giudice del rinvio dovrà verificare se e in quale misura il trattamento di dati personali raccolti a partire da fonti esterne al social network Facebook risulti effettivamente necessario per garantire che non sia compromessa la sicurezza interna di tale network.

121 In tale contesto, come rilevato ai punti 108 e 109 della presente sentenza, esso dovrà altresì verificare, da un lato, se il legittimo interesse al trattamento dei dati perseguito non possa ragionevolmente essere raggiunto in modo altrettanto efficace mediante altri mezzi meno pregiudizievoli per le libertà e i diritti fondamentali degli interessati, in particolare per i diritti al rispetto della vita privata e alla protezione dei dati personali garantiti dagli articoli 7 e 8 della Carta e, dall'altro, se sia rispettato il principio cosiddetto della "minimizzazione dei dati" sancito all'articolo 5, paragrafo 1, lettera c), del RGPD.

122 In terzo luogo, riguardo all'obiettivo diretto al miglioramento del prodotto, non si può escludere a priori che l'interesse del titolare del trattamento a migliorare il suo prodotto o servizio al fine di renderlo più performante e quindi più attrattivo possa costituire un legittimo interesse idoneo a giustificare un trattamento di dati personali e che un siffatto trattamento possa essere necessario per il perseguimento di tale interesse.

123 Tuttavia, fatta salva la valutazione finale che deve essere effettuata al riguardo dal giudice del rinvio, appare dubbio che, relativamente al trattamento di dati in causa nel procedimento principale, l'obiettivo diretto al miglioramento del prodotto possa – tenuto conto della portata di tale trattamento e del suo notevole impatto sull'utente, nonché della circostanza che quest'ultimo non possa ragionevolmente attendersi che tali dati siano trattati dalla M.P.I. – prevalere sui diritti fondamentali e sugli interessi di detto utente, tanto più nel caso in cui quest'ultimo sia minorenne.

124 In quarto luogo, relativamente all'obiettivo evocato dal giudice del rinvio, riguardante l'informazione delle autorità preposte all'esercizio di azioni penali e all'esecuzione di pene dirette ad evitare, a individuare e a perseguire reati, si deve constatare che tale obiettivo non può, in linea di principio, costituire un legittimo interesse perseguito dal titolare del trattamento, ai sensi dell'articolo 6, paragrafo 1, primo comma, lettera f), del RGPD. Infatti, un operatore privato come M.P.I. non può addurre un simile legittimo interesse, estraneo alla sua attività economica e commerciale. Per contro, detto

obiettivo può giustificare il trattamento effettuato da tale operatore, qualora sia oggettivamente necessario al rispetto di un obbligo legale al quale esso è soggetto.

125 Alla luce dell'insieme delle considerazioni che precedono, occorre rispondere alla terza e quarta questione dichiarando che l'articolo 6, paragrafo 1, primo comma, lettera b), del RGPD deve essere interpretato nel senso che il trattamento di dati personali effettuato da un operatore di un social network online – consistente nel raccogliere dati degli utenti di tale social network provenienti da altri servizi del gruppo al quale appartiene tale operatore oppure derivanti dalla consultazione, da parte di tali utenti, di siti Internet o di applicazioni di terzi, nel mettere in relazione tali dati con l'account del social network di detti utenti e nell'utilizzare detti dati – può essere considerato necessario per l'esecuzione di un contratto del quale gli interessati sono parti, ai sensi di tale disposizione, solo a condizione che detto trattamento sia oggettivamente indispensabile per realizzare una finalità che costituisce parte integrante della prestazione contrattuale destinata a quegli stessi utenti, cosicché l'oggetto principale del contratto non potrebbe essere conseguito in assenza di tale trattamento.

126 L'articolo 6, paragrafo 1, primo comma, lettera f), del RGPD deve essere interpretato nel senso che un trattamento siffatto può essere considerato necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, ai sensi di tale disposizione, solo a condizione che il suddetto operatore abbia indicato agli utenti presso i quali i dati sono stati raccolti un legittimo interesse perseguito dal loro trattamento, che tale trattamento sia effettuato entro i limiti di quanto strettamente necessario alla realizzazione di tale legittimo interesse e che dal contemperamento dei contrapposti interessi, alla luce di tutte le circostanze pertinenti, risulti che le libertà e i diritti fondamentali e gli interessi di tali utenti non prevalgono su detto legittimo interesse del titolare del trattamento o di terzi.

Sulla quinta questione

127 In primo luogo, nei limiti in cui tale questione riguarda l'articolo 6, paragrafo 1, primo comma, lettere c) ed e), del RGPD, occorre ricordare che, in forza di tale lettera c), un trattamento di dati personali è lecito se è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento. Inoltre, secondo tale lettera e), è altresì lecito il trattamento che è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento.

128 L'articolo 6, paragrafo 3, del RGPD precisa in particolare, con riferimento a queste due ipotesi di liceità, che il trattamento deve essere basato sul diritto dell'Unione o sul diritto dello Stato membro cui è soggetto il titolare del trattamento, e che tale base giuridica deve rispondere a un obiettivo di interesse pubblico ed essere proporzionata al legittimo obiettivo perseguito.

129 Nel caso di specie, il giudice del rinvio chiede se un trattamento di dati personali, come quello in causa nel procedimento principale, possa essere considerato giustificato alla luce dell'articolo 6, paragrafo 1, primo comma, lettera c), del RGPD, qualora miri a "rispondere ad una legittima richiesta di dati specifici", e, alla luce dell'articolo 6, paragrafo 1, primo comma, lettera e), di tale regolamento, quando abbia ad oggetto "ricerche a beneficio della società" e sia volto a "promuovere protezione, integrità e sicurezza".

130 Tuttavia, si deve constatare che detto giudice non ha fornito alla Corte elementi che le consentano di pronunciarsi concretamente al riguardo.

131 Tale giudice sarà dunque tenuto a verificare, alla luce delle condizioni indicate al punto 128 della presente sentenza, se il trattamento in questione possa essere considerato giustificato dalle finalità addotte.

132 In particolare, in considerazione di quanto rilevato al punto 124 della presente sentenza, quest'ultimo dovrà verificare, ai fini dell'applicazione dell'articolo 6, paragrafo 1, primo comma, lettera c), del RGPD, se M.P.I. sia soggetta a un obbligo legale di raccolta e di conservazione di dati personali in modo preventivo al fine di poter rispondere a qualsiasi richiesta di un'autorità nazionale diretta ad ottenere taluni dati relativi ai suoi utenti.

133 Analogamente, spetterà a detto giudice accertare, alla luce dell'articolo 6, paragrafo 1, primo comma, lettera e), del RGPD, se M.P.I. sia investita di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, in particolare al fine di assicurare ricerche a beneficio della società nonché di promuovere protezione, integrità e sicurezza, restando inteso che, data la natura e il carattere essenzialmente economico e commerciale della sua attività, appare poco probabile che tale operatore privato sia investito di un siffatto compito.

134 Inoltre, il giudice del rinvio dovrà, se del caso, verificare se, tenuto conto della portata del trattamento di dati effettuato da M.P.I. e del suo notevole impatto per gli utenti del social network Facebook, detto trattamento sia effettuato nei limiti dello stretto necessario.

135 Per quanto riguarda, in secondo luogo, l'articolo 6, paragrafo 1, primo comma, lettera d), del RGPD, tale disposizione prevede che il trattamento di dati personali è lecito se è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.

136 Come risulta dal considerando 46 di tale regolamento, tale disposizione riguarda la situazione particolare in cui il trattamento dei dati personali è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. A tal riguardo, questo considerando cita in particolare, a titolo di esempio,

i fini umanitari, quali il controllo dell'evoluzione delle epidemie e della loro diffusione nonché le situazioni di emergenza umanitaria, come i casi di catastrofi di origine naturale e umana.
137 Da tali esempi, nonché dall'interpretazione restrittiva dell'articolo 6, paragrafo 1, primo comma, lettera d), del RGPD che è opportuno adottare, risulta che, alla luce della natura dei servizi forniti dall'operatore di un social network online, un simile operatore, la cui attività riveste un carattere essenzialmente economico e commerciale, non può addurre la protezione di un interesse essenziale alla vita dei suoi utenti o di un'altra persona per giustificare, in assoluto e in modo puramente astratto e preventivo, la liceità di un trattamento di dati come quello di cui trattasi nel procedimento principale.
138 Alla luce di quanto precede, occorre rispondere alla quinta questione dichiarando che l'articolo 6, paragrafo 1, primo comma, lettera c), del RGPD deve essere interpretato nel senso che il trattamento di dati personali effettuato da un operatore di un social network online – consistente nel raccogliere dati degli utenti di tale social network provenienti da altri servizi del gruppo al quale appartiene tale operatore oppure derivanti dalla consultazione, da parte di tali utenti, di siti Internet o di applicazioni di terzi, nel mettere in relazione tali dati con l'account del social network di detti utenti e nell'utilizzare detti dati – è giustificato, ai sensi di tale disposizione, allorché è effettivamente necessario per adempiere un obbligo legale al quale il titolare del trattamento è soggetto, in forza di una disposizione del diritto dell'Unione o del diritto dello Stato membro interessato, tale base giuridica risponde ad un obiettivo di interesse pubblico ed è proporzionata all'obiettivo legittimo perseguito e tale trattamento è effettuato nei limiti dello stretto necessario.
139 L'articolo 6, paragrafo 1, primo comma, lettere d) ed e), del RGPD deve essere interpretato nel senso che un trattamento siffatto non può, in linea di principio e ferma restando la verifica che deve essere effettuata dal giudice del rinvio, essere considerato necessario alla salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, ai sensi della lettera d), oppure all'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ai sensi della lettera e).
Sulla sesta questione
140 Con la sesta questione, il giudice del rinvio chiede, in sostanza, se l'articolo 6, paragrafo 1, primo comma, lettera a), e l'articolo 9, paragrafo 2, lettera a), del RGPD debbano essere interpretati nel senso che si può ritenere che un consenso prestato dall'utente di un social network online all'operatore di tale social network soddisfi le condizioni di validità previste all'articolo 4, punto 11, di tale regolamento, in particolare quella secondo cui tale consenso deve essere prestato liberamente, qualora tale operatore occupi una posizione dominante sul mercato dei social network online.
141 L'articolo 6, paragrafo 1, primo comma, lettera a), e l'articolo 9, paragrafo 2, lettera a), del RGPD richiedono il consenso dell'interessato ai fini, rispettivamente, del trattamento, per una o più finalità specifiche, dei suoi dati personali e del trattamento di categorie particolari di dati considerati da tale articolo 9, paragrafo 1.
142 Dal canto suo, l'articolo 4, punto 11, del RGPD definisce la nozione di "consenso" come "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, [a] che i dati personali che lo riguardano siano oggetto di trattamento".
143 Dati gli interrogativi sollevati dal giudice del rinvio, occorre ricordare, in primo luogo, che, conformemente al considerando 42 del RGPD, il consenso non può essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio.
144 In secondo luogo, il considerando 43 di tale regolamento enuncia che, per garantire che il consenso sia prestato liberamente, è opportuno che quest'ultimo non costituisca un valido fondamento giuridico per il trattamento dei dati personali, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento. Tale considerando precisa altresì che si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso.
145 In terzo luogo, l'articolo 7, paragrafo 4, del RGPD prevede che, nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.
146 È sulla scorta di tali considerazioni che occorre rispondere alla sesta questione.
147 A tal riguardo, occorre constatare che, certamente, la circostanza che l'operatore di un social network online, in quanto titolare del trattamento, occupi una posizione dominante sul mercato dei social network non osta, di per sé, a che gli utenti di tale social network possano validamente acconsentire, ai sensi dell'articolo 4, punto 11, del RGPD, al trattamento dei loro dati personali effettuato da tale operatore.
148 Ciò nonostante, come rilevato, in sostanza, dall'avvocato generale al paragrafo 75 delle sue conclusioni,

una circostanza del genere deve essere presa in considerazione nella valutazione della validità e, in particolare, della libertà del consenso prestato dall'utente di detto social network, in quanto essa può incidere sulla libertà di scelta di tale utente, il quale potrebbe non essere in grado di rifiutare o di revocare il suo consenso senza subire pregiudizio, come indicato dal considerando 42 del RGPD.

149 Inoltre, l'esistenza di una siffatta posizione dominante è tale da creare uno squilibrio evidente, ai sensi del considerando 43 del RGPD, tra l'interessato e il titolare del trattamento, squilibrio che favorisce, segnatamente, l'imposizione di condizioni che non sono strettamente necessarie all'esecuzione del contratto, il che deve essere preso in considerazione conformemente all'articolo 7, paragrafo 4, di tale regolamento. In questo contesto, si deve ricordare che, come indicato ai punti da 102 a 104 della presente sentenza, non risulta, fatte salve le verifiche che il giudice nazionale dovrà effettuare, che il trattamento in causa nel procedimento principale sia strettamente necessario all'esecuzione del contratto tra M.P.I. e gli utenti del social network Facebook.

150 Pertanto, tali utenti devono disporre della libertà di rifiutare individualmente, nell'ambito della procedura contrattuale, di prestare il loro consenso a operazioni particolari di trattamento di dati non necessarie all'esecuzione del contratto, senza essere per questo tenuti a rinunciare integralmente alla fruizione del servizio offerto dall'operatore del social network online, il che implica che a detti utenti venga proposta, se del caso a fronte di un adeguato corrispettivo, un'alternativa equivalente non accompagnata da simili operazioni di trattamento di dati.

151 Oltre a ciò, tenuto conto della portata del trattamento dei dati in questione e del suo notevole impatto sugli utenti di tale network, nonché della circostanza che tali utenti non possano ragionevolmente attendersi che dati diversi da quelli relativi al loro comportamento all'interno del social network siano trattati dall'operatore di quest'ultimo, è opportuno, ai sensi di tale considerando 43, che possa essere prestato un consenso separato per il trattamento di questi ultimi dati, da un lato, e dei dati off Facebook, dall'altro. Spetta al giudice del rinvio verificare l'esistenza di una tale possibilità, in assenza della quale si deve presumere che il consenso di detti utenti al trattamento dei dati off Facebook non sia stato prestato liberamente.

152 Infine, occorre ricordare che, in forza dell'articolo 7, paragrafo 1, del RGPD, qualora il trattamento sia basato sul consenso, grava sul titolare del trattamento l'onere di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei dati personali che lo riguardano.

153 È alla luce dei suesposti criteri e di un esame dettagliato di tutte le circostanze del caso di specie che il giudice del rinvio dovrà stabilire se gli utenti del social network Facebook abbiano validamente e, in particolare, liberamente espresso il loro consenso al trattamento in causa nel procedimento principale.

154 Alla luce di quanto precede, occorre rispondere alla sesta questione dichiarando che l'articolo 6, paragrafo 1, primo comma, lettera a), e l'articolo 9, paragrafo 2, lettera a), del RGPD devono essere interpretati nel senso che la circostanza che l'operatore di un social network online occupi una posizione dominante sul mercato dei social network online non osta, di per sé, a che gli utenti di tale social network possano validamente acconsentire, ai sensi dell'articolo 4, punto 11, di detto regolamento, al trattamento dei loro dati personali effettuato da tale operatore. Tale circostanza costituisce nondimeno un elemento importante per determinare se il consenso sia stato effettivamente prestato validamente e, in particolare, liberamente, circostanza che spetta a detto operatore dimostrare.

Sulle spese

155 Nei confronti delle parti nel procedimento principale la presente causa costituisce un incidente sollevato dinanzi al giudice nazionale, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.

P.Q.M.

Per questi motivi, la Corte (Grande Sezione) dichiara:

1) Gli articoli 51 e seguenti del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) nonché l'articolo 4, paragrafo 3, TUE devono essere interpretati nel senso che:

fermo restando il rispetto del suo obbligo di leale cooperazione con le autorità di controllo, un'autorità garante della concorrenza di uno Stato membro può constatare, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa, ai sensi dell'articolo 102 TFUE, che le condizioni generali d'uso di tale impresa relative al trattamento dei dati personali e la loro applicazione non sono conformi a detto regolamento, qualora tale constatazione sia necessaria per accertare l'esistenza di un tale abuso.

Alla luce di tale obbligo di leale cooperazione, l'autorità nazionale garante della concorrenza non può discostarsi da una decisione dell'autorità nazionale di controllo competente o dell'autorità di controllo capofila competente che riguardi tali condizioni generali o condizioni

generali analoghe. Laddove nutra dubbi sulla portata di tale decisione, laddove dette condizioni o condizioni analoghe siano, al contempo, oggetto di esame da parte di tali autorità, o, ancora, laddove, in assenza di un'indagine o di una decisione di dette autorità, ritenga che le condizioni in questione non siano conformi al regolamento 2016/679, l'autorità nazionale garante della concorrenza deve consultare dette autorità di controllo e chiederne la cooperazione, al fine di fugare i propri dubbi o di determinare se si debba attendere l'adozione di una decisione da parte di tali autorità prima di iniziare la propria valutazione. In assenza di obiezioni o di risposta di queste ultime entro un termine ragionevole, l'autorità nazionale garante della concorrenza può proseguire la propria indagine.

2) L'articolo 9, paragrafo 1, del regolamento 2016/679

deve essere interpretato nel senso che:

nel caso in cui un utente di un social network online consulti siti Internet oppure applicazioni correlati a una o più delle categorie menzionate da tale disposizione e, se del caso, inserisca in essi dati, iscrivendosi oppure effettuando ordini online, il trattamento di dati personali da parte dell'operatore di tale social network online – consistente nel raccogliere, tramite interfacce integrate, cookie o simili tecnologie di registrazione, i dati risultanti dalla consultazione di tali siti e di tali applicazioni nonché i dati inseriti dall'utente, nel mettere in relazione l'insieme di tali dati con l'account del social network di quest'ultimo e nell'utilizzare detti dati – deve essere considerato un "trattamento di categorie particolari di dati personali" ai sensi di detta disposizione, il quale è in linea di principio vietato, fatte salve le deroghe previste da detto articolo 9, paragrafo 2, qualora tale trattamento di dati sia tale da rivelare informazioni rientranti in una di dette categorie, a prescindere dal fatto che tali informazioni riguardino un utente di tale social network o qualsiasi altra persona fisica.

3) L'articolo 9, paragrafo 2, lettera e), del regolamento 2016/679

deve essere interpretato nel senso che:

un utente di un social network online, allorché consulta siti Internet oppure applicazioni correlati a una o più delle categorie menzionate all'articolo 9, paragrafo 1, di detto regolamento, non rende manifestamente pubbliche, ai sensi della prima di tali disposizioni, i dati relativi a tale consultazione, raccolti dall'operatore di detto social network online mediante cookie o simili tecnologie di registrazione.

Quando inserisce dati in tali siti Internet o applicazioni nonché quando attiva pulsanti di selezione integrati in questi ultimi, come i pulsanti "Mi piace" o "Condividi" o i pulsanti che consentono all'utente di identificarsi su un sito Internet o su un'applicazione utilizzando gli identificativi di connessione collegati al suo account di utente del social network, il suo numero di telefono o il suo indirizzo di posta elettronica, tale utente rende manifestamente pubblici, ai sensi di detto articolo 9, paragrafo 2, lettera e), del RGPD, i dati così inseriti o risultanti dall'attivazione di tali pulsanti soltanto se abbia esplicitamente espresso preliminarmente, se del caso sulla base di un'impostazione individuale di parametri effettuata con piena cognizione di causa, la sua scelta di rendere i dati che lo riguardano pubblicamente accessibili a un numero illimitato di persone.

4) L'articolo 6, paragrafo 1, primo comma, lettera b), del regolamento 2016/679

deve essere interpretato nel senso che:

il trattamento di dati personali effettuato da un operatore di un social network online – consistente nel raccogliere dati degli utenti di tale social network provenienti da altri servizi del gruppo al quale appartiene tale operatore oppure derivanti dalla consultazione, da parte di tali utenti, di siti Internet o di applicazioni di terzi, nel mettere in relazione tali dati con l'account del social network di detti utenti e nell'utilizzare detti dati – può essere considerato necessario per l'esecuzione di un contratto del quale gli interessati sono parti, ai sensi di tale disposizione, solo a condizione che detto trattamento sia oggettivamente indispensabile per realizzare una finalità che costituisce parte integrante della prestazione contrattuale destinata a quegli stessi utenti, cosicché l'oggetto principale del contratto non potrebbe essere conseguito in assenza di tale trattamento.

5) L'articolo 6, paragrafo 1, primo comma, lettera f), del regolamento 2016/679

deve essere interpretato nel senso che:

il trattamento di dati personali effettuato da un operatore di un social network online – consistente nel raccogliere dati degli utenti di tale social network provenienti da altri servizi del gruppo al quale appartiene tale operatore oppure derivanti dalla consultazione, da parte di tali utenti, di siti Internet o di applicazioni di terzi, nel mettere in relazione tali dati con l'account del social network di detti utenti e nell'utilizzare detti dati – può essere considerato necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, ai sensi di tale disposizione, solo a condizione che il suddetto operatore abbia indicato agli utenti presso i quali i dati sono stati raccolti un legittimo interesse perseguito dal loro trattamento, che tale trattamento sia effettuato entro i limiti di quanto strettamente necessario alla realizzazione di tale legittimo interesse e che dal contemperamento dei contrapposti interessi, alla luce di tutte le circostanze pertinenti, risulti che le libertà e i diritti fondamentali e gli interessi di tali utenti non prevalgono su detto legittimo interesse del titolare del trattamento o di terzi.

6) L'articolo 6, paragrafo 1, primo comma, lettera c), del regolamento 2016/679
deve essere interpretato nel senso che:
il trattamento di dati personali effettuato da un operatore di un social network online – consistente nel raccogliere dati degli utenti di tale social network provenienti da altri servizi del gruppo al quale appartiene tale operatore oppure derivanti dalla consultazione, da parte di tali utenti, di siti Internet o di applicazioni di terzi, nel mettere in relazione tali dati con l'account del social network di detti utenti e nell'utilizzare detti dati – è giustificato, ai sensi di tale disposizione, allorché è effettivamente necessario per adempiere un obbligo legale al quale il titolare del trattamento è soggetto, in forza di una disposizione del diritto dell'Unione o del diritto dello Stato membro interessato, tale base giuridica risponde ad un obiettivo di interesse pubblico ed è proporzionata all'obiettivo legittimo perseguito e tale trattamento è effettuato nei limiti dello stretto necessario.
7) L'articolo 6, paragrafo 1, primo comma, lettere d) ed e), del regolamento 2016/679
deve essere interpretato nel senso che:
il trattamento di dati personali effettuato da un operatore di un social network online – consistente nel raccogliere dati degli utenti di tale social network provenienti da altri servizi del gruppo al quale appartiene tale operatore oppure derivanti dalla consultazione, da parte di tali utenti, di siti Internet o di applicazioni di terzi, nel mettere in relazione tali dati con l'account del social network di detti utenti e nell'utilizzare detti dati – non può, in linea di principio e ferma restando la verifica che deve essere effettuata dal giudice del rinvio, essere considerato necessario alla salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, ai sensi della lettera d), oppure all'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ai sensi della lettera e).
8) L'articolo 6, paragrafo 1, primo comma, lettera a), e l'articolo 9, paragrafo 2, lettera a), del regolamento 2016/679
devono essere interpretati nel senso che:
la circostanza che l'operatore di un social network online occupi una posizione dominante sul mercato dei social network online non osta, di per sé, a che gli utenti di tale social network possano validamente acconsentire, ai sensi dell'articolo 4, punto 11, di detto regolamento, al trattamento dei loro dati personali effettuato da tale operatore. Tale circostanza costituisce nondimeno un elemento importante per determinare se il consenso sia stato effettivamente prestato validamente e, in particolare, liberamente, circostanza che spetta a detto operatore dimostrare.
*...Omissis...*

# IL COMMENTO

*di Giuseppe Cassano*

**Sommario:** 1. Servizi online gratuiti. – 2. Profilazione di un utente. – 3. Patrimonializzazione del dato personale. – 4. La vicenda oggetto di controversia. – 5. Le questioni pregiudiziali. – 6. L'intervento della CGUE: i rapporti tra Authority. – 6.1 (Segue) La pubblicità personalizzata. – 6.2. (Segue) Il trattamento di dati sensibili.

Questo contributo muove alcune critiche alla recente sentenza resa dalla Corte di Giustizia che, peccando forse di eccessivo formalismo nell'interpretare le norme in materia di privacy, finisce per far correre il rischio agli operatori professionali di subire una compromissione delle entrate economiche legate alla pubblicità personalizzata. Non ogni aspetto delle transazioni online deve essere vagliato esclusivamente alla luce del GDPR e un operatore professionale può legittimamente proporre ai suoi utenti messaggi pubblicitari personalizzati raccogliendo l'adesione al trattamento dati in sede di iscrizione ad un social network.

*This contribution raises some criticisms of the recent ruling rendered by the Court of Justice which, perhaps sinning of excessive formalism in interpreting the rules on privacy, ends up causing professional operators to run the risk of immediately compromising the economic revenues linked to personalized advertising. Not every aspect of online transactions needs to be examined exclusively in light of the GDPR and a professional operator can legitimately offer its users personalized advertising messages by collecting consent to data processing when registering with a social network.*

## 1. Servizi online gratuiti

È noto come un'ampia gamma di informazioni – ben organizzate e selezionate – siano accessibili agli utenti della rete internet avvalendosi di servizi online prevalentemente gratuiti (1), alcuni fruibili da chiunque liberamente, mentre per altri è richiesta la previa creazione di un profilo utente ("account").

A consentire una tale gratuità sono gli annunci pubblicitari che, per quanto qui rileva, possono essere di due tipi, standardizzati, ossia mostrati a prescindere dalle caratteristiche proprie di chi li vede, oppure personalizzati sulla base delle precedenti attività di navigazione degli utenti cui si rivolgono.

Questi ultimi, ovvero gli annunci personalizzati, incontrano con maggior grado di probabilità l'interesse dei consumatori e hanno, pertanto, un maggior valore sia per questi, che per gli inserzionisti.

La copertura giuridica relativa alla personalizzazione di tali annunci è alla base della recente sentenza resa dalla CGUE, Grande Sezione, 4 luglio 2023, n. 252 sul cui argomentare, in questo lavoro, si svolgeranno alcune riflessioni critiche.

La Corte che, in realtà, non offre all'interprete una chiave di lettura univoca delle norme di riferimento, rimettendo al Giudice del rinvio la valutazione concreta, segue un filo conduttore che, oggi, non ha ragione di esistere: quello di un'applicazione rigorosa ed estremamente formale del GDPR senza tenere in debito conto né l'evoluzione del concetto di consumatore (2), né l'ambito di riferimento della questione sottoposta al suo giudizio. E cioè a dire, quanto a quest'ultimo profilo, la calibrazione ad personam della pubblicità sulla piattaforma social Facebook.

Quello della pubblicità è un settore economico che ha copertura costituzionale (3) e che si snoda attraverso operazioni commerciali che mirano a massimizzare il profitto del produttore del bene, o dell'offerente il servizio pubblicizzato, attraverso studi e ricerche e, soprattutto nell'ambito dell'economia digitale, attraverso la profilazione del consumatore finale (4).

## 2. Profilazione di un utente

Per capire cosa si intende per profilazione di un utente possiamo rifarci alla definizione del Legislatore, agli studi della dottrina (5), o ancora a quelli degli esperti di ingegneria del software o delle tecniche di marketing.

Ma si può anche fare riferimento a un dato di esperienza comune ai più. Chi alla cassa di un supermercato almeno una volta non si è sentito chiedere: "Ha la nostra *fidality card*"?

Ecco spiegata la profilazione: nata nel settore della distribuzione commerciale, e passata nel volgere di pochi anni da un ambito ristretto a un ambito di generale applicazione nell'economica digitale, essa altro non è che una tecnica, molto remunerativa, per offrire al consumatore promozioni, sconti e vantaggi mirati e, quindi, per implementare transazioni commerciali e conseguenti vantaggi per i consumatori e gli operatori economici.

Dal punto di vista prettamente giuridico è indispensabile muovere dal concetto di "profilazione", come delineato dal Legislatore all'art. 4 GDPR, che consta di una "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare (...) le preferenze personali, gli interessi (...) di detta persona fisica" (6).

Uno degli ambiti di utilizzo della profilazione è la pubblicità comportamentale, che trovando terreno fertile nel mondo delle comunicazioni informatiche, prevede il tracciamento delle informazioni rilasciate dagli uten-

(1) Tra cui piattaforme multimediali, navigatori, posta elettronica, archiviazione dati etc.

(2) Il consumatore è oggi il vero protagonista dell'e-commerce tanto da essersi coniata, e diffusa, l'espressione "cyber consumatore". Si vedano in dottrina: D'Amico, *La tutela del consumatore alla prova dell'effettività*, in *Il Foro italiano*, 2023, IX, IV, 390; Manfredonia, *I servizi finanziari 'online' e la tutela del consumatore 'telematico'*, in *Rassegna di diritto civile*, 2004, IV, 1171; Punzi, *Le influenze del consumatore digitale. Il diritto di fronte all'influencer marketing*, in *Rivista internazionale di filosofia del diritto*, 2022, III-IV, 517; Sirgiovanni, *Lo 'smart contract' e la tutela del consumatore: la traduzione del linguaggio naturale in linguaggio informatico attraverso il legal design*, in *Le Nuove leggi civili commentate*, 2023, I, 214; Valenza, *Contratti di abbonamento a servizi online e recesso del consumatore. La Corte di giustizia sull'importo dovuto per le prestazioni già eseguite*, in *Il corriere giuridico*, 2021, VII, 893.

(3) La pubblicità commerciale è "considerata una componente dell'attività delle imprese, come tale assistita dalle garanzie di cui all'art. 41 Cost., e assoggettabile, in ipotesi, alle limitazioni ivi previste al secondo e terzo comma" (Corte Cost., 17 ottobre 1985, n. 231).

(4) Come noto, le operazioni di marketing mirate concernenti un pubblico ristretto sono più efficaci e redditizie di quelle non mirate, e passive, concernenti il grande pubblico.

(5) De Meo, *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Il diritto dell'informazione e dell'informatica*, 2013, III, 587; Soccorso - Quaranta, *Profilazione della clientela ai fini della valutazione di adeguatezza. Recenti tendenze*, in *Bancaria editrice*, 2023, XI, 71; Sborlini, *Profilazione elettorale e protezione dei dati personali: prospettive di soluzione in ambito europeo*, in *Il diritto dell'informazione e dell'informatica*, 2022, VI, 1173; Spangaro, Il concetto di profilazione tra "direttiva madre" e GDPR, in *Giurisprudenza italiana*, 2022, VII, 1577; Pellecchia, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della* responsible research and innovation, in Le *Nuove leggi civili commentate*, 2018, V, 1209.

(6) Le linee guida del Garante della privacy non possono dettare una definizione di profilazione in contrasto con quanto risulta in maniera vincolante dalla previsione legale (Cass. civ., sez. VI - 2, ord., 8 novembre 2021, n. 32411).

ti, «al fine di creare segmenti pubblicitari ad personam, modellati sugli interessi dell'utente considerato» (7).
Attraverso complessi sistemi di profilazione gli operatori hanno la capacità di intercettare le preferenze dell'utenza, in modo da variare l'offerta dei contenuti della pubblicità a seconda dei destinatari e di aumentare a dismisura le visualizzazioni, di fatto contribuendo, in modo causalmente determinante, alla diffusione di prodotti e servizi (8).
L'attività di profilazione – che come visto si traduce in un trattamento automatizzato di dati personali – pone a monte la questione della base legale per procedere a tale trattamento, tema che si declina in termini peculiari in riferimento alle attività online e su cui si pronuncia la Corte di Giustizia nella sua sentenza qui in esame fornendo, come si cercherà di dimostrare nei prossimi paragrafi, una lettura del GDPR improntata al formalismo giuridico (9).

## 3. Patrimonializzazione del dato personale

Prima di addentrarci sull'argomentare della CGUE è opportuna una riflessione sul fenomeno della cd. patrimonializzazione del dato personale (10).
Precisamente, a fronte della tutela del dato personale quale espressione di un diritto della personalità dell'individuo (11) sussiste anche un diverso campo di protezione del dato stesso, inteso quale possibile oggetto di una transazione economica, posta in essere sia tra gli operatori del mercato che tra questi e i soggetti interessati.
Trattasi di un fenomeno tipico delle nuove economie dei mercati digitali che impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore il quale deve essere reso edotto dello scambio di prestazioni che è sotteso alla sua adesione ad un contratto per la fruizione di un servizio, quale è quello di utilizzo di un social network.
Questa possibilità di sfruttamento economico del dato personale nell'ambito delle piattaforme social, unitamente alla conseguente necessità di tutelare il consumatore che le utilizzi, non può definirsi un concetto del tutto innovativo (12): ciò che rileva è, in particolare, la natura patrimoniale del bene oggetto della decisione che il consumatore deve assumere, che fa sì che la stessa possa essere qualificata come decisione di natura "commerciale", ai fini della quale risulta necessaria un'informazione quanto più chiara e completa da parte del professionista.
Il fatto, poi, che anche ove l'utente si sia determinato nel senso di non accettare la cessione gli sia comunque consentito accedere a taluni dei servizi forniti, e che quindi il dato non costituisca un corrispettivo in senso tecnico del servizio, è un'eventualità successiva che non elimina la necessità di una corretta informazione al fine di assicurare una scelta consapevole sull'accettazione, o

(7) V. Trib. Milano, sez. I, 11 aprile 2023, n. 2128.

(8) V. Cass. civ., sez. I, ord., 13 dicembre 2021, n. 39763 secondo cui «i servizi prestati on line e, segnatamente, l'attività di hosting hanno subito nel corso degli ultimi anni un'evoluzione radicale. La cernita ed il riordino dei contenuti, lungi dall'essere assorbiti dalla nozione di mera memorizzazione, sono invece oggigiorno il cuore dell'attività economica di un hosting provider. Grazie a sistemi di data mining (insieme di tecniche e metodologie che hanno per oggetto l'estrazione di informazioni utili da grandi quantità di dati attraverso metodi automatici o semiautomatici e il loro utilizzo scientifico, aziendale, industriale o operativo) e di elaborazione massiva di big data, questi prestatori di servizi sono in grado di trarre enormi guadagni dalla loro attività di hosting».

(9) Sulla premessa secondo cui il consenso in questione deve essere ricondotto alla nozione di "consenso informato (nozione, questa, ampiamente impiegata in taluni settori – basti pensare al campo delle prestazioni sanitarie) la giurisprudenza (Cass. civ., sez. I, 2 luglio 2018, n. 17278) ha affrontato, con riguardo all'aspetto della libertà, la specifica questione se un "condizionamento" – tale da far sì che il consenso non sia conforme al dettato normativo – possa essere ravvisato nell'ipotesi in cui l'offerta di un determinato servizio da parte del gestore di un sito internet sia condizionato alla prestazione del consenso all'utilizzo dei dati personali per il successivo invio, da parte di terzi, di messaggi pubblicitari. Ha ritenuto la Suprema Corte che la risposta a tale quesito non possa essere univoca e, cioè, che il condizionamento non possa sempre, e comunque, essere dato per scontato e debba, invece, essere ritenuto tanto più sussistente, quanto più la prestazione offerta dal gestore del sito internet sia, ad un tempo, infungibile e irrinunciabile per l'interessato. Il che non può certo dirsi accadere nell'ipotesi dell'offerta di un generico servizio informativo giacché, all'evidenza, si tratterebbe di informazioni agevolmente acquisibili per altra via, eventualmente attraverso altri siti (anche) a pagamento, se non attraverso il ricorso all'editoria cartacea, con la conseguenza che ben può rinunciarsi a detto servizio senza un sacrificio gravoso. La Suprema Corte, sempre nella decisione n. 17278/2018, conclude il suo argomentare con l'affermazione, in punto di diritto, del seguente principio di diritto: «In tema di consenso al trattamento dei dati personali, la previsione dell'art. 23 del Codice della privacy, nello stabilire che il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, consente al gestore di un sito Internet, il quale somministri un servizio fungibile, cui l'utente possa rinunciare senza gravoso sacrificio (nella specie servizio di newsletter su tematiche legate alla finanza, al fisco, al diritto e al lavoro), di condizionare la fornitura del servizio al trattamento dei dati per finalità pubblicitarie, sempre che il consenso sia singolarmente ed inequivocabilmente prestato in riferimento a tale effetto, il che comporta altresì la necessità, almeno, dell'indicazione dei settori merceologici o dei servizi cui i messaggi pubblicitari saranno riferiti».

(10) Versaci, *Il valore negoziale dei dati personali del consumatore: spigolature sul recepimento della Direttiva 2019/770/Ue in una prospettiva comparata*, in *Rivista di diritto privato*, 2022, II, 207.

(11) In quanto tale soggetto a specifiche e non rinunciabili forme di protezione, quali il diritto di revoca del consenso, di accesso, rettifica, oblio.

(12) Invero già negli "Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali" del 25 maggio 2016, la Commissione Europea aveva affermato che "i dati personali, le preferenze dei consumatori e altri contenuti generati dagli utenti hanno un valore economico de facto".

meno, dell'utilizzo a fini pubblicitari delle preferenze personali (13).

## 4. La vicenda oggetto di controversia

Alla luce di quanto fin qui messo in evidenza – e cioè la copertura costituzionale della pubblicità, l'efficienza dei meccanismi di profilazione, l'indispensabilità del trattamento lecito dei dati personali e la patrimonializzazione degli stessi – può ora passarsi all'analisi della sentenza della CGUE.

Questa è resa su domanda di pronuncia pregiudiziale, proposta sensi dell'art. 267 TFUE, dall'*Oberlandesgericht Düsseldorf* (Tribunale Superiore del Land, *Düsseldorf*, Germania) che tratta, in estrema sintesi, della decisione del *Bundeskartellamt* (ovvero dell'Autorità federale tedesca garante della concorrenza), di vietare ad alcune società (14) di procedere al trattamento di taluni dati personali previsto dalle condizioni generali di utilizzo del social network Facebook (15).

Ricostruito il contesto normativo di riferimento (secondo le coordinate dettate dal diritto euro-unionale e dal diritto tedesco) la Corte sottolinea come:

- Meta Platforms Inc. (di seguito, Meta) gestisca l'offerta del social network Facebook nell'U.E. e promuova (all'indirizzo www.facebook.com) servizi gratuiti per gli utenti privati (16);
- dal punto di vista economico, Facebook si fondi sul finanziamento tramite la pubblicità online, che viene confezionata su "misura per i singoli utenti del social network in funzione, in particolare, del loro comportamento di consumo, dei loro interessi, del loro potere d'acquisto e della loro situazione personale" (17) (*id est*, profilazione degli utenti);
- Meta si basi sul contratto d'uso a cui gli utenti di Facebook aderiscono e con il quale accettano le condizioni generali stabilite da detta società, accettazione – quest'ultima – necessaria per utilizzare lo stesso social network (18). A loro volta, le condizioni generali rinviano alle regole sull'uso dei dati e dei marcatori (cookies) adottate dalla suddetta società: in forza di queste ultime, Meta raccoglie dati riferiti agli utenti e ai loro dispositivi, relativi alle loro attività all'interno e all'esterno del social network, e li mette in relazione con gli account Facebook degli utenti interessati. Per quanto riguarda, in particolare, i dati relativi alle attività al di fuori del social network (indicati in sentenza come "dati off Facebook"), si tratta, da un lato, dei dati concernenti la consultazione di pagine Internet e di applicazioni di terzi che sono collegate a Facebook attraverso interfacce di programmazione – gli "Strumenti business di Facebook" – e, dall'altro, dei dati riguardanti l'utilizzo degli altri servizi online appartenenti al gruppo Meta.

Orbene, l'Autorità federale garante della concorrenza, da parte sua, aveva sostanzialmente vietato alle menzionate società di subordinare, nelle condizioni generali, l'uso di Facebook da parte di utenti privati residenti in Germania al trattamento dei loro "dati off Facebook" e di procedere, senza il consenso di detti utenti, al trattamento di tali dati sulla base delle condizioni generali allora vigenti (19).

---

(13) T.a.r. Lazio, Roma, sez. I, 18 novembre 2022, n. 15326.

(14) Si tratta di "Meta Platforms Inc., già Facebook Inc., Meta Platforms Ireland Limited, già Facebook Ireland Ltd., Facebook Deutschland GmbH".

(15) Precisamente: «"1 La domanda di pronuncia pregiudiziale verte sull'interpretazione dell'articolo 4, paragrafo 3, TUE nonché dell'articolo 6, paragrafo 1, dell'articolo 9, paragrafi 1 e 2, dell'articolo 51, paragrafo 1, e dell'articolo 56, paragrafo 1, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU 2016, L 119, pag. 1, e rettifiche in GU 2016, L 314, pag. 72, GU 2018, L 127, pag. 3 e GU 2021, L 74, pag. 35; in prosieguo: il "RGPD").

2 Tale domanda è stata presentata nell'ambito di una controversia tra M.P. Inc., già F. Inc., M.P.I. Ltd, già F.I. Ltd, e F.D. GmbH, da un lato, e il *Bundeskartellamt* (autorità federale garante della concorrenza, Germania), dall'altro, in merito alla decisione di quest'ultimo di vietare a tali società di procedere al trattamento di taluni dati personali previsto dalle condizioni generali di utilizzo del social network F. (in prosieguo: le "condizioni generali")».

(16) Al tempo stesso le altre società del gruppo Meta offrono, sempre nell'U.E., altri servizi online tra cui Instagram, WhatsApp, Oculus e - fino al 13 marzo 2020 - Masquerade.

(17) Secondo quanto si afferma nella pronuncia dell'*Oberlandesgericht Düsseldorf Beschluss*: «*Facebook.com wird durch Online-Werbung finanziert, die auf den individuellen Nutzer des sozialen Netzwerks zugeschnitten ist und darauf abzielt, dem Nutzer diejenige Werbung zu zeigen, die ihn auf Grund seines persönlichen Konsumverhaltens, seiner Interessen, Kaufkraft und Lebenssituation interessieren könnte. Werbetreibende können mittels des „Werbeanzeigenmanagers" die gewünschte Zielgruppe spezifizieren und die Werbung den Nutzern anzeigen lassen, zudem ihre Kundenlis ten in verschlüsselter Form an Facebook übermitteln und ihre Werbung durch Abgleich mit den Daten aus dem sozialen Netzwerk weiter verfeinern*».

(18) Ancora secondo la pronuncia dell'*Oberlandesgericht Düsseldorf Beschluss*: «*Private Nutzer in Europa schließen mit der Betätigung der Schaltfläche "Registrieren" einen Nutzungsvertrag über Facebook.com ab und stimmen damit gleichzeitig den von Facebook Ireland gestellten Nutzungsbedingungen zu. Nach diesen verarbeitet Facebook Ireland personenbezogene Daten, für deren Erläuterung insbesondere auf die von Facebook Ireland gestellten Daten- und Cookie-Richtlinien verwiesen wird. Danach erfasst Facebook Ireland nutzer- und gerätebezogene Daten über Nutzeraktivitäten innerhalb und außerhalb des sozialen Netzwerks und ordnet sie den Facebook.com-Konten der betroffenen Nutzer zu. Bei den außerhalb des sozialen Netzwerks stattfindenden Nutzeraktivitäten geht es zum einen um den Besuch von dritten Webseiten und Apps, die mittels Programmierschnittstellen ("Facebook Business Tools") mit Facebook.com verbunden sind, und zum anderen um die Nutzung der anderen zu Facebook gehörenden Dienste Instagram, WhatsApp und Oculus, in Bezug auf die eine Datenverarbeitung "über die anderen FacebookUnternehmen und –Produkte hinweg" erfolgt*».

(19) Inoltre, essa ha ordinato loro di adeguare dette condizioni generali in modo che da esse risultasse chiaramente che tali dati non sarebbero stati né raccolti, né messi in relazione con gli account degli utenti Face-

Alla base di tale decisione vi è, in punto di diritto, la considerazione secondo la quale il trattamento dei dati come regolato nelle riferite condizioni generali, costituiva uno sfruttamento abusivo della posizione dominante di tale società sul mercato dei sociali network online per gli utenti privati in Germania.
Nel contesto di tale vicenda, in un primo momento, Meta (esattamente il 31 luglio 2019) ha introdotto nuove condizioni generali, le quali indicano espressamente che l'utente, invece di pagare per l'uso dei prodotti Facebook, dichiara di acconsentire alle inserzioni pubblicitarie e, poi, dal 28 gennaio 2020 la stessa Meta offre in tutto il mondo, il cd. "Off-Facebook-Activity" che consente agli utenti di Facebook di visualizzare un riepilogo delle informazioni che li riguardano, che le società del gruppo Meta ottengono in relazione alle loro attività su altri siti Internet e applicazioni, e di scollegare, se lo desiderano, tali dati dal loro account Facebook, tanto per il passato quanto per il futuro.

## 5. Le questioni pregiudiziali

Il Tribunale Superiore del Land, *Düsseldorf* nutre una serie di dubbi – che portano a sottoporre alla Corte un complesso ventaglio di questioni pregiudiziali – che si possono così riepilogare:
- in primo luogo, in merito alla possibilità per le autorità nazionali garanti della concorrenza di controllare, nell'ambito dell'esercizio delle loro competenze, la conformità di un trattamento di dati personali alle condizioni stabilite nel GDPR;
- in secondo luogo, in merito alla possibilità per un operatore di un social network online di trattare i dati personali sensibili della persona interessata (ai sensi dell'art. 9, paragrafi 1 e 2, GDPR);
- ancora, in merito alla liceità del trattamento dei dati personali dell'utente interessato da parte di un siffatto operatore (art. 6, paragrafo 1, GDPR);
- infine, in merito alla validità - alla luce dell'art. 6, paragrafo 1, I, lettera a), e dell'articolo 9, paragrafo 2, lettera a), del medesimo Regolamento - del consenso prestato a un'impresa che detiene una posizione dominante sul mercato nazionale dei social network online, ai fini di un trattamento di dati del tipo di quello qui rilevante.

## 6. L'intervento della CGUE: i rapporti tra Authority

Come anticipato, la lettura della pronuncia resa dall'adita CGUE non può non far sorgere qualche dubbio in capo all'interprete.

book, né utilizzati senza il consenso dell'utente interessato, e ha chiarito che tale consenso non è valido qualora costituisca una condizione per l'utilizzo del social network.

In particolare, la prima questione posta dall'A.G. tedesca ha carattere procedurale e consiste nello stabile se un'autorità per la concorrenza possa pronunciarsi su questioni interpretative ed applicative del GDPR. Il che si traduce in una riflessione sulla cd. l'applicazione cd. "indiretta" del Regolamento privacy.
Su questo specifico punto la Corte pone i seguenti capisaldi:
- in primis, l'autorità garante della concorrenza è tenuta al rispetto dell'obbligo di leale cooperazione con le altre autorità di controllo (20),
- quindi, un'autorità garante della concorrenza può constatare, nell'ambito di una procedura per abuso di posizione dominante, che le condizioni generali d'uso poste in essere dall'impresa attenzionata, e relative al trattamento dei dati personali (e alla loro applicazione), non siano conformi al GDPR sempreché detta constatazione sia necessaria per accertare l'esistenza di un tale abuso;
- l'autorità nazionale garante della concorrenza non può discostarsi da una decisione dell'autorità nazionale di controllo competente, o dell'autorità di controllo capofila competente, che riguardi tali condizioni generali o condizioni generali analoghe;
- laddove sorgano dubbi sulla portata di tale decisione l'autorità nazionale garante della concorrenza deve consultare dette autorità di controllo e chiederne la cooperazione, al fine di fugare i propri dubbi o di determinare se si debba attendere l'adozione di una decisione da parte di tali autorità prima di iniziare la propria valutazione;
- infine, in assenza di obiezioni o di risposta di queste ultime entro un termine ragionevole, l'autorità nazionale garante della concorrenza può proseguire la propria indagine.
In estrema sintesi, il meccanismo delineato dalla Corte è tale per cui un'autorità nazionale garante della concorrenza può soffermarsi in tema di valutazione del trattamento dati (nell'ambito di una procedura su un

(20) Al tema della cooperazione tra autorità amministrative indipendenti non è estranea la giurisprudenza nazionale che, da ultimo, ponendo l'accento sullo spettro amplissimo di ipotesi riconducibili all'attività di trattamento e dunque rilevanti in materia di dati personali delle persone fisiche (e quindi ricadenti nella sfera di applicazione del GDPR) ha escluso la possibilità di sostenere compartimenti "stagni", non permeabili tra di loro, con riferimento all'ambito di competenza e dei poteri di AGCM rispetto a quelli di altre Autorità, in particolare del Garante privacy. E allora non si può validamente <<escludere "a priori" qualsiasi forma di collaborazione tra le due Autorità nel corso di una indagine che, seppure fondamentalmente indirizzata all'esame circa la compatibilità o meno con la disciplina consumeristica di condotte sviluppate da professionisti, abbia indubitabilmente addentellati forti e robuste caratterizzazioni osmotiche con la tutela dei dati personali, potendosi, in thesi, sostenere addirittura una funzionalizzazione tra i comportamenti contestati e la violazione, contemporanea, di discipline normative differenti perché riferite a settori specialistici e quindi la doverosità della cooperazione tra Autorità» (Cons. Stato, sez. VI, 15 gennaio 2024, n. 497).

abuso di posizione dominante) e, tuttavia, non si può discostare da una decisione adottata dell'autorità garante della privacy (primo limite) e deve consultare e cercare la cooperazione di quest'ultima (secondo limite).
Una volta consultate le autorità competenti in materia di privacy se le stesse non si oppongono, o non rispondono "entro un termine ragionevole", l'autorità nazionale per la concorrenza può procedere.
Queste affermazioni in punto di diritto, da parte della Corte, che pur non incidono sulle fondamenta del principio dello sportello unico ("one-stop-shop") (21) in tema di privacy, possono comunque compromettere significativamente i vantaggi dell'armonizzazione nell'applicazione del GDPR imponendo a diverse autorità di controllo una collaborazione che potrebbe non essere sempre proficua (problemi operativi non tarderanno a sorgere in conseguenza della necessità per le autorità privacy di controllare le attività delle varie autorità nazionali per la concorrenza, il tutto in danno dell'armonizzazione).

### *6.1. (Segue) La pubblicità personalizzata*

Il rapporto tra pubblicità personalizzata e corretta applicazione del GDPR è il profilo di maggiore portata della sentenza in esame per i suoi risvolti non solo di natura giuridica, ma anche economica, giacchè, come detto nelle prime battute di questo lavoro, la pubblicità è indispensabile per il sostentamento dei social media (22).
La Corte muove da un'affermazione che non motiva e cioè a dire che, malgrado la gratuità dei servizi resi da Facebook, l'utente di quest'ultimo non possa ragionevolmente attendersi che, senza il suo consenso, l'operatore di tale social network tratti i suoi dati personali a fini di personalizzazione della pubblicità.
Insiste, poi, sul fatto che i diritti fondamentali e gli interessi degli utenti prevalgono sull'interesse dell'operatore ad una tale personalizzazione della pubblicità ragion per cui il trattamento di dati da quest'ultimo così effettuato non può rientrare nell'ambito di applicazione dell'art. 6, paragrafo 1, I, lettera f), GDPR (cioè del trattamento "necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi").
Inoltre, sottolinea la Corte come il trattamento qui in esame sia potenzialmente illimitato, tanto da poter suscitare nell'utente la sensazione che la sua vita privata sia oggetto di continua sorveglianza, e come, al contempo, l'obiettivo di garantire la sicurezza del network costituisca comunque un legittimo interesse di Meta, idoneo cioè a giustificare il trattamento di cui trattasi.
La Corte, da un lato, rimette alla decisione del Giudice del rinvio il compito di verificare se, e in quale misura, il trattamento di dati personali raccolti a partire da fonti esterne a Facebook risulti effettivamente necessario per garantire che non sia compromessa la sicurezza interna di tale network (23).
Dall'altro lato non esclude, a priori, che l'interesse del titolare del trattamento a migliorare il suo prodotto (o servizio) al fine di renderlo più performante, e quindi più attrattivo, possa costituire un legittimo interesse idoneo a giustificare un trattamento di dati personali.
E al contempo appare dubbio, alla Corte, che, relativamente al trattamento di dati in causa nel procedimento principale, "l'obiettivo diretto al miglioramento del prodotto possa – tenuto conto della portata di tale trattamento e del suo notevole impatto sull'utente, nonché della circostanza che quest'ultimo non possa ragionevolmente attendersi che tali dati siano trattati dalla Meta – prevalere sui diritti fondamentali e sugli interessi di detto utente, tanto più nel caso in cui quest'ultimo sia minorenne".
Orbene è certo che i dati personali debbano essere trattati in modo "lecito" ai sensi del GDPR che, all'art. 6, precisa come il trattamento sia lecito solo se, e nella misura in cui, ricorre almeno una delle seguenti condizioni:
a) l'interessato abbia espresso il proprio "consenso" al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento sia "necessario all'esecuzione di un contratto" (o di misure precontrattuali) di cui l'interessato sia parte;
c) il trattamento sia necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento sia necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento sia necessario per il "perseguimento del legittimo interesse del titolare del trattamento o di terzi", a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che ri-

(21) V. art. 60 GDPR.

(22) Conti, *Fare business con Facebook*, Hoepli, 2012; D'Acquisto G., Naldi M., *Big Data e Privacy by Design. Anonimizzazione, Pseudonimizzazione, Sicurezza*, Giappichelli, 2017; Loguercio M., *Le nuove vie del marketing digitale*, Milano, 2002; Mantelero A., *Big data: I rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il diritto dell'informazione e dell'informatica*, 2012, 139; Stabile S., *Le nuove frontiere della pubblicità e del marketing su Internet*, in *Diritto Industriale, 2009, V,* 482.

(23) In tale contesto, il Giudice è chiamato altresì a verificare il rispetto del principio della "minimizzazione dei dati" (art. 5, paragrafo 1, lett. c, GDPR).

chiedono la protezione dei dati personali, in particolare se l'interessato è un minore (24).
Ai fini del nostro argomentare, in particolare, occorre stabilire se Meta possa fare affidamento per una corretta pubblicità personalizzata sul legittimo interesse, oppure sul trattamento necessario all'esecuzione del contratto o, infine, sul consenso esplicito dell'utente (25).
Sul punto la Corte offre una interpretazione restrittiva del cennato requisito della necessità contrattuale: e cioè a dire, l'operazione di trattamento dati deve essere "oggettivamente indispensabile" per realizzare una finalità che è parte integrante della prestazione contrattuale destinata all'interessato gravando a carico del responsabile del trattamento dimostrare in che modo l'oggetto principale del contratto non potrebbe essere conseguito in assenza del trattamento dati (26).
Con particolare riferimento alla personalizzazione della pubblicità la Corte riconosce come essa sia utile per l'utente, in quanto gli consente in particolare di visualizzare un contenuto in larga misura corrispondente ai suoi interessi, e tuttavia rimane il fatto "che, salvo verifica del giudice del rinvio, la personalizzazione dei contenuti non appare necessaria per offrire a tale utente i servizi del social network online. Tali servizi possono, eventualmente, essergli forniti sotto forma di un'alternativa equivalente che non implichi tale personalizzazione, che non è dunque oggettivamente indispensabile per una finalità che faccia parte integrante di detti servizi".
E cioè a dire la Corte non si pronuncia in via espressa e definitiva, ma lascia la soluzione della questione al Tribunale nazionale, né la stessa – si noti bene – fa riferimento diretto alla pubblicità personalizzata riferendosi piuttosto alla "personalizzazione dei contenuti" che, in ogni caso, è ritenuta operazione strettamente non necessaria.
Passiamo ora all'altro profilo e precisamente a quello riguardante gli interessi legittimi in riferimento al quale la Corte sviluppa il suo argomentare lungo due direttrici fondamentali sulle quali, in realtà, si è già avuto modo di riflettere.

La prima attiene alla considerazione secondo cui, per gli iscritti a Facebook, non era ragionevole ritenere che, pur a fronte di servizi gratuiti, i loro dati sarebbero stati oggetto di trattamento per la pubblicità personalizzata e la seconda direttrice pone l'accento sul pericolo di un possibile, continuo, monitoraggio di abitudini e preferenze dei medesimi utenti.
Si potrebbe quindi pensare, sempre in riferimento agli interessi legittimi, ad una distinzione tra "grandi" social network e altri fornitori di servizi online anche per la pubblicità personalizzata: i primi potrebbero essere tenuti a uno standard più severo di quello richiesto per i secondi, data la vastità dei dati da essi raccolti.
Quanto al consenso la Corte rimette – ancora una volta – al giudice del rinvio il compito di stabilire se gli utenti di Facebook abbiano validamente e, in particolare, liberamente espresso il loro consenso al trattamento.
Quindi dichiara che gli artt. 6 e 9 GDPR devono essere interpretati nel senso che "la circostanza che l'operatore di un social network online occupi una posizione dominante sul mercato dei social network online non osta, di per sé, a che gli utenti di tale social network possano validamente acconsentire, ai sensi dell'articolo 4, punto 11, di detto regolamento, al trattamento dei loro dati personali effettuato da tale operatore. Tale circostanza costituisce nondimeno un elemento importante per determinare se il consenso sia stato effettivamente prestato validamente e, in particolare, liberamente, circostanza che spetta a detto operatore dimostrare".
Riportandosi dunque al diritto antitrust e della concorrenza, e al concetto di "posizione dominante", la Corte se da un lato sottolinea che il consenso deve essere prestato liberamente (altrimenti essendo invalido), dall'altro lato precisa che la mera posizione dominante non vuol dire, *ex se*, che il consenso degli utenti non sia valido.
Gli utenti – secondo la Corte – devono disporre della libertà di rifiutare individualmente, nell'ambito della procedura contrattuale, di prestare il loro consenso a operazioni particolari di trattamento di dati non necessarie all'esecuzione del contratto, senza essere per questo tenuti a rinunciare integralmente alla fruizione del servizio offerto dall'operatore del social network online, il che implica che a detti utenti venga proposta, se del caso a fronte di un adeguato corrispettivo, un'alternativa equivalente non accompagnata da simili operazioni di trattamento dati. È importante sottolineare due aspetti importanti in questa affermazione della Corte. In primo luogo, la Corte ritiene che una alternativa binaria (o consenso alla profilazione, o alternativa equivalente dietro di un adeguato corrispettivo) soddisfa chiaramente i requisiti del GDPR.
In secondo luogo, invece, se non è chiaro, né univoco, cosa si intenda nella pratica per "alternativa equivalen-

(24) V. CGUE, sez. I, 7 dicembre 2023, n. 26/22.

(25) In riferimento, come detto, ai dati off Facebook, e "riformulando la domanda del tribunale richiedente" la Corte con il suo interventi ha od oggetto l'operazione di "trattamento di dati personali effettuato da un operatore di un social network online - consistente nel raccogliere dati degli utenti di tale social network provenienti da altri servizi del gruppo al quale appartiene tale operatore oppure derivanti dalla consultazione, da parte di tali utenti, di siti Internet o di applicazioni di terzi, nel mettere in relazione tali dati con l'account del social network di detti utenti e nell'utilizzare detti dati".

(26) Di conseguenza, secondo la Corte, la circostanza che un trattamento sia menzionato nel contratto oppure che sia soltanto "utile per l'esecuzione" di quest'ultimo è, di per sé, circostanza irrilevante ai fini in esame.

te, tuttavia bene fa la Corte a respingere la tesi per cui il consenso non è prestato liberamente ogni volta che l'alternativa al medesimo consenso non sia gratuita (cioè quando l'alternativa al consenso è il pagamento di un corrispettivo).
Ma la Corte, nel suo argomentare, cade forse in contraddizione?
A ben vedere sì: invero, da un lato, essa rifiuta (o almeno dubita) che l'utilizzo di dati personali di terzi per la pubblicità personalizzata sia necessario per l'esecuzione di un contratto ma, dall'altro lato, si noti bene, essa stessa suggerisce un'alternativa equivalente non accompagnata dal trattamento dati per la pubblicità personalizzata (dietro adeguato corrispettivo) (27).
E tale alternativa non può non avere matrice contrattuale: l'esecuzione dell'accordo tra le parti necessita di uno scambio di prestazioni e, dal lato dell'utente finale del servizio, queste potranno essere rappresentante dalla cessione dei propri dati o da non meglio specificate alternative che comunque dovranno essere di natura giuridica omogenea. E allora è evidente che sussiste una necessità di natura contrattuale per prestare il servizio!
Come emerge altresì con evidenza l'erroneità di una interpretazione così ristretta di "necessità contrattuale".
Il tutto senza sottacere che dal considerando n. 4 del Regolamento europeo qui in esame emerge, testualmente, che il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità (28).

### *6.2. (Segue) Il trattamento di dati sensibili*

Concludiamo in ordine alla possibilità, per un operatore di un social network online, di trattare i dati personali sensibili della persona interessata (ai sensi dell'art. 9, paragrafi 1 e 2, GDPR), questione sulla quale la Corte, nuovamente, non fornisce all'interprete indicazioni precise.
È certamente possibile – secondo la Corte – che alla semplice navigazione possa corrispondere la rivelazione di dati sensibili dell'utente ma è rimesso al Giudice del caso concreto stabilire se in relazione al caso specifico ciò accada o meno. La problematica è complessa e presenta diverse sfaccettature. Da un lato è importante distinguere tra dati sensibili e dati di natura non sensibile che pero' potrebbero svelare inferenze sensibili in seguito ad ulteriori trattamenti o combinazioni con altri dati.
In ogni caso, Sulla questione del rapporto tra "Pubblicità sulle piattaforme online" e "trattamento di dati sensibili" viene in soccorso il DSA che al comma 3 dell'art. 26 è chiaro nello stabilire che "I fornitori di piattaforme online non possono presentare pubblicità ai destinatari del servizio basate sulla profilazione, ..., utilizzando le categorie speciali di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679."
E il successivo art. 28 DSA ("Protezione online dei minori") vieta ai fornitori di piattaforme online di presentare sulla loro interfaccia pubblicità basata sulla profilazione "che usa i dati personali del destinatario del servizio se sono consapevoli, con ragionevole certezza, che il destinatario del servizio è minore".
Infine ulteriori obblighi di trasparenza della pubblicità online sono dettati all'art. 39 DSA per i fornitori di "piattaforme online di dimensioni molto grandi", o di motori di ricerca online di "dimensioni molto grandi" (con una utenza pari o superiore a 45 milioni in U.E.) che presentano pubblicità sulle loro interfacce online.
Questi sono chiamati a compilare e rendere accessibile al pubblico in una specifica sezione della loro interfaccia online un registro contenente tutta una serie di informazioni (29) per l'intero periodo durante il quale presentano pubblicità e fino a un anno dopo la data dell'ultima presentazione dell'annuncio pubblicitario sulle loro interfacce online.

(27) V.: <https://www.barczentewicz.com/post/the-cjeus-decision-in-metas-competition-case-consequences-for-personalized-advertising-under-the-gdpr-part-1/> nonché <https://www.barczentewicz.com/post/the-cjeus-decision-in-metas-competition-case-part-2-sensitive-data-and-privacy-enforcement-by-competition-authorities/>.

(28) App. Genova, sez. lav., 30 settembre 2023, n. 168.

(29) Art. 39, II, DSA: «Il registro comprende come minimo tutte le informazioni seguenti: a) il contenuto della pubblicità, compreso il nome del prodotto, del servizio o del marchio e l'oggetto della pubblicità; b) la persona fisica o giuridica per conto della quale viene presentata la pubblicità; c) la persona fisica o giuridica che ha pagato la pubblicità, se diversa da quella di cui alla lettera b); d) il periodo durante il quale è stata presentata la pubblicità; e) un'indicazione volta a precisare se la pubblicità fosse destinata a essere presentata a uno o più gruppi specifici di destinatari del servizio e, in tal caso, i principali parametri utilizzati a tal fine, compresi, se del caso, i principali parametri utilizzati per escludere uno o più di tali particolari gruppi; f) le comunicazioni commerciali pubblicate sulle piattaforme online di dimensioni molto grandi e individuate a norma dell'articolo 26, paragrafo 2; g) il numero totale di destinatari del servizio raggiunti e, ove opportuno, i dati aggregati suddivisi per ciascuno Stato membro relativi al gruppo o ai gruppi di destinatari ai quali la pubblicità era specificamente destinata».

# Comunicazioni presuntivamente diffamatorie trasmesse tramite Facebook, mediante l'invio di molteplici messaggi privati indirizzati a singoli destinatari

CORTE DI CASSAZIONE; sezione terza; Sentenza 4 marzo 2024, n. 5701; Pres. Travaglino; Rel. Rubino; M.G. (Avv. Serranò) c. S.G. (Avv. Ulivi).

*Ai fini della configurabilità della diffamazione è richiesto, in capo all'autore della condotta dedotta come lesiva dell'altrui onorabilità, solo il dolo generico e non anche il dolo specifico. Infatti in tema di responsabilità civile per diffamazione, è necessario e sufficiente che ricorra l'elemento soggettivo del c.d. dolo generico, anche nelle forme del dolo eventuale, cioè non è richiesta la volontà ma è sufficiente la consapevolezza di poter, con le proprie dichiarazioni, offendere l'onore e la reputazione altrui, la quale si può desumere anche dalla intrinseca consistenza diffamatoria delle espressioni usate.*

*...Omissis...*

**Motivi della decisione**

M.G. aveva proposto ricorso per Cassazione nei confronti di S.G. avverso la Sentenza n. 984 del 29 marzo 2021 pronunciata dalla Corte di Appello di Milano, articolandolo in tre motivi.

I fatti all'origine della fattispecie sono i seguenti.

M.G. adiva il Tribunale di Milano, chiedendo la condanna di S.G., con la quale aveva intrattenuto una relazione sentimentale, al risarcimento dei danni derivanti dall'essere stato accusato ingiustamente del compimento di atti persecutori e dunque coinvolto nel relativo procedimento penale all'esito del quale era stato assolto con formula piena, nonché dall'essere stato screditato agli occhi di amici e colleghi mediante l'invio di *mail* e messaggi divulgati tramite *Facebook* con l'intenzione di danneggiarlo e isolarlo dall'ambiente lavorativo e sociale.

Il Tribunale adito rigettava la domanda inerente alla calunnia e accoglieva la domanda risarcitoria per diffamazione, altresì condannando la S.G. al risarcimento del danno morale nei confronti di M.G.

Dipoi, in accoglimento dell'impugnazione di S.G., la Corte di Appello di Milano, rigettava la domanda risarcitoria, ritenendo carenti gli estremi della diffamazione sul presupposto per cui i messaggi contestati erano stati inviati da S.G. a un solo destinatario per volta, e dunque in forma riservata, senza eccedere i limiti della continenza.

Inoltre, il Giudice di secondo grado rilevava l'insussistenza, nel caso di specie, dell'elemento oggettivo necessario per integrare la condotta di diffamazione (ovvero la comunicazione diretta a plurimi destinatari), ritenendo privo di valenza denigratoria il contenuto dei messaggi trasmessi dalla S.G., poiché «*semplice espressione della* [propria] *delusione personale*» nei confronti delle condotte poste in essere dal proprio *ex*.

Avverso tale pronuncia, la parte soccombente M.G. proponeva ricorso dinanzi alla Corte di Cassazione.

"Con il primo motivo denuncia l'omesso esame di un fatto decisivo della controversia oggetto di discussione tra le parti, avendo erroneamente ritenuto la corte d'appello che i messaggi della S.G. erano stati indirizzati a due amici del M.G., separatamente, quindi in forma confidenziale e riservata, senza considerare che di uno dei messaggi era venuta a conoscenza anche una terza persona, e che il contenuto di uno di essi non era in realtà riservato. Sostiene, proponendo alla Corte una rilettura del testo dei messaggi, che le parole usate celassero in realtà una volontà denigratoria, e che, per come gli stessi erano formulati, non fossero volti a precludere la divulgazione del messaggio.

Con il secondo motivo il ricorrente denuncia la violazione e falsa applicazione degli artt. 595 c.p., 115 e 116 c.p.c. per aver la corte d'appello ritenuto assente il dolo nell'utilizzo, da parte della S.G., di espressioni e parole offensive, riconducendo i suoi messaggi all'espressione del diritto di critica. Sottolinea per contro il contenuto effettivamente denigratorio delle frasi pronunciate dalla ex compagna. Sostiene poi che le comunicazioni non erano riservate, tant'è che dall'attività istruttoria svolta emergerebbe che il loro contenuto era stato effettivamente divulgato. Richiama l'orientamento di legittimità secondo il quale, in caso di diffamazione commessa

mediante scritti, sussiste il requisito della comunicazione con più persone, necessario per integrare il reato, anche quando le espressioni offensive siano state comunicate a una sola persona ma destinate ad essere riferite almeno ad un'altra persona che ne abbia poi effettiva conoscenza (e richiama Cass. n. 31728 del 2004 ed altri precedenti). Sottolinea poi che il dolo richiesto per il reato di diffamazione è soltanto il dolo generico e che il contenuto dei messaggi non poteva essere legittimamente ricondotto nell'ambito della critica lecita perché la controricorrente aveva utilizzato epiteti ed espressioni di per sé offensivi, perché volti a sottolineare l'immaturità del ricorrente e dei suoi comportamenti.

Con il terzo motivo denuncia la nullità della sentenza, per violazione dell'art. 132, secondo comma, n. 4 c.p.c., per non aver il giudice d'appello esplicitato le ragioni del suo convincimento in ordine alla mancanza dell'elemento oggettivo della diffusione a terzi delle comunicazioni, e alla mancanza dell'elemento soggettivo del dolo. Attraverso le argomentazioni a supporto del motivo il ricorrente torna a ribadire che ad integrare la diffamazione sia sufficiente il dolo generico e che quindi non fosse necessario accertare la sussistenza della volontà di offendere, in capo alla S.G., ma che la corte avrebbe dovuto piuttosto valutare l'obiettiva idoneità screditante ed offensiva delle espressioni utilizzate.".

Attraverso le argomentazioni a supporto del motivo il ricorrente torna a ribadire che ad integrare la diffamazione sia sufficiente il dolo generico e che quindi non fosse necessario accertare la sussistenza della volontà di offendere, in capo alla S.G., ma che la corte avrebbe dovuto piuttosto valutare l'obiettiva idoneità screditante ed offensiva delle espressioni utilizzate.

I tre motivi possono essere trattati congiuntamente in quanto connessi.

Tutti presentano profili di inammissibilità, in quanto in tema di azione di risarcimento dei danni da diffamazione, la ricostruzione storica dei fatti, la valutazione del contenuto degli scritti (in questo caso, dei messaggi inviati tramite Facebook sul profilo privato dei destinatari), l'apprezzamento in concreto delle espressioni usate come lesive dell'altrui reputazione, costituiscono oggetto di accertamenti in fatto, riservati al giudice di merito ed insindacabili in sede di legittimità se sorretti da idonea motivazione, mentre il controllo affidato alla Corte di cassazione è limitato alla verifica dell'avvenuto esame, da parte del giudice del merito, della sussistenza del requisito della continenza nell'esprimere i propri giudizi su un'altra persona e della avvenuta diffusione dei messaggi aventi intrinseca valenza diffamatoria tra più persone, restando estraneo al giudizio di legittimità l'accertamento relativo alla capacità diffamatoria delle espressioni in contestazione.

Pertanto, laddove sollecitano la Corte, riproducendo il testo dei messaggi inviati dalla S.G. agli amici e colleghi del M.G., ad apprezzarne direttamente la potenzialità denigratoria, i motivi vanno incontro al rilievo della inammissibilità.

Peraltro, essi pongono anche alcune questioni giuridiche, e sotto questo profilo sono infondati, dovendosi confermare la correttezza dei principi applicati dalla corte d'appello.

In primo luogo, è ben vero che ai fini della configurabilità della diffamazione è richiesto, in capo all'autore della condotta dedotta come lesiva dell'altrui onorabilità, solo il dolo generico e non anche il dolo specifico. Come precisato da Cass. n. 25420 del 2017, in tema di responsabilità civile per diffamazione, è necessario e sufficiente che ricorra l'elemento soggettivo del cd. dolo generico, anche nelle forme del dolo eventuale, cioè non è richiesta la volontà ma è sufficiente la consapevolezza di poter, con le proprie dichiarazioni, offendere l'onore e la reputazione altrui, la quale si può desumere anche dalla intrinseca consistenza diffamatoria delle espressioni usate.

E tuttavia, con valutazione in fatto non superabile, la corte d'appello ha escluso che le espressioni usate dalla B.B. esprimessero, oltre che una delusione personale e una certa preoccupazione sul conto del suo ex, anche la consapevolezza che quelle espressioni, pur non direttamente offensive, avrebbero potuto avere comunque l'effetto di tracciare un quadro non lusinghiero del ricorrente, dipinto indirettamente come una persona instabile e immatura.

Vi è poi da considerare la seconda questione, ovvero la configurabilità o meno del presupposto obiettivo della diffamazione, integrato dall'essere stata la comunicazione indirizzata a una pluralità di destinatari (v. Cass. n. 11271 del 2020)

Nel caso in cui, come nella specie, ci siano state più comunicazioni, ma tutte indirizzate ad un singolo destinatario, l'elemento oggettivo della diffamazione, integrato dalla diffusività della condotta denigratoria, potrebbe sussistere solo nell'ipotesi in cui l'agente, pur comunicando direttamente con un'unica persona, esprima la volontà o ponga comunque in essere un comportamento tale da provocare, da parte dell'agente medesimo, l'ulteriore diffusione del contenuto diffamatorio attraverso il destinatario.

Valutando le espressioni usate dalla controricorrente nei suoi messaggi con amici del M.G., la corte d'appello ha però preso in considerazione anche questo profilo ed ha escluso, con valutazione in fatto non sindacabile in questa sede, che in realtà le affermazioni della S.G., nel senso di pregare gli amici di non far sapere al M.G. dei suoi messaggi esprimenti preoccupazione sul suo conto, fossero surrettiziamente volte a sollecitare in effetti la

diffusione dei messaggi stessi e comunque di notizie preoccupanti sul conto del M.G. nell'ambiente musicale al quale tutte le persone coinvolte appartenevano.
Ne può ritenersi che il particolare strumento di comunicazione usato (messaggi inviati sul canale Facebook privato) si presti di per sé, per le caratteristiche intrinseche del mezzo di facilitare la diffusione delle comunicazioni, a far ritenere formata in capo al mittente l'accettazione del rischio di diffusione.
Diversamente opinando, l'apprezzamento aprioristico della potenziale idoneità diffusiva del mezzo di comunicazione usato, scisso dalla considerazione delle circostanze del caso concreto, avrebbe l'effetto di ribaltare impropriamente sul mittente di un messaggio con unico destinatario l'onere della prova di non aver voluto l'ulteriore diffusione del messaggio. Non si può quindi affermare, senza ribaltare la distribuzione degli oneri probatori, che in mancanza di una prova del divieto di diffusione da parte del mittente, si presume che i messaggi inviati tramite social network sui canali di posta privati siano destinati alla diffusione o che, comunque, il mittente abbia consapevolmente accettato il rischio della diffusione da parte del destinatario e debba subire, per questo, le conseguenze dell'eventuale diffusione qualora essa integri un obiettivo discredito della persona di cui si parla.
Nel caso di specie, la corte d'appello ha fatto corretto uso dei principi indicati, e non ha ritenuto provata in capo alla S.G. la volontà o l'accettazione del rischio che i suoi messaggi, sol perché indirizzati ad un destinatario determinato tramite Facebook, fossero diffusi ad altri".
*...Omissis...*
P.Q.M.
La Corte rigetta il ricorso. Compensa le spese del giudizio di legittimità tra le parti
*...Omissis...*

# IL COMMENTO

*di Antonio Maria Russo*

**Sommario:** 1. Il caso di specie. – 2. Elemento soggettivo e oggettivo della diffamazione. – 3. Brevi riflessioni.

Il presente contributo prende in esame una sentenza pronunciata il 4 marzo 2024 dalla Suprema Corte di Cassazione, n. 5701, la quale si sofferma sulla individuazione degli elementi costitutivi del reato di diffamazione. In specie, la Corte, aderendo a un consolidato orientamento giurisprudenziale, rileva come la fattispecie diffamatoria richieda l'accertamento in capo al soggetto agente del dolo generico, anche se eventuale, e non nel dolo specifico. In materia di responsabilità civile per diffamazione è dunque sufficiente la presenza dell'elemento soggettivo del dolo generico, anche se eventuale, ovverosia non è richiesta una specifica volontà lesiva del soggetto agente, ma la consapevolezza di quest'ultimo di poter, tramite le proprie dichiarazioni, offendere l'onore e la reputazione altrui. L'autore esamina la decisione di cui si tratta e il caso di specie, in cui le comunicazioni presuntivamente diffamatorie erano state trasmesse tramite *Facebook* mediante l'invio di molteplici messaggi privati indirizzati a singoli destinatari, approfondendo i presupposti per la configurabilità della diffamazione anche alla luce dello sviluppo della materia dovuto alle nuove tecnologie.

*The present contribution examines a judgment issued on March 4, 2024, by the Supreme Court of Cassation, no. 5701, which focuses on identifying the constitutive elements of the crime of defamation. Specifically, the Court, adhering to a consolidated jurisprudential orientation, observes that the defamatory conduct requires the ascertainment of generic intent (dolo generico) on the part of the acting subject, even if only potential, and not specific intent (dolo specifico). In terms of civil liability for defamation, the presence of the subjective element of generic intent, even if only potential, is therefore sufficient, meaning that a specific injurious intent on the part of the acting subject is not required, but rather the awareness that the statements could potentially offend the honor and reputation of others. The author examines the decision in question and the specific case, in which the allegedly defamatory communications were transmitted via Facebook by sending multiple private messages to individual recipients, delving into the prerequisites for the configurability of defamation in light of the development of the matter due to new technologies.*

## 1. Il caso di specie

Per meglio comprendere la decisione resa nel caso di specie occorre necessariamente ripercorrerne le tappe fondamentali.
Con la Sentenza in esame, la Suprema Corte di Cassazione ha escluso la configurabilità del reato di diffamazione nel caso in cui l'invio di messaggi asseritamente diffamatori sia stato perpetrato attraverso la piattaforma *social* "*Facebook*", ma in via individuale e "riservata", tramite messaggi privati a singoli destinatari, ritenendo che non venga così soddisfatto il requisito della divulgazione a più destinatari.
È stato in tal senso respinto, allora, il ricorso di M.G. contro S.G., la quale aveva inviato messaggi privati a due amici del ricorrente "*con l'intento preciso di danneggiarlo e di isolarlo dal contesto degli amici e colleghi di lavoro*".
In primo grado, il Tribunale aveva dato ragione a M.G., con la relativa condanna di S.G. al risarcimento di Euro 5.000 per danni morali.

Tuttavia, successivamente, la Corte d'Appello di Milano ha ribaltato tale decisione, sostenendo che non vi fossero gli elementi propri della diffamazione, poiché i messaggi erano stati inviati individualmente ai destinatari e uno per volta, in modo riservato e senza eccedere i limiti della continenza.
La Corte ha così specificato che mancava il requisito oggettivo richiesto ai fini della configurabilità della diffamazione, ovverosia la comunicazione diretta a plurimi destinatari (1).
Inoltre, è stato ritenuto dalla medesima Corte che l'oggetto delle comunicazioni non avesse carattere denigratorio, ma che esse esprimessero solo il sentimento di delusione personale della S.G. e le preoccupazioni della stessa riguardo alla condotta ritenuta immatura del proprio *ex* compagno M.G.
Infine, la Suprema Corte di Cassazione ha concluso per la inammissibilità dei motivi articolati da M.G. nel proprio ricorso, statuendo, tra l'altro, la regola per cui non è possibile desumere dalle caratteristiche intrinseche del mezzo di comunicazione utilizzato la volontà divulgativa del mittente/agente, senza che ciò comporti un ribaltamento del riparto degli oneri probatori.

## 2. L'elemento soggettivo e oggettivo della diffamazione

In principio è d'uopo rammentare quanto previsto ai sensi dell'art. 595 c.p., che punisce "*chiunque, fuori dei casi indicati dall'articolo precedente, comunicando con più persone, offende l'altrui reputazione*".
In proposito, è del tutto ovvio che quello di cui si tratta è un giudizio civile e non penale, così come – per converso – che lo stesso giudice civile può accertare incidentalmente la ricorrenza di un fatto reato nella vicenda sottoposta alla sua attenzione e che ai sensi dell'art. 185 c.p. ogni illecito penale costituisce un illecito civile (2).
Anzi, prima delle storiche decisioni della Suprema Corte intervenute nell'anno 2003 la commissione di un reato costituiva la principale ipotesi di "caso previsto dalla legge" che consentiva la liquidazione del danno patrimoniale ai sensi dell'art. 2059 c.c. (3) Peraltro, se – come si è appena detto – ogni reato integra gli estremi di un illecito aquiliano non vale la reciproca, secondo una considerazione che sta alla base delle differenze che sussistono fra diffamazione penale e civile (4): ma poiché esse non vengono in rilievo nel caso di specie, nel prosieguo l'elaborazione dei formanti dottrinali e giurisprudenziali verrà considerata unitariamente (5).
Ciò premesso, vale qui la pena di rammentare che il concetto di reputazione è stato prevalentemente definito come quella particolare considerazione goduta dall'individuo nella comunità di appartenenza (6).
In dottrina, si è parlato in tal senso di "*riflesso oggettivo dell'onore inteso in senso ampio*" (7).
Trattasi sostanzialmente dell'insieme delle qualità che definiscono il valore di un individuo all'interno della società.
Non manca però chi ha obiettato che, poiché non tutti gli individui godono di una particolare considerazione nella propria comunità di riferimento, il reato non si perfezionerebbe nel caso in cui l'agente si "scagliasse" contro un soggetto con una reputazione già compromessa.
Tuttavia, si è affermato che anche in detto caso può aversi un reato di diffamazione, poiché i termini di onore e reputazione sono da intendersi in senso formale "*in quanto concernono sentimenti e valutazioni relativi a ogni individuo, a prescindere dai suoi meriti effettivi*" (8).
Requisito fondamentale, come sancito dalla pronuncia in esame, è poi la "*comunicazione con più persone*" dei termini offensivi.
Tale divulgazione può avvenire sia in modo verbale che per iscritto e altresì a mezzo *social*, ma per divenire penalmente illecita deve essere percepita da almeno due soggetti.
In tal senso, la Corte di Cassazione ha sancito che si configura una comunicazione con più individui anche allorquando il soggetto agente ponga in essere la propria condotta divulgativa in modo del tutto riservato nei

(1) L'art. 595, comma 1, c.p. così statuisce "*chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a milletrentadue euro*".

(2) L'art. 185 c.p. così statuisce: "[o]*gni reato obbliga alle restituzioni, a norma delle leggi civili. Ogni reato, che abbia cagionato un danno patrimoniale o non patrimoniale, obbliga al risarcimento il colpevole e le persone che, a norma delle leggi civili, debbono rispondere per il fatto di lui*". Ebbene, tale articolo svolge un ruolo rilevante nella disciplina delle sanzioni civili derivanti dal reato. Difatti, al secondo comma dell'articolo appena citato, è previsto il risarcimento del danno da reato, sia patrimoniale che non patrimoniale. Perciò, condividendo il pensiero di Zencovich, si potrebbe affermare che l'art. 185 c.p. si pone quale "ponte" tra il sistema penale e il sistema civile.

(3) Cass., 31 maggio 2003, n. 8827, in *Arch. civ.*, 2004, 162; Cass., 31 maggio 2003, n. 8828, *Ibidem*, 2004, 415.

(4) Per un ampio approfondimento sul tema della diffamazione in ambito civile e penale si rimanda a un interessante testo che ne ripercorre le problematiche sottese: Cassano, Sgroi, *La diffamazione civile e penale*, Milano, 2011.

(5) Di recente, per un'ampia citazione di dottrina e giurisprudenza, Tassone e Cariani, *La reputazione del minore, delle vittime e dei soggetti deboli* online, in Iaselli (a cura di), *Investigazioni digitali*, Milano, 2021, 221 ss.

(6) Cass., 21 settembre 2012, n. 43184, in banca dati *One Legale*.

(7) Antolisei, *Manuale di Diritto Penale, Parte Speciale II*, XV, Milano, 2002, 192.

(8) Cass., 4 luglio 2008, n. 35032, in banca dati *One Legale*.

confronti di un unico destinatario, purché vi sia la volontà "*da parte dell'agente medesimo, dell'ulteriore diffusione del contenuto diffamatorio attraverso il destinatario*" (9).
L'ultimo requisito è invece rappresentato dalla necessaria assenza del soggetto leso, il quale, come ampiamente messo in luce dalla dottrina (10), non deve essere presente nel momento dell'azione criminosa.
In proposito, è interessante riportare quanto spiegato da un'autorevole voce allorquando delimita la reputazione e l'ingiuria, soffermandosi sulla reputazione: "*la reputazione non è altro che il riflesso oggettivo dell'onore inteso in senso ampio, e cioè la valutazione che il pubblico fa del pregio dell'individuo e, quindi, la stima che questi gode fra i consociati. [...] [L]a base della reputazione è la stessa di quell'onore e decoro di cui il codice parla a proposito dell'ingiuria* (11) *e, perciò, comprende tutte le qualità (morali, intellettuali, fisiche, ecc.) che concorrono a determinare il valore sociale della persona*" (12).
Ebbene, è da ritenersi diffamatoria ogni condotta che, se tenuta in presenza del soggettivo passivo, costituirebbe ingiuria e anche la giurisprudenza di merito precisa che "[l]*a realizzazione del reato di diffamazione richiede la contestuale ricorrenza dei seguenti elementi: a) l'assenza dell'offeso, da intendersi come impossibilità per il soggetto passivo di percepire la condotta diffamatoria e difendersi dall'addebito; b) la comunicazione, anche se non contemporanea e diretta, con più persone (almeno due), in grado di percepirne il contenuto; c) l'offesa all'altrui reputazione, quale opinione sociale dell'onore di una persona, attraverso l'utilizzo di espressioni attributive di qualità sfavorevoli o comunque idonee a gettare una luce negativa su quest'ultima*" (13).
Sotto l'aspetto soggettivo, la giurisprudenza è ormai unanime nel ritenere che, la fattispecie *de qua* sia sorretta dal dolo generico, anche eventuale.
Al contrario non è necessario il dolo specifico, il c.d. *animus diffamandi*, ossia l'intenzione di causare un effettivo o potenziale danno alla reputazione della persona offesa: "[n]*ell'accertamento dell'elemento soggettivo della diffamazione, sono irrilevanti l'intenzione, lo scopo, le particolari finalità, le motivazioni dell'agente, giacché l'art. 595 c.p. non esige il dolo specifico, essendo invece che sussista quello generico, inteso come coscienza e volontà della condotta adottate, cioè della comunicazione dell'addebito offensivo ad almeno due persone, con la consapevolezza dell'idoneità delle espressioni adottate a menomare apprezzabilmente la reputazione del soggetto passivo*" (14).
Come anticipato, il dolo generico può assumere anche la forma del dolo eventuale, poiché è sufficiente che il soggetto agente in modo del tutto consapevole faccia utilizzo di epiteti o espressioni che possano risultare offensivi nell'ambiente sociale in base al significato oggettivo che viene loro attribuito, al di là delle intenzioni del soggetto agente: "[p]*er la ravvisabilità del delitto di diffamazione, è sufficiente la sussistenza del dolo eventuale, e cioè che l'autore abbia previsto ed accettato il rischio di verificarsi della lesione al bene protetto; tale giudizio di prevedibilità va effettuato con riferimento all'agente modello, in rapporto all'attività concretamente svolta*" (15).
Infine, per quanto attiene all'elemento oggettivo della diffamazione risulta necessario in detta sede rilevare che, essendo configurabile quale reato a forma libera, la condotta del soggetto agente si perfeziona allorquando venga offesa la reputazione del soggetto passivo purché egli sia assente e che la stessa divulgazione avvenga attraverso ogni mezzo idoneo ai fini della comunicazione a plurimi destinatari.

## 3. Brevi riflessioni

Nell'era digitale la comunicazione avviene sempre di più per mezzo delle piattaforme *social* che negli ultimi anni stanno influenzando in modo sempre più incisivo il vivere umano.
Il noto brocardo *ubi societas ibi ius* sicuramente dovrebbe trovare applicazione nella società c.d. "virtuale", nel senso che – come forma dell'agire umano – è anch'essa in tutto e per tutto soggetta all'ordinamento giuridico.
Ciò non vuol dire, peraltro, che il modo in cui il diritto si applica e/o i problemi che incontra non mutino, intanto perché il diritto deve evolvere insieme alla società che progredisce: il diritto è sempre stato "essenza regolatrice" e deve continuare a essere tale anche per le nuove tecnologie, garantendo così certezza e non frammentarietà, pena il suo arretramento di fronte a una prassi "tecnologica" che avanza.
Perciò, se sono le nuove tecnologie a influenzare il diritto, questo deve per un verso regolamentarle, ma per l'altro evolversi tenendo conto delle necessità di adattamento che essere richiedono, al fine di regolare con coerenza la "nuova società" e non essere un *héritage historique*.
Invero, il diritto è una materia viva e, come tale, deve essere trattata.
Senza allargare il discorso al diritto dell'era digitale e i tanti temi che lo stesso impone di affrontare – come

(9) Cass., 12 giugno 2020, n. 11271, in banca dati *One Legale*.

(10) Antolisei, *Manuale di Diritto Penale, Parte Speciale I*, IX, Milano, 1986, 165.

(11) Ai sensi dell'art. 594 c.p. l'ingiuria consiste nel fatto di colui che "*offende l'onore o il decoro di una persona presente*".

(12) Antolisei, *Manuale di Diritto Penale*, cit., 166.

(13) Cass., 5 maggio 2021, n. 173589, in banca dati *One Legale*.

(14) Cass., 19 dicembre 2001, n.2972, in banca dati *One Legale*.

(15) Cass., 19 dicembre 2001, n. 2972, cit.

quelli della responsabilità del *provider* e della personalità (elettronica?) (16), in questa sede ci si limita a evidenziare che la decisione della Suprema Corte di Cassazione pare coerente con le telegrafiche considerazioni appena esposte.

In effetti, la Corte ha stabilito che il requisito della comunicazione avvenuta con più destinatari ai sensi dell'art. 595 c.p. sussiste solo se viene fornita la prova – in questo caso non fornita – della volontà esplicita del mittente di divulgare il messaggio a una pluralità di persone e non è pensabile affermare che lo strumento di diffusione/comunicazione utilizzato (che sia *Facebook*, *Instagram*, etc.) possa di per sé dare una tale dimostrazione: ossia – per usare le parole della decisione – che esso sia idoneo "*per le caratteristiche intrinseche del mezzo di facilitare la diffusione delle comunicazioni, a far ritenere formata in capo al mittente l'accettazione del rischio di diffusione*", anche alla luce delle nuove frontiere della comunicazione a distanza di tipo telematico (17).

In altri termini, ai fini dell'accertamento incidentale della fattispecie di diffamazione e dunque della responsabilità in capo all'agente per i danni cagionati al soggetto passivo, non rileva il mezzo di comunicazione utilizzato e dunque la potenziale capacità di quest'ultimo di raggiungere un numero indeterminato di destinatari, qualora i messaggi presuntivamente diffamatori siano stati trasmessi, separatamente, a singoli individui.

Difatti, ai fini della configurabilità del dolo generico o eventuale è necessario che l'agente, pur trasmettendo singoli messaggi, voglia o sia comunque consapevole della diffusione degli stessi a terzi, accettando dunque il rischio della loro divulgazione oltre la sfera del singolo destinatario: secondo una consapevolezza che deve essere accertata, dal giudice di merito, anche alla luce del contenuto delle singole comunicazioni.

Diversamente, come affermato dalla Sentenza, verrebbe violato l'ordinario riparto dell'onere probatorio, obbligando il mittente a dimostrare una circostanza negativa ossia che la sua volontà *non* era quella di provocare la diffusione del messaggio.

---

(16) Ruffolo, *Il problema della "personalità elettronica"*, in *Journal of Ethics and Legal Technologies*, 2020, 75-88; Tassone, *Riflessioni su intelligenza artificiale e soggettività giuridica*, in *questa* ***Rivista***, 2023, 2, 1-20.

(17) Sul punto si richiama un interessante articolo di Oggiano, *Diffamazione con il mezzo informatico: la Cassazione indica i requisiti oggettivi della condotta e si sofferma sui limiti di sindacabilità in sede di legittimità*. Il testo è disponibile nella versione on line di *questa* ***Rivista***, in *www.dirittodiinternet.it*.

# Scrittura privata inviata come allegato alla pec: data certa rispetto ai terzi e onere della prova

Corte di Cassazione; sezione prima; ordinanza 13 febbraio 2024, n. 10091; Pres. Ferro; Rel. Fidanzia; Gieffe s.r.l. (Avv. Meloni, Campana) c. Fallimento Bricosarda s.r.l. (avv. Fodde).

*La indicazione del contenuto di una scrittura privata in un atto avente data certa non è un fatto idoneo ad attribuire data certa.*
*La ricevuta di consegna del messaggio pec non è prova del contenuto del file allegato al messaggio pec, che non acquista data certa.*

*...Omissis...*
Con decreto depositato il 2.10.2018 il Tribunale di Cagliari ha rigettato l'opposizione *ex* art. 98 legge fall. proposta da Gieffe Srl avverso il decreto con cui il G.D. del fallimento Bricosarda Srl aveva rigettato la sua domanda di insinuazione del credito dell'importo di Euro 231.540,70, richiesto a titoli di canoni d'affitto d'azienda di cui al contratto sottoscritto tra le parti in data 8.7.2010.
Il Tribunale ha condiviso l'impostazione del G.D., ritenendo il contratto di affitto d'azienda in oggetto non opponibile alla procedura in quanto privo di data certa.
In particolare, ha osservato che, pur potendo costituire un significativo elemento di prova della data certa la pec datata 21.1.2013 con cui la società I Gabbiani Immobiliare (poi fusa in Gieffe Srl) aveva chiesto il pagamento dei canoni insoluti imputandoli "al contratto in data 8.7.2010", il cui contenuto era stato descritto nei suoi tratti essenziali nella nota sopra richiamata (tale per cui, secondo il decreto impugnato, se tale nota "fosse dotata di data certa, estenderebbe la certezza della data alla scrittura privata ed alle previsioni essenziali in essa contenute"), tuttavia, tale documento non era dotato di data certa, essendovi solo la prova che, in data 21.1.2013, l'odierna ricorrente aveva inviato una pec alla Bricosarda, ma non anche che il documento allegato alla pec fosse la nota prodotta.
Il Tribunale di Cagliari ha quindi ritenuto che l'opponente avrebbe dovuto corrispondentemente riprodurre il documento già in formato elettronico, così da poter verificare se allegata alla pec vi fosse effettivamente la comunicazione prodotta.
*...Omissis...*
Lamenta la ricorrente che il giudice di primo grado, nonostante l'inequivoca facoltà concessa alla parte dalla legge (art. 16-*bis* legge cit.), all'atto della prima costituzione in giudizio, di depositare i documenti in cartaceo, ha ritenuto imprescindibile, per provare il contenuto di un documento allegato ad una pec, la produzione dello stesso in via telematica, non considerando che il deposito in via telematica costituisce una semplice alternativa e che la prova del contenuto dell'allegato può essere fornita producendo documentazione attestante l'accettazione e la consegna del messaggio inviato via pec.
La ricorrente ha, altresì, osservato che in nessuna fase della procedura (né di ammissione, né in sede di opposizione allo stato passivo) la procedura aveva contestato di aver ricevuto le diffide - e cioè la pec - con quel contenuto.
Doveva, pertanto, ritenersi pacifico che, per effetto della mancata contestazione da parte del fallimento, le pec avessero quel contenuto, incombendo semmai al fallimento provare un allegato diverso da quello prodotto in cartaceo.
Il Tribunale ha quindi omesso di decidere su un fatto decisivo costituito dalla data certa del credito derivante dalle lettere oggetto di discussione tra le parti.
In subordine, la ricorrente allega che il giudice di primo grado avrebbe violato gli artt. 101 comma 2 e 112 cod. proc. civ., avendo posto a fondamento della propria decisione una questione rilevabile d'ufficio senza assegnare alle parti un termine per depositare memorie sul punto.
Il motivo presenta concomitanti profili di infondatezza e inammissibilità, anche se la motivazione del Tribunale deve essere corretta in diritto a norma dell'art. 384 ult. comma cod. proc. civ.
Va preliminarmente osservato che questa Corte (vedi Cass. n. 32165/2023), nell'esaminare un'analoga questione in cui era stato invocato dall'istante che il documento allegato ad una posta elettronica certificata è attratto al regime di quest'ultima, ed è pertanto atto opponibile a terzi, ha affermato che "la posta elettronica certificata dimostra l'invio e la ricezione del messaggio,

ma non garantisce il contenuto del documento allegato".
Non si può, in altri termini, dalla circostanza che la posta elettronica è certificata, dedurre che anche il documento allegato lo è, o meglio, che quel documento è riferibile al suo autore, e che ha effettivamente quel contenuto. Si supponga il caso in cui con posta certificata si invia un documento dal falso contenuto, o proveniente da un terzo: si dovrebbe dire che, avendo il mittente certificato la posta (ossia attestato che proviene da lui e che è stata spedita a quell'ora) ha altresì attestato che il documento allegato è vero o che è riferibile ad un terzo...".
Dunque, la Pec è in grado di attestare in maniera certa l'avvenuta trasmissione e ricezione del messaggio, le modalità di spedizione (data, ora e formato) ed anche il suo contenuto, ma limitatamente alla Pec stessa, non al file allegato ad essa. Pertanto, se alla Pec è stato allegato un file con un determinato nome, estensione, formato e dimensioni la ricevuta lo attesterà, ma non farà prova del contenuto di quel file, occorrendo, a tal fine, che sul file allegato sia apposta la firma digitale, che certificherà la provenienza del documento e la sua integrità.
Ne consegue che non è corretta la stessa affermazione del tribunale secondo cui la produzione del documento (pec) in formato elettronico sarebbe idonea a fornire la prova del contenuto del documento allegato (e della data certa).
Non corretta giuridicamente è, inoltre, l'affermazione del Tribunale secondo cui la data certa di un documento (nel caso di specie, la nota del 21.1.2013 inviata via pec) che richiama, al suo interno, il contenuto di un contratto nei suoi tratti essenziali (nella specie, il contratto di affitto d'azienda) "estenderebbe la certezza della data anche alla scrittura privata ed alle previsioni essenziali in essa contenute". Sul punto questa Corte (vedi Cass. n. 34755/2023) ha recentemente affermato – nell'esaminare una questione in cui l'istante intendeva provare la data certa di un mandato professionale desumendola dalla menzione dello stesso all'interno di una domanda di concordato preventivo depositata in giudizio – ..." che la mera menzione di un mandato professionale supposto quale preesistente rispetto ad un atto, depositato in giudizio e da quel momento avente natura di data certa, non conferisce alcuna data certa anche al contratto cui il mandato citato ineriva, se non ne sia contestualmente depositato il relativo documento: atteso che l'istituto della data certa, ai fini della opponibilità, riguarda un atto che, con un giudizio di certezza, viene in rilievo nella sua precisa, conoscibile, dunque completa, esistenza, non è certo sufficiente, a tal fine, la mera menzione del suo contenuto in altro atto.
Nel caso di specie, non vi sono i presupposti per il riconoscimento della data certa, cioè della violazione da parte del giudice di merito dei criteri codicistici enunciati, in quanto con la domanda di concordato preventivo quel mandato non risultava depositato, ma solo menzionato nel corpo del ricorso e peraltro neanche nella sua integralità...".
Il principio enunciato da questa Corte nella predetta ordinanza risulta pienamente applicabile anche al caso di specie.
*...Omissis...*

# COMMENTO

*di Marcello Stella*

**Sommario:** 1. Un caso clinico: allegato alla pec e data certa *ex* art. 2704 c.c. – 2. L'onere soggettivo della prova del contenuto del documento allegato alla pec. – 3. La prova della esistenza degli allegati al messaggio di posta elettronica certificata nel processo telematico.

La Cassazione afferma che la spedizione di una scrittura privata come allegato a una pec non è un fatto idoneo a fare acquistare data certa, rispetto ai terzi, alla scrittura privata che ne sia priva. Il commento esprime le ragioni di dissenso rispetto al *dictum* della Corte.

*In the case at hand, the Supreme Court held that the date of a private deed does not become certain with respect to third parties, even if the deed was sent as an attachment to a certified electronic mail. The Author disagrees with the decision, in the light of the statutory rules regarding certified electronic mail.*

## 1. Un caso clinico: documento allegato alla pec e data certa *ex* art. 2704 c.c.

La vicenda appare tanto frequente (1) quanto idonea a fornire materia, qualcuno avrebbe detto, per un nutriente caso di "clinica retrospettiva" del diritto: di quelli che andrebbero proposti agli studenti per consentir loro di toccare con mano il concreto atteggiarsi dei principii nella dinamica del processo su fattispecie tangibilmente concrete.

Qui i principii rilevanti sono almeno tre: inopponibilità della scrittura privata priva di data certa al fallimento e alla massa dei creditori; natura processuale o sostanziale del fatto (e in questo secondo caso: fatto costitutivo o impeditivo?) della certezza della data della scrittura privata ed onere soggettivo della prova; principio di non contestazione.

Ed ecco la vicenda: un creditore del fallito domanda la ammissione nello stato passivo di crediti per canoni di affitto d'azienda insoluti. Il giudice delegato prima e il collegio del tribunale in sede di opposizione allo stato passivo poi respingono la domanda ritenendo priva di data certa ed inopponibile al fallimento la scrittura privata.

Il creditore, che aveva optato di costituirsi nelle tradizionali forme cartacee (*olim* ancora permesse), si era limitato a produrre in giudizio le copie analogiche delle ricevute di accettazione e consegna di un messaggio di posta elettronica certificata, che risultava contenere in allegato una diffida ad adempiere. La diffida menzionava la data di stipulazione del contratto di affitto. Il creditore, tuttavia, aveva omesso di produrre il documento informatico allegato alla pec, appunto la diffida "enunciativa" della scrittura privata. Di talché, a giudizio del tribunale, non era dimostrato che il contenuto del documento cartaceo prodotto in giudizio corrispondesse a quello del file a suo tempo inviato come allegato alla pec.

Nel respingere il ricorso per cassazione del creditore, dichiarato inammissibile, la Cassazione ha tuttavia sentito il bisogno di correggere la motivazione del tribunale.

Il Giudice di legittimità ha puntualizzato, da un lato, che neppure la tempestiva produzione del documento informatico asseritamente allegato al messaggio pec sarebbe stata idonea a stabilire con certezza la data della scrittura privata, dal momento che la diffida ad adempiere si limitava soltanto a menzionare la esistenza dell'anteriore contratto.

Dall'altro lato, la Cassazione ha affermato che la efficacia di prova legale della data di spedizione e di ricevimento di un messaggio pec non si estende al contenuto di eventuali allegati al messaggio.

In altri termini, se anche il creditore avesse prodotto copia informatica del documento informatico (ossia della diffida "enunciante", o finanche il contratto di affitto d'azienda stesso) inviato a suo tempo come allegato alla pec, ciò non sarebbe bastato ad integrare il requisito della data certa della scrittura privata.

## 2. L'onere soggettivo della prova del contenuto del documento allegato alla pec

*Nulla quaestio* riguardo al principio di diritto di cui alla prima massima.

Per attribuire data certa a una scrittura privata non è sufficiente che questa sia semplicemente menzionata da un altro atto avente data certa. Così, non poteva dirsi idonea a dimostrare la anteriorità del contratto di affitto la semplice menzione della sua esistenza in una diffida stragiudiziale formata dal medesimo creditore, ancorché inviata a mezzo pec alla impresa debitrice prima della dichiarazione di fallimento.

Nel solco di una giurisprudenza consolidata (2), ai fini dell'art. 2704 c.c. e della opponibilità a terzi della data di una scrittura privata non autenticata, il "fatto atipico", da cui risulti l'anteriorità della formazione del documento, dev'essere fornito di un livello di certezza uguale a quello dei fatti tipici menzionati nella prima parte della stessa norma.

La mera indicazione del documento in un altro atto, seppure quest'ultimo sia munito di data certa, non è contemplata dalla norma, e non garantirebbe che l'atto citato sia proprio quello rappresentato dal documento di cui trattasi (3).

La giurisprudenza, a tale stregua, ha affermato che la "riproduzione", più o meno integrale, del contenuto della scrittura privata in un atto processuale di parte (l'atto di citazione), avente data certa in ragione della notificazione mediante ufficiale giudiziario, non è un fatto idoneo a stabilire l'anteriorità della formazione del documento con certezza analoga a quella derivante dalla morte di uno dei sottoscrittori o dalla riproduzione della scrittura in un atto pubblico (4).

(1) V., infatti, per un caso analogo in cui un geometra adduceva come prova scritta del proprio credito, oggetto della domanda di ammissione nello stato passivo, varie pec recanti come allegati "documentazione in via esclusiva riferibile agli incarichi professionali correlati all'appalto", Cass. 22 aprile 2024, n. 10717. In tale precedente, tuttavia, la Cassazione ha respinto il motivo siccome inammissibile, poiché ritenuto volto a sollecitare un rinnovato apprezzamento delle prove da parte della S.C. e, di conseguenza, tale decisione non si lascia apprezzare per un particolare valore nomofilattico.

(2) Di cui è recente espressione il precedente di Cass. 12 dicembre 2023, n. 34755 citato dalla motivazione della pronuncia che si commenta.

(3) Cass. 23 ottobre 2019 n. 27192.

(4) Cass. 19 novembre 2009, n. 24414, considerata in Patti, *Prove*, Bologna, 2015, 427, nota 4. Tale pronuncia si richiama al precedente di

Se per "riproduzione" si intende dunque, in senso atecnico, la indicazione dell'esistenza o la trascrizione o il riassunto del contenuto della scrittura privata compiuti in un atto processuale di parte, che pure sia stato notificato a mezzo u.g., deve senz'altro negarsi la idoneità di tale fatto a dimostrare l'anteriorità del documento con il grado di certezza richiesto dall'art. 2704 c.c.

Ci si potrebbe chiedere, tuttavia, se analoga conclusione debba valere anche nella diversa ipotesi in cui la scrittura privata, anziché essere semplicemente "enunciata", sia invece graficamente e per intero riprodotta, come copia per immagine, nel corpo del messaggio di posta elettronica certificata.

Nella diversa costellazione casistica che veniamo ora ipotizzando si avrebbe, a ben vedere, una copia informatica di un documento analogico, idonea a dimostrare la esistenza dell'originale, salvo contestazione di conformità della riproduzione all'originale, che ben potrebbe giovarsi della certezza della data di spedizione a mezzo posta elettronica certificata.

Desta invece perplessità l'affermazione della S.C., specie se considerata in modo avulso dalle peculiarità del caso concreto, in base a cui la spedizione di un documento informatico come allegato a una pec non sarebbe idonea ad attribuire data certa al documento. Certo, la mera produzione cartacea del documento che la parte affermi di aver spedito come allegato informatico a una pec di per sé non potrebbe mai dimostrare che il file allegato alla pec avesse proprio *quel determinato contenuto*, corrispondente al documento cartaceo prodotto dalla parte (in difetto di qualsivoglia attestazione da parte di pubblico ufficiale abilitato a certificare la conformità al *file* spedito). Ma ciò non vuol dire, invece, che il file allegato alla pec non acquisti data certa dal momento della spedizione e ricevimento, come subito diremo.

Prima di interrogarsi sul mezzo di prova, occorre tuttavia chiedersi su quale parte del processo gravi il relativo onere dimostrativo.

La S.C., nella fattispecie, non solo ha omesso di confrontarsi con l'indirizzo altrettanto consolidato in base a cui, riguardo ad atti negoziali ricettizi inviati tramite posta raccomandata, l'onere di dimostrare che il plico è privo di contenuto o abbia un contenuto diverso da quello descritto dal mittente, volta che sia provato l'invio e la ricezione del plico (tramite produzione della cartolina di ricevimento o, se il destinatario era irreperibile, dell'avviso di giacenza nell'ufficio postale), grava sul destinatario della raccomandata (5), ma neppure sembra aver tenuto conto del fatto che la giurisprudenza delle Sez. Un. qualifica come eccezione in senso lato, avente ad oggetto un fatto impeditivo, quella di carenza di data certa della scrittura privata.

Per quanto concerne il primo profilo, il ribaltamento dell'onere soggettivo della prova del contenuto del plico raccomandato presuppone che la parte interessata a giovarsi dell'effetto sostanziale dell'atto recettizio abbia allegato puntualmente il contenuto dell'atto spedito tramite raccomandata. Di contro, "la mancanza di una puntuale indicazione del testo della lettera asseritamene interruttiva esonera il destinatario dal provare l'effettivo contenuto di tale lettera" (6).

Si tratta di verificare se questi stessi principii si attaglino anche al caso della spedizione di un messaggio con allegati a mezzo posta elettronica certificata, al di fuori, beninteso, del procedimento notificatorio dove la prova del contenuto dei documenti o degli atti notificati è affidata alla relazione di notificazione (7).

Pur assodato che il curatore non è un successore del fallito e va considerato terzo rispetto alla scrittura privata invocata dal creditore (8), non può sottacersi che

Cass. 15 novembre 1995, n. 11824. In quel precedente più risalente si legge: "il fatto che un documento *sia indicato* in un atto introduttivo del giudizio non è situazione idonea a conferire al documento (solo successivamente depositato nel fascicolo) ed all'atto, data anteriore alla notifica delle citazione stessa con il criterio di certezza richiesto dall'art. 2704 c.c., non rientrando il caso in alcuna delle situazioni specifiche previste dall'art. 2704, né integrando le altre situazioni che in base allo stesso articolo stabiliscono in modo egualmente certo l'anteriorità della formazione del documento" (ns. enfasi).

(5) C. App. Milano 15 novembre 2022 n. 882; Cass. 28 settembre 2017 n. 22687; Cass. 13 maggio 2014, n. 10389; Cass. 24 giugno 2013 n. 15762; Cass. 23 giugno 2011 n. 13877; Cass. 7 aprile 2009 n. 8409; Cass. 3 luglio 2003 n. 10536; Cass. 11 maggio 2006 n. 10849. In ambito tributario, con riferimento alla notificazione a mezzo posta raccomandata della cartella di pagamento, Cass. 21 settembre 2023, n. 27004: "*in tema di notifica della cartella di pagamento mediante raccomandata, la consegna del plico al domicilio del destinatario risultante dall'avviso di ricevimento fa presumere, ai sensi dell'art. 1335 c.c., in conformità al principio di cd. vicinanza della prova, la conoscenza dell'atto da parte del destinatario, il quale, ove deduca che il plico non conteneva alcun atto o che lo stesso era diverso da quello che si assume spedito, è onerato della relativa prova*".

(6) Cass. 3 luglio 2003, n. 10536.

(7) Questo è il campo, naturalmente meglio arato dalla dottrina processualcivilistica, in cui è ben presto venuta affermandosi una giurisprudenza volta a valorizzare il principio di raggiungimento dello scopo, che ha degradato a mera irregolarità la spedizione di un atto processuale in un formato diverso da quello consentito dalle regole tecniche (es. file con estensione .word, anziché .pdf), rifiutandosi di ricondurre alla nullità o addirittura alla inesistenza pure la conseguente discrepanza tra il contenuto della relazione di notificazione, che dia atto della trasmissione di un file recante una certa estensione, e l'effettiva estensione del file allegato al messaggio pec (diversa, appunto, dalla descrizione offerta dalla relazione di notificazione). Particolarmente critica rispetto a tale giurisprudenza della Cassazione appare Porcelli, *Le comunicazioni e le notificazioni*, in Ruffini, *Il processo telematico nel sistema del diritto processuale civile*, Milano, 2019, 329 ss., spec. 406-409. Sulla notificazione elettronica nei sistemi francese e spagnolo, Mancuso, *Le notificazioni civili: il perfezionamento*, Torino, 2015, 208-216.

(8) Cass. sez. un. 20 febbraio 2013, n. 4213, in *Fall.*, 2014, 175 ss., con nota di Ficarella, *L'eccezione di carenza di «data certa» del documento nel procedimento di accertamento del passivo*.

il curatore e, oggi, il liquidatore giudiziale non è invece terzo rispetto alla fonte di prova: vale a dire alla casella di posta elettronica certificata dell'impresa fallita.
Difatti, in base all'art. 148 cc.ii., che disciplina uno degli effetti c.d. personali derivanti dalla apertura della liquidazione giudiziale (9), il debitore è tenuto a "consegnare" la corrispondenza, *inclusa quella elettronica*, al liquidatore.
Ne consegue che il curatore è o deve presumersi sia in potere di verificare il contenuto della casella pec dell'imprenditore fallito. E il silenzio del curatore, come vedremo, non può ritenersi del tutto privo di significato ai fini dell'art. 115 c.p.c., a fronte di una domanda di ammissione di credito che pretenda basarsi sull'invio a mezzo pec di una scrittura privata.
Tuttavia, date le caratteristiche "fenomeniche" della pec, mittente e destinatario si trovano in posizione di perfetta equidistanza, per così dire, dalla fonte di prova.
Il mittente, infatti, e a differenza della spedizione cartacea con raccomandata, è in grado di dimostrare non solo la data di spedizione e di ricevimento del messaggio di posta elettronica certificata ma anche l'esatto contenuto degli allegati informatici al messaggio pec inviato.
Sarebbe dunque incongruo fare operare in questo contesto le presunzioni giurisprudenziali e la conseguente inversione dell'onere della prova che si sono vedute affiorare dalla giurisprudenza a proposito della spedizione di un atto ricettizio a mezzo posta raccomandata. Tali approdi giurisprudenziali, tuttavia, non è escluso possano sovvenire nella circostanza particolare in cui il mittente affermi e dimostri di aver perduto il messaggio di posta elettronica certificata originale (ad es. per averlo inavvertitamente cancellato dalla sua casella).

### 3. La prova della esistenza degli allegati al messaggio di posta elettronica certificata nel processo telematico

Per venire ora al profilo relativo alla dimostrazione della avvenuta spedizione di un allegato informatico alla pec, va anzitutto osservato che l'art. 1, comma 1, lett. "g", D.P.R. 11 febbraio 2005, n. 68 ("Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata") definisce messaggio di posta elettronica certificata "un documento informatico composto dal testo del messaggio, dai dati di certificazione *e dagli eventuali documenti informatici allegati*" (ns. enfasi).
L'art. 6, comma 7, D.P.R. cit. prevede che "nel caso in cui il mittente non abbia più la disponibilità delle ricevute dei messaggi di posta elettronica certificata inviati, le informazioni di cui all'articolo 11, detenute dai gestori, sono opponibili ai terzi ai sensi dell'articolo 14, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445".
L'art. 11, comma 2, D.P.R. cit. dispone infine che "durante le fasi di trasmissione del messaggio di posta elettronica certificata, i gestori mantengono traccia delle operazioni svolte su un apposito log dei messaggi. I dati contenuti nel suddetto registro sono conservati dal gestore di posta elettronica certificata per trenta mesi".
Alla luce di tali indici normativi non può ritenersi corretta la statuizione della Cassazione in base a cui "(...) se alla Pec è stato allegato un file con un determinato nome, estensione, formato e dimensioni la ricevuta lo attesterà, ma non farà prova del contenuto di quel file, occorrendo, a tal fine, che sul file allegato sia apposta la firma digitale, che certificherà la provenienza del documento e la sua integrità". In questa statuizione si mischiano non complanari profili.
Ai sensi dell'art. 48, comma 3, d.lgs. 7 marzo 2005, n. 82, infatti, la data e l'ora di trasmissione e ricezione di un documento informatico trasmesso mediante pec sono opponibili ai terzi (10), a prescindere dalla sottoscrizione digitale dell'allegato. Poiché nella nozione di messaggio di posta elettronica certificata sono ricompresi anche gli allegati informatici, quale ne sia la forma, la certezza della data di spedizione si estenderà anche a quelli.
Se la preoccupazione della S.C. fosse quella di prevenire fenomeni di sleale produzione postuma di un documento informatico con denominazione identica a quella dell'allegato risultante dalle ricevute del messaggio pec, ma "slegato" dalla spedizione attestata da quelle ricevute, d'altra parte, basti notare che tale rischio è già scongiurato dalle regole tecniche del processo telematico.
Segnatamente, in base all'art. 13, comma 1, lett. "h", Provvedimento DGSIA del 18 dicembre 2015, recante le Specifiche tecniche previste dall'art. 34, comma 1, d.m. 44 del 21 febbraio 2011, nel processo telematico è ammessa la produzione di documenti informatici in formato ".eml", a patto che questi contengano file nei formati ammessi dalle lettere precedenti (cioè documenti informatici nei formati: .pdf, .rtf, .txt, .jpg, .gif, .tiff).
Per dimostrare l'avvenuto invio di un messaggio pec e dei relativi allegati, è sufficiente estrarre copia informatica del medesimo in formato ".eml": ciò consentirà al giudice di verificare non solo il testo del messaggio pec ma altresì esistenza, tipologia e contenuto di tutti i fi-

(9) Su cui Poli, *Gli effetti della liquidazione giudiziale per il debitore*, in Trisorio Liuzzi, *Diritto della crisi d'impresa*, Bari, 2023, 377 ss., 402.

(10) E lo stesso sito della Agenzia per l'Italia Digitale riporta che: "La Posta Elettronica Certificata (PEC) ha lo stesso valore legale di una raccomandata tradizionale con avviso di ricevimento. Per certificare l'invio e la ricezione di un messaggio di PEC, il gestore di posta invia al mittente una ricevuta che costituisce *prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata*".

les informatici che siano stati eventualmente allegati al messaggio pec, esattamente come se si trattasse dell'originale inviato al destinatario.
Se, dunque, alla pec sia allegata, quale documento informatico, una scrittura privata priva di data certa, la spedizione di tale documento a mezzo pec integra un "altro fatto" idoneo a dimostrare la anteriorità della formazione della scrittura, rilevante ai sensi dell'art. 2704 c.c.
Potrebbe presentarsi la eventualità, dicevamo in precedenza, in cui il mittente abbia inavvertitamente cancellato il messaggio pec inviato e sia perciò nella impossibilità di produrre in giudizio un documento informatico in formato ".eml", comprensivo del messaggio pec e dei suoi allegati. Neppure in tal caso, diremmo, il diritto alla prova subirà una irrimediabile vulnerazione. Potrà infatti soccorrere un ordine di esibizione diretto alla controparte o al terzo gestore della casella di posta elettronica certificata (sia della casella del mittente, sia della casella del destinatario, se non di entrambi), sempre che i dati relativi al messaggio ed ai suoi allegati siano stati conservati e l'ordine di esibizione sia impartito entro il relativo termine di conservazione obbligatoria. Neppure può escludersi che il giudice disponga una assai più snella e fruttuosa ispezione giudiziale del contenuto della casella di posta del destinatario ai sensi dell'art. 258 c.p.c.
Il ricorso alla "prova diretta", qui riatteggiata in chiave di oculare verifica di un fatto semplice (suscettibile di essere conosciuto ed apprezzato dal giudicante senza bisogno di particolari conoscenze tecnico-scientifiche), ossia del contenuto di documenti informatici ricevuti dal destinatario del messaggio pec, potrà aversi solo nei casi in cui ciò appaia indispensabile (11). E tuttavia, almeno nei casi in cui la scrittura privata sia invocata nei confronti del fallimento di un imprenditore diverso dalla persona fisica, neppure verranno in gioco fondamentali esigenze di riservatezza della corrispondenza tali da precludere una mirata verifica giudiziale, nel contraddittorio tra le parti.
In ultimo, occorre chiedersi se il silenzio della controparte, ossia la non contestazione del fatto di invio a mezzo pec di un determinato allegato informatico, sia rilevante nel processo in cui il mittente pretenda di giovarsi degli effetti della scrittura privata e della sua opponibilità, e possa così determinare l'effetto di *relevatio ab onere probandi*.
Riteniamo che il principio di non contestazione possa operare nella fattispecie.

(11) Su poteri istruttori officiosi e ricerca della prova di fatti a mezzo *internet* si v., più in generale, con propensioni tuttavia, a nostro avviso, esorbitanti dal modello del processo isonomico, Della Pietra, *La vicinanza della prova e la prova «più prossima» che c'è: internet*, in *Giusto proc. civ.*, 2018, 1033 ss.

Qui si ha a che fare con un fatto sostanziale, la data certa della scrittura privata, altrimenti inopponibile al fallimento, senz'altro rilevante ai fini della decisione di merito, non della ammissibilità della domanda di ammissione allo stato passivo (12). La curatela fallimentare, come veduto, può professarsi estranea rispetto alla scrittura privata, ma nondimeno soggiace all'onere di contestare il fatto che tale scrittura sia stata inviata alla pec della impresa come allegato informatico. Tanto più che la giurisprudenza qualifica come eccezione (sia pure in senso lato) quella di carenza di data certa della scrittura privata invocata dal creditore come titolo del credito di cui richiede la ammissione nello stato passivo.
Fermo, dunque, l'indirizzo giurisprudenziale in base a cui gli effetti della non contestazione *ex* art. 115 c.p.c. si producono con riferimento alle sole allegazioni in fatto

(12) Cass. sez. un. 28 agosto 1990, n. 8879. In precedenza, una parte della giurisprudenza inclinava a qualificare la opponibilità della scrittura privata, e così la data certa, alla stregua di una condizione di ammissibilità della azione del creditore principiata con la domanda di ammissione nello stato passivo. Domanda che avrebbe avuto ad oggetto il diritto di credito nella sua "porzione concorsuale" (Fabiani). Le Sezioni Unite del 1990, invece, hanno ribadito che la data certa è fatto *costitutivo del diritto di credito* e che l'onere di dimostrare tale fatto grava sul creditore. Ma tale indirizzo ha avuto breve corso, come emerge dalla panoramica giurisprudenziale condotta da V. Farina, *Data certa e fallimento: un problema sempre attuale*, in *I Contratti*, 2021, 431 ss., 439. A partire da Cass. sez. un., 20 febbraio 2013, n. 4213, la giurisprudenza ha preso a riqualificare la mancanza di data certa come eccezione in senso lato, sul rilievo che "l'art. 2704 è inserito nel libro sesto (tutela dei diritti), titolo secondo (delle prove), capo secondo (della prova documentale), sezione seconda (della scrittura privata), e regola quindi l'efficacia dell'atto senza incidere in alcun modo sulla sua validità. Da tale rilievo (consistente cioè nel fatto che l'atto a sostegno della richiesta è valido, pur non essendo opponibile al terzo) discende pertanto che l'onere probatorio incombente su creditore istante in sede di ammissione può ritenersi soddisfatto ove prodotta documentazione idonea a dimostrare la fondatezza della pretesa formulata, mentre l'eventuale mancanza di data certa nella detta documentazione costituisce un semplice fatto impeditivo del riconoscimento del diritto fatto valere (...)". Sempre le Sezioni Unite del 2013 riconobbero che "la distribuzione dell'onere della prova nell'ambito dei generali principi esistenti deve tener conto anche del principio della disponibilità dei mezzi di prova, che induce a privilegiare interpretazioni della legge che non rendano impossibile o troppo difficile il diritto di azione costituzionalmente garantito (C. 12/6008, C. 09/15406, C. 09/10744), eccessiva difficoltà, se non impossibilità, che si determinerebbe nel caso in cui si volesse imporre al creditore che formula istanza di ammissione al passivo l'onere di dimostrare l'anteriorità del credito all'apertura della procedura concorsuale"; nello stesso senso Cass. 18 dicembre 2023, n. 35252; Cass. 6 ottobre 2023, n. 28144; Cass. 17 luglio 2023, n. 20462. Da ult., nel senso che la mancanza di data certa della scrittura privata configura un fatto impeditivo rilevabile d'ufficio e idoneo a determinare il rigetto della domanda di ammissione al passivo, Cass. 19 marzo 2024, n. 7253, che tuttavia ha cassato con rinvio la sentenza di rigetto della opposizione allo stato passivo per avere il giudice di merito respinto la domanda per mancata prova della anteriorità al fallimento della scrittura, e dunque sulla base del rilievo di un fatto impeditivo, non preceduto però dalla attivazione del contraddittorio delle parti sulla questione rilevata d'ufficio ai sensi dell'art. 101 c.p.c. così che alla banca ricorrente era stato impedito di produrre gli estratti conto periodici inviati alla impresa fallita, da cui sarebbe risultata provata, con elevato grado di certezza, la anteriorità della stipulazione del contratto di mutuo che fungeva da titolo del credito.

della controparte e non al contenuto delle prove assunte (13), la cui valutazione è rimessa all'apprezzamento del giudice, se il *fatto dell'invio a mezzo pec* di una scrittura privata (di per sé altrimenti priva di data certa) *non sia contestato dal curatore o liquidatore*, il giudice potrà porre tale fatto a base del suo convincimento: a meno che dai documenti acquisiti al processo non risulti prova contraria (es.: dalle ricevute di accettazione e consegna della pec non risulta che al messaggio pec fosse allegato alcun documento informatico: fatto incompatibile con la affermazione della trasmissione di allegati, compiuta dall'attore in giudizio).

(13) Cass. 1 febbraio 2019, n. 3126; Cass. 21 giugno 2016, n. 12748.

# Provare di aver adottato soluzioni idonee a prevenire o ridurre l'uso fraudolento dei sistemi elettronici di pagamento è onere della Banca

Corte di Cassazione; sezione terza; sentenza12 febbraio 2024, n. 3780; Pres. Scarano; Rel. Moscarini; Poste Italiane S.p.A. c. M. P.

*È responsabile la banca per l'uso non autorizzato dello strumento di pagamento del cliente se non ricorre una situazione di colpa grave dell'utente, configurabile, ad esempio, nel caso di protratta attesa prima di comunicare l'operazione sospetta; infatti, la possibile sottrazione dei codici al correntista attraverso tecniche fraudolente rappresenta una eventualità rientrante nel rischio d'impresa, sicché la banca, per liberarsi dalla propria responsabilità, deve dimostrare la sopravvenienza di eventi che si collochino al di là dello sforzo diligente richiesto al debitore.*

*È onere della banca provare di aver adottato soluzioni idonee a prevenire o ridurre l'uso fraudolento dei sistemi elettronici di pagamento, quali, ad esempio, l'invio al titolare della carta di appositi sms alert di conferma di ogni singola operazione, sulla base del principio di buona fede nell'esecuzione del contratto; in assenza delle quali è corretto imputare alla banca il rischio professionale della possibilità che terzi accedano ai profili dei clienti con condotte fraudolente.*

*...Omissis...*

**Ragioni della decisione**

Con il primo motivo di ricorso – violazione e falsa applicazione dell'art. 7 co. 2 dell'art. 10 co. 2 e 12 co. 4 D.lgs. 27/1/2010 n. 11 in riferimento all'art. 360, co. 1 n. 3 c.p.c. – la ricorrente assume che la sentenza impugnata ha violato le specifiche disposizioni che in materia configurano a carico dell'utente dei servizi telematici oneri di particolare cautela e diligenza nell'uso dei propri codici ed ha disatteso le regole disciplinanti la responsabilità di Poste Italiane S.p.A.

Con il secondo motivo di ricorso – omesso esame circa un fatto decisivo per il giudizio in riferimento all'art. 360 co. 1 n. 5 c.p.c. – lamenta che la sentenza impugnata ha omesso di attribuire rilevanza al fatto decisivo costituito dall'avere l'utente consegnato spontaneamente a terzi dati identificativi del proprio conto, operando su un sito che non era di Poste Italiane S.p.A.; ove tale fatto fosse stato considerato, il giudice del gravame non avrebbe potuto concludere per la sussistenza della responsabilità di Poste.

I motivi sono infondati.

La giurisprudenza di questa Corte, qualificata in termini contrattuali la responsabilità della banca, ha affermato che la diligenza posta a carico del professionista, per quanto concerne i servizi posti in essere in favore del cliente, ha natura tecnica e deve valutarsi tenendo conto dei rischi tipici della sfera professionale di riferimento assumendo come parametro quello dell'accorto banchiere (Cass. n. 806 del 2016); dunque la diligenza della banca va a coprire operazioni che devono essere ricondotte nella sua sfera di controllo tecnico, sulla base anche di una valutazione di prevedibilità ed evitabilità tale che la condotta, per esonerare il debitore, la cui responsabilità contrattuale è presunta, deve porsi al di là delle possibilità esigibili della sua sfera di controllo.

La giurisprudenza di questa Corte è infatti consolidata nel senso di ritenere che la responsabilità della banca per operazioni effettuate a mezzo di strumenti elettronici, con particolare verifica della loro riconducibilità alla volontà del cliente mediante il controllo dell'utilizzazione illecita dei relativi codici da parte di terzi, va esclusa se ricorre una situazione di colpa grave dell'utente configurabile, ad esempio, nel caso di protratta attesa prima di comunicare l'uso non autorizzato dello strumento di pagamento ma il riparto degli oneri probatori posto a carico delle parti segue il regime della responsabilità contrattuale. Mentre, pertanto, il cliente è tenuto soltanto a provare la fonte del proprio diritto ed il termine di scadenza, il debitore, cioè la banca, deve provare il fatto estintivo dell'altrui pretesa, sicché non può omettere la verifica dell'adozione delle misure atte a garantire la sicurezza del servizio. Ne consegue che, essendo la possibilità della sottrazione dei codici al correntista attraverso tecniche fraudolente una eventualità rientrante nel rischio d'impresa, la banca per liberarsi

dalla propria responsabilità, deve dimostrare la sopravvenienza di eventi che si collochino al di là dello sforzo diligente richiesto al debitore (Cass., 1, n. 2950 del 3/2/2017; Cass., 3, n. 18045 del 5/7/2019; Cass., 6-3, n. 26916 del 26/11/2020).
Era pertanto onere di Poste Italiane, come correttamente ritenuto dalla impugnata sentenza, a dover provare di aver adottato soluzioni idonee a prevenire o ridurre l'uso fraudolento dei sistemi elettronici di pagamento, quali ad esempio l'invio al titolare della carta di appositi sms alert di conferma di ogni singola operazione, sulla base di un principio di buona fede nell'esecuzione del contratto. In assenza di tale prova è corretta la decisione di imputare alla banca il rischio professionale della possibilità che terzi accedano ai profili dei clienti con condotte fraudolente.
Da quanto esposto consegue il rigetto del ricorso.
Non occorre provvedere sulle spese perché l'intimata non ha svolto attività difensiva in questa sede.
*...Omissis...*

# IL COMMENTO

*di Mario Passaretta*

**Sommario:** 1. Gli strumenti di pagamento online e l'uso non autorizzato: la soluzione adottata dalla S.C. – 2. L'ordine di pagamento impartito al PSP. – 3. Gli obblighi del PSP. – 4. Gli obblighi a carico dell'utilizzatore. – 5. Il phishing e la responsabilità del PSP.

Il contributo prende in esame una recente sentenza della Suprema Corte con cui si affronta un caso di *phishing*, a seguito del quale un terzo non legittimato aveva dato avvio a un'operazione di pagamento non autorizzato. La pronuncia della Cassazione conferma l'orientamento secondo cui il prestatore di servizi è responsabile per l'indebito utilizzo dello strumento di pagamento, se non dimostra la condotta negligente del proprio cliente. La sentenza stimola, in particolare, alcune riflessioni sulla riferibilità dell'ordine di pagamento impartito al prestatore di servizi e il regime di responsabilità di quest'ultimo anche alla luce degli orientamenti dell'Arbitro Bancario Finanziario.

*The contribution examines a recent judgment of the Supreme Court addressing a case of phishing, in which an unauthorized third party initiated an unauthorized payment operation. The ruling of the Cassation Court confirms the orientation according to which the service provider is responsible for the unauthorized use of the payment instrument if they fail to demonstrate the negligent conduct of their own customer. This particularly stimulates some considerations on the attributability of the payment order given to the service provider and the liability regime of the latter, also according to the orientations of the Financial Banking Arbitrator.*

## 1. Gli strumenti di pagamento *online* e l'uso non autorizzato: la soluzione adottata dalla S.C.

Nell'odierno panorama economico-finanziario, caratterizzato dalla prevalenza di transazioni gestite attraverso intermediari quali banche, Poste Italiane, istituti di moneta elettronica e di pagamento, si assiste ad una crescente dematerializzazione dei mezzi di scambio (1). Tale processo, intrinsecamente legato ai rapporti bancari e commerciali, segna una trasformazione profonda nelle operazioni di pagamento, che, originariamente bilaterali, evolvono in una struttura trilaterale: un nuovo attore, il prestatore di servizi di pagamento (PSP), s'interpone tra debitore e creditore, facendo da tramite nel trasferimento delle somme di danaro dovute, secondo un meccanismo riconducibile allo schema della delegazione di pagamento (2).
Il passaggio a un sistema di pagamento intermediato introduce la necessità di proceduralizzazione l'operazione, indissolubilmente legata all'utilizzo di tecnologie avanzate quali piattaforme di *home banking* e portafogli elettronici che, pur facilitando le transazioni, espone gli utenti e i PSP a rischi di frodi, tra cui il *phishing* (3).

(1) Cfr., in ordine all'interposizione bancaria nei pagamenti, Sciarrone Alibrandi, *L'interposizione della banca nell'adempimento dell'obbligazione pecuniaria*, Milano, 1997, 23 ss.; v. anche Spada, *Carte di credito e carte bancarie: "terza generazione" dei mezzi di pagamento*, in *Riv. dir. civ.*, 1976, I, 489 ss.; Brozzetti, *Le carte di pagamento*, in *L'attività delle banche*, a cura di Urbani, Padova, 2020, 533 ss.

(2) Nel senso di ritenere l'obbligazione pecuniaria come «fatalmente [...] adempiuta attraverso l'intermediazione di un terzo» che pone in essere l'attività materiale di prestazione, riconducibile a un'attività delegatoria, v. Abatangelo, *Intermediazione nel pagamento e ripetizione dell'indebito*, Padova, 2009,3; De Stasio, *Riparto delle responsabilità e restituzioni nei pagamenti non autorizzati*, in *Attualità di Diritto bancario*, a cura di Minneci e Tina, Milano, 2021, 75; Id, *Ordine di pagamento non autorizzato e restituzione della moneta*, Milano, 2016, 24 ss.

(3) Nella maggior parte dei casi il testo segnala un accesso abusivo al conto corrente bancario del destinatario del messaggio e si richiede pertanto di certificare le proprie credenziali, normalmente nome utente e *password*, attraverso l'accesso ad un sito internet che graficamente è identico o simile a quello del sistema bancario normalmente utilizzato dal destinatario del messaggio di posta elettronica. I messaggi vengono mandati in modo del tutto casuale a centinaia di migliaia di utenti. Il mittente

Quest'ultimo, attuato tramite tecniche ingannevoli di raccolta informazioni, si manifesta attraverso fasi ben delineate, dall'invio massivo di comunicazioni truffaldine fino al prelievo indebito di fondi o all'acquisto di beni *online* mediante l'utilizzo dei dati personali ottenuti illecitamente (4).

La Suprema Corte, nella sentenza in commento, affronta proprio il caso di un pagamento non autorizzato dopo un episodio di *phishing*. Un cliente, infatti, aveva lamentato l'uso non autorizzato del proprio strumento di pagamento dopo aver ricevuto sulla *e-mail* un messaggio contenente l'invito a cambiare la *password* utile per accedere alla piattaforma di pagamento del PSP. Di contro, il prestatore, al quale veniva chiesta la restituzione dell'importo trasferito illecitamente, aveva ritenuto che il cliente avesse violato gli obblighi di diligenza su di lui gravanti, poiché aveva incautamente comunicato i propri dati d'accesso allo strumento di pagamento.

Il giudizio di primo grado era stato definito con il rigetto della domanda di restituzione dell'importo sottratto al cliente/utilizzatore; sicché, quest'ultimo aveva proposto appello, poi accolto. E, infatti, il giudice del gravame aveva imputato gli effetti dannosi, derivanti dall'uso non autorizzato dello strumento di pagamento, come diretta conseguenza dell'esercizio di un'attività pericolosa, non avendo comunque l'intermediario dimostrato la riconducibilità dell'operazione al cliente. L'uso dei codici d'accesso al sistema da parte di terzi, dunque, rientra nel rischio professionale del prestatore di servizi di pagamento, ed essendo la condotta prevedibile ed evitabile con appropriate misure tecniche, anche al fine di garantire la fiducia degli utenti nella sicurezza del sistema, è del tutto ragionevole ricondurre nell'alveo del rischio professionale del prestatore di servizi di pagamento la possibilità di un uso non autorizzato dei codici di accesso al sistema (5).

Il prestatore di servizi ha quindi impugnato la sentenza di secondo grado, senza tuttavia vedere accolto il proprio ricorso. La Cassazione, al riguardo, conferma l'orientamento adottato dal giudice del gravame, precisando, nel proprio percorso argomentativo, che la responsabilità dell'intermediario si qualifica in termini contrattuali. Nel dettaglio, si afferma che la diligenza posta a carico del professionista, per quanto concerne i servizi posti in essere in favore del cliente, ha natura tecnica e deve valutarsi tenendo conto dei rischi tipici della sfera professionale di riferimento, assumendo come parametro quello dell'accorto banchiere; dunque, la diligenza che egli deve adottare rientra nella sua normale sfera di controllo tecnico, sulla base anche di una valutazione di prevedibilità ed evitabilità. Di conseguenza, il prestatore di servizi deve provare di aver adottato soluzioni idonee a prevenire o ridurre l'uso fraudolento dei sistemi elettronici di pagamento, come, ad esempio, l'invio al titolare dello strumento di appositi *sms alert* di conferma per ogni singola operazione. Pertanto, se manca tale prova, il rischio deve imputarsi al prestatore di servizi di pagamento.

La sentenza della S.C., sebbene s'inserisca in un consolidato orientamento giurisprudenziale, stimola alcune riflessioni sul bilanciamento delle responsabilità tra cliente e prestatore di servizi di pagamento, qualora il primo sia vittima di *phishing*.

## 2. L'ordine di pagamento impartito al PSP

La disposizione di pagamenti non autorizzati richiede, nei limiti qui concessi, di ricostruire l'operazione/procedimento di pagamento intermediato, per meglio comprendere le soluzioni prospettate dalla giurisprudenza. È, dunque, preliminare individuare nell'art. 1, lett. o) e lett. s), d.lgs. 11/2010, il dato normativo di riferimento, poiché definisce la disposizione di pagamento come un'istruzione impartita dal pagatore a un proprio prestatore di servizi di eseguire un'operazione di pagamento, secondo un insieme di procedure concordate (6). Tale

della *e-mail* non ha alcun riferimento in merito alla banca utilizzata dal destinatario del messaggio; da qui, la truffa prende il nome di "pesca con l'amo" (*phishing*). Cfr. FRAU, *Responsabilità civile della banca per operazioni di home banking contestate dal cliente*, in *Resp. civ. prev.*, 2019, 38 ss.

(4) Il *phishing* rientra fra i reati informatici, su cui v. *amplius* DESTITO, voce «*Reati informatici*», in *Dig. Disc. pen.*, Agg. V, Torino, 2010, 739 ss. e *ivi* ulteriori riferimenti.

(5) La giurisprudenza di merito riconosce la portata generale del principio che attribuisce alla banca l'onere della prova della riconducibilità dell'operazione al cliente e, di conseguenza, ne ammette l'applicabilità anche in data anteriore alla vigenza del d.lgs. n. 11 del 2010: così, App. Bolzano, 26 gennaio 2019, in *ONE Legale*; Trib. Roma, 30 ottobre 2023, in *Top24Diritto*; Trib. Como, 24 ottobre 2023, in *Top24Diritto*; Trib. Napoli Nord, 31 maggio 2022, in *ONE Legale*; Trib. Venezia, 17 maggio 2022, in *ONE Legale*; Trib. Parma, 6 settembre 2018, in *ONE Legale*; Trib. Roma, 31 agosto 2016, in *DeJure*; Trib. Palermo, 12 gennaio 2010, in *DeJure*. E ancora, sulla responsabilità del PSP, Trib. Napoli, 01 marzo 2024, n. 2456, Trib. di Como, 24 ottobre 2023, n. 1186, tutte in *ONE Legale*. Sulla responsabilità del correntista, v. Trib. di Prato, 11 febbraio 2024, Trib. Milano, 17 novembre 2023, n. 9186, Trib. Palermo, 26 ottobre 2023, n. 4739, reperibili tutte in *ONE Legale*.

(6) L'adempimento intermediato a mezzo banca ha subito un'evoluzione significativa. Inizialmente, si è cercato di adattare le regole del codice civile, ma tale adattamento non è stato sempre puntuale né adeguato. Successivamente, è stata introdotta una nuova disciplina legislativa che presenta due caratteristiche: da un lato è complessa e ancora non completamente messa a punto, dall'altro è così minuziosa e dettagliata da far sorgere dubbi sull'utilità del ricorso al codice civile, originariamente pensato per pagamenti "immediati" tramite *res* qualificate. Questa nuova disciplina rimane "muta" riguardo alla ricostruzione giuridica o, meglio, alle diverse ricostruzioni giuridiche del pagamento con strumenti "diversi", lasciando inevitabilmente alcuni conflitti di interesse privi di composizione. Di conseguenza, si legittima il ricorso, almeno in via residuale, alla disciplina prevista dal codice civile (ONZA, *Gli strumenti di pagamento nel contesto dei pagamenti on line*, in *Dir. banc. fin.*, 2017, 680 ss.).

istruzione, con la quale il cliente autorizza il PSP, si inquadra in una logica delegatoria, secondo cui il prestatore di servizi si obbliga nei confronti del pagatore a eseguire il pagamento in favore del beneficiario. L'ordine di pagamento e la sua esecuzione richiede il consenso del pagatore, «elemento necessario», ai sensi dell'art. 5, comma 1, d.lgs. 11/2010, senza il quale «un'operazione di pagamento non può considerarsi autorizzata». Il cliente, quindi, ordina il pagamento nella forma e secondo la procedura concordata nel contratto quadro o nel contratto relativo a singole operazioni di pagamento (art. 5, comma 2, d.lgs. 11/2010); in questo sostanziandosi la riferibilità dello *iussum delegatorum*.
Il PSP deve, dunque, dotarsi di «tecniche» in grado di rendere riferibile al titolare dello strumento l'ordine impartito a distanza; ciò avviene mediante l'uso di carte utilizzabili con *password* o codici alfanumerici, che devono essere adeguatamente custoditi dal titolare stesso ed essere usati in conformità con il contratto quadro (7). L'inadempimento, relativo, ad esempio, alla mancata custodia, in base agli stati soggettivi dell'agente, determina una allocazione del rischio da uso indebito o illegittimo dello strumento di pagamento. Il cliente deve utilizzare le tecniche di riferibilità ed i relativi codici conformemente al contratto quadro, deve costudirle diligentemente e comunicare, non appena ne viene a conoscenza, l'eventuale uso indebito. Il PSP, dal suo canto, deve assicurare l'inaccessibilità a terzi dei dispositivi personalizzati necessari per l'utilizzo dello strumento, mettendo a disposizione del cliente un sistema di comunicazione sull'uso indebito; infine, deve impedire utilizzi successivi alla denuncia di smarrimento dei codici o all'uso indebito dello strumento (c.d. blocco).
Fra gli eventi non riferibili all'utente devono comprendersi, oltre alle ipotesi di clonazione dello strumento di pagamento, il c.d. *man-in-the-browser*, invero una pagina *web* identica a quella del prestatore di servizi, nella quale l'utente immette tutti i propri dati d'accesso allo strumento, consegnando, di fatto, lo stesso al truffatore; il c.d. furto di identità digitale, dove è il debitore ad essere "illegittimo" avendo qualcuno creato un *alter ego* virtuale del debitore "legittimo"; ed il c.d. *phishing*, come poco prima illustrato. Essi danno avvio a un procedimento non preceduto da uno *iussum* ascrivibile alla volontà del cliente, la cui colpa, per aver eventualmente concorso alla poco diligente custodia dei codici d'accesso, deve essere verificata caso per caso. Nel prosieguo d'indagine, infatti, si vedrà, specie nella giurisprudenza arbitrale, come il *phishing* sia anche diretta conseguenza della colpa grave di chi risponda (ingenuamente) alla *e-mail* rilasciando i propri codici d'accesso allo strumento di pagamento (8), diversamente dalla truffa del c.d. *man-in-the-browser*, dove la differenza rispetto alla pagina digitale riferibile al PSP è spesso racchiusa in un dettaglio non facilmente percepibile.

## 3. Gli obblighi del PSP

Il d.lgs. 11/2010 prevede un complesso di norme (artt. 6-14) che definisce lo statuto degli obblighi del PSP e del pagatore, per l'uso di strumenti/conti di pagamento. Il sistema normativo adottato dal legislatore nazionale, anche dopo il recepimento della PSD2 (9), riflette il principio elaborato dalla teoria economica del *cheapest cost avoider*, secondo cui ciascuna delle parti coinvolte in un'operazione di pagamento deve farsi carico dei rischi che è meglio in grado di prevenire, gestire e sopportare (10). Il PSP deve, dunque, dotarsi di un apparato tecnico "performante" in grado di prevenire l'uso non autorizzato di strumenti e conti di pagamento.
L'art. 6 d.lgs. 11/2010 stabilisce le ipotesi in cui il contratto quadro può porre dei limiti all'utilizzo dello strumento di pagamento e, in particolare, riconosce il diritto del prestatore di servizi di bloccare l'utilizzo dello stesso qualora vi sia il rischio di una compromissione del sistema di sicurezza dello strumento, oppure un suo uso fraudolento o non autorizzato. La norma, essenzialmente, pone a carico del PSP un obbligo di monitoraggio sugli strumenti di pagamento emessi, connaturato al tipo d'impresa esercitata. Ci si chiede, tuttavia, se il prestatore di servizi sia in ogni caso legittimato bloccare lo strumento di pagamento "a rischio" e, cioè, anche qualora il contratto quadro non contenga una specifica previsione in tal senso. La soluzione, in assenza di una espressa previsione nella disciplina speciale, si ricava

(7) Nella disciplina del generale riparto di responsabilità fra utente/pagatore e PSP relativa a eventuali utilizzi non autorizzati dello strumento, fatta eccezione per alcune modifiche terminologiche, non sembrano riscontrarsi sostanziose differenze di impostazione rispetto alla PSD. Permane pressoché intatta la previsione dei reciproci obblighi di condotta gravanti sulle parti: così, Berti de Marinis, *La disciplina dei pagamenti non autorizzati nel nuovo sistema delineato dal recepimento della direttiva PSD2*, in *Dir. banc. fin.*, 2018, I, 638.

(8) Tali pagamenti rappresentano una "anomalia", tipica dei pagamenti *on line*, che pertanto genera un avvio "non riferibile" del procedimento, la cui imputabilità per colpa (almeno grave) al titolare deve verificarsi caso per caso, specie nel *phishing*. L'ABF ritiene l'anzidetto fenomeno «ormai del tutto noto con l'effetto che qualunque utente dotato di normale avvedutezza e prudenza è in grado di non farsi trarre in inganno anche per il risalto che viene dato al fenomeno in tutti i siti degli intermediari»: cfr. ABF Milano, 14 ottobre 2016, n. 9177; ABF Napoli, 20 ottobre 2016, n. 9322; ABF Napoli, 20 ottobre 2016, n. 9343; ABF Milano, 21 ottobre 2016, n. 9409; ABF Milano, 22 novembre 2016, n. 10306.

(9) Sul recepimento della PSD2 e, in particolare, sulla disciplina prevista per i *Third Party Providers*, v., fra molti, Messore, *La nuova disciplina dei servizi di pagamento digitali prestati dai Third Party Providers*, in *Nuove leggi civ. comm.*, 2020, 511 ss.

(10) In tal senso, v. Ciraolo, *Pagamento fraudolento con carta di credito e ripartizione delle responsabilità. Dagli orientamenti attuali alla revisione della PSD*, in *Dir. banc. fin.*, 2017, 156-157.

dalla disciplina contrattuale, alla luce del principio di buona fede *in executivis*, ai sensi dell'art. 1375 c.c. (11). Conseguentemente, ove ricorra uno dei motivi (giustificati) indicati dall'art. 6, comma 2, d.lgs. 11/2010, il PSP non solo può ma, invero, deve obbligatoriamente attivarsi per il blocco dello strumento di pagamento. Il principio di buona fede in esecuzione del contratto, pertanto, contribuisce in pieno a realizzare, come regola concorrente, il comportamento dovuto dal prestatore di servizi, anche in assenza di una espressa previsione contrattuale.

Ancora, perché sia correttamente riferibile l'ordine di pagamento, il prestatore di servizi deve altresì assicurare che le credenziali di sicurezza personalizzate non siano accessibili a soggetti diversi dall'utente abilitato a usare lo strumento di pagamento e che siano adottati sistemi di sicurezza idonei a scongiurare l'uso non autorizzato, come il sistema di autenticazione a due fattori (12). Unitamente ai predetti presidi, il PSP deve dotarsi di un canale di comunicazione diretto con lo stesso perché siano comunicate le frodi o l'uso non autorizzato correlato allo strumento (cfr. artt. 8 e 10-*bis*).

## 4. Gli obblighi a carico dell'utilizzatore

L'utilizzatore, dal suo canto, deve osservare alcuni doveri di condotta, prescritti dall'art. 7 d.lgs. 11/2010. Essi possono essere suddivisi in obblighi nella fase c.d. fisiologica del rapporto e, in particolare, nel corretto uso dello strumento di pagamento in conformità con i termini esplicitati nel contratto quadro (lett. a); e nella fase c.d. patologica, ossia obblighi legati a comportamenti da adottare una volta a conoscenza dell'indebito utilizzo dello strumento (lett. b). La norma, essenzialmente, nella prima parte, lascia emergere un obbligo di condotta del pagatore comunque soggiacente alla sua sfera di controllo, sicché egli dovrà adottare tutte quelle cautele utili per evitare interferenze da parte di terzi (13). Condotte, talvolta, anche descritte dallo stesso prestatore di servizi mediante l'invio di documenti informativi, che aiutano a individuare i comportamenti a rischio che il cliente dovrebbe evitare, come, ad esempio, la conservazione del *pin* e della carta nella medesima custodia, ovvero annotare il primo sulla seconda.

Gli obblighi, invece, riguardanti la c.d. fase patologica – che non devono confondersi con il diritto di rettifica dell'operazione contestata riconosciuto dall'art. 9 d.lgs. 11/2010 – richiedono al cliente del PSP di comunicare tempestivamente, invero «senza indugio» una volta venuto a conoscenza, lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato di uno strumento in suo possesso. Si tratta di una prerogativa utile al prestatore di servizi per adottare le contromisure idonee al superamento del rischio anche di operazioni non autorizzate e, conseguentemente, evitare di esporsi in termini di responsabilità proprio nei confronti del cliente. Tuttavia, la norma non indica un termine entro il quale denunciare il furto o l'uso illegittimo dello strumento di pagamento; sicché si impone di valutare le specifiche circostanze dell'omessa o tardiva denuncia, per stabilire se il titolare dello strumento abbia violato quei doveri minimi di diligenza ed accortezza che chiunque dovrebbe osservare (14).

## 5. Il *phishing* e la responsabilità del PSP

Orbene, una volta delineato lo scenario normativo degli obblighi a carico dell'utilizzatore e del prestatore di servizi, il bilanciamento delle responsabilità tra intermediario e cliente, per operazioni non "riferibili" al pagatore, si risolve essenzialmente nel dimostrare la grave negligenza di quest'ultimo, posto che il riscontro di tale elemento comporta la responsabilità dell'utilizzatore, con l'effetto inoltre di neutralizzare anche la franchigia di 50 euro, prevista con riferimento alle operazioni abusive di pagamento eseguite prima della comunicazione di cui

(11) Cfr. Troiano - Pironti, *Commento sub art. 6*, in *La nuova disciplina dei servizi di pagamento*, a cura di Mancini, Rispoli Farina, Santoro, Sciarrone Alibrandi, Troiano, Torino, 2011, 109 ss.

(12) Il sistema di autenticazione a due fattori, *two-factors authentication*, è un metodo che si basa sull'utilizzo congiunto di due autenticazioni individuali (ad esempio PIN/password e smart card). In argomento, v. Garante per la protezione dei dati personali, *Linee-guida in materia di riconoscimento biometrico e firma grafometrica*, Allegato A al Provvedimento del Garante del 12 novembre 2014. Va tuttavia precisato che l'adozione di un sistema di autenticazione forte non libera, di per sé sola, l'intermediario dalle proprie responsabilità: sul punto v. ABF Bari, 5 marzo 2021, n. 6017; ABF Napoli, 15 marzo 2021, n. 7013; ABF Roma, 3 dicembre 2020, n. 21844. In dottrina, v. Ciraolo, *Le carte di debito nell'ordinamento italiano*, Milano, 2008, 193 ss.

(13) Si tratta, se si vuole, dell'esplicitazione dei principi iscritti negli artt. 1176 e 1375 c.c., dove la prima può considerarsi norma elastica, che permea il sistema di diritto delle obbligazioni (cfr. Sicchiero, *Principi generali, norme elastiche, clausole generali*, in *Contratto e impresa*, 1052 ss.). Con questo, si evidenzia che la disciplina sui servizi di pagamento non si muove propriamente nell'ottica consumeristica, ma nella direzione di perseguimento di un preciso obiettivo: una legislazione unitaria dei contratti sovranazionale. In questi termini, v. Santoro, *I servizi di pagamento*, in *I contratti bancari*, a cura di Capobianco, Torino, 2016, 1681; Troiano, *Contratto di pagamento*, in *Enc. dir.*, V, Milano, 2012, 395. Naturalmente, vale la pena precisarlo, diligenza non significa verifica periodica e ravvicinata di disponibilità dello strumento di pagamento da parte del suo titolare, ma solo dovere di diligente custodia (ABF Roma, 27 marzo 2015, n. 2371). Inoltre, v. Trib. Firenze, 19 gennaio 2016, in *Dir. banc. fin.*, 2017, 143 ss., secondo cui il comportamento del titolare della carta accortosi del furto o dello smarrimento della stessa solamente dopo otto giorni da tale avvenimento non sia qualificabile *ex se* come negligente.

(14) Ancora una volta l'ABF delinea i confini delle fattispecie di uso non autorizzato dello strumento di pagamento. Ha ritenuto, infatti, responsabile un soggetto che si era avveduto del furto della propria carta di pagamento con due giorni di ritardo (ABF Milano, 3 novembre 2015, n. 8251).

all'art. 7 d.lgs. 11/2010. Tali principi sono evocati anche nella sentenza in commento, ma richiedono un corretto bilanciamento tra quanto dovuto dal PSP, in termini di sicurezza, e quanto richiesto al cliente, relativamente alla diligenza con cui quest'ultimo deve custodire le proprie credenziali. Bisogna, in sostanza, stabilire se l'inadempimento, da parte del titolare dello strumento di pagamento, di uno o più obblighi a lui incombenti, possa ritenersi giustificabile, o se appaia essere, piuttosto, il frutto di una straordinaria ed inescusabile leggerezza. La disciplina speciale, al riguardo, non dispone, dettagliatamente, le ipotesi di negligenza. Essa rinvia invece, "in bianco" (15), alle condizioni contrattuali; non indica, poi, se non in modo del tutto generico, quali accorgimenti debba in concreto osservare l'utilizzatore per evitare che possano essere compiute operazioni senza il suo consenso; non chiarisce in quali casi ed entro quali termini la notifica all'emittente possa considerarsi tempestiva.

Il PSP, tuttavia, incorre nell'onere della prova, ai sensi dell'art. 2697 c.c., in tal senso ribaltata a suo carico, di dimostrare l'assoluta correttezza delle operazioni eseguite e l'eventuale negligenza (grave) del proprio cliente, nonché deve dimostrare di aver adottato i presidi di sicurezza necessari, poiché il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente (come l'autenticazione a due fattori) (cfr. art. 12, comma 2 *bis* d.lgs. 11/2010) (16).

La giurisprudenza, prima dell'entrata in vigore del d.lgs. 11/2010, aveva definito la diligenza richiesta dalla banca, nell'ambito, soprattutto, di operazioni in *home banking*, come diligenza professionale richiesta dall'incarico, che impone l'adozione di misure di sicurezza onde evitare manomissioni (17). La stessa giurisprudenza di legittimità, del resto, ha chiarito che, anche laddove il cliente ometta di rispettare determinati obblighi comportamentali, la banca rimarrebbe comunque tenuta ad osservare, nella fornitura dei propri servizi, la diligenza *del bonus argentarius*, tenuto conto anche dei rischi professionali tipici della sfera di riferimento (18). Tuttavia, non sempre l'intermediario risponderebbe del furto delle credenziali d'accesso allo strumento: potrebbe, infatti, palesarsi anche un concorso di colpa, ai sensi dell'art. 1227 c.c., se il cliente negligente sia colposamente venuto meno agli obblighi imposti dal contratto, anche in caso di leggerezza nell'uso degli strumenti di pagamento *online* (19).

Il quadro normativo di riferimento, in particolare gli artt. 9 e 10 d.lgs. 11/2010, lascia emergere inoltre una responsabilità da *status*, qualora il PSP debba farsi carico anche del c.d. rischio tecnologico, connaturata alla propria organizzazione imprenditoriale, senza potersi

(15) Espressione impiegata da Ciraolo, *Pagamento fraudolento con carta di credito e ripartizione delle responsabilità. Dagli orientamenti attuali alla revisione della PSD*, in *Dir. banc. fin.*, 2017, 156-157.

(16) È evidente che la prova della colpa grave dell'utilizzatore possa risultare assai difficoltosa per l'intermediario. Tale prova, tuttavia, può essere fornita dal PSP anche facendo ricorso allo strumento delle presunzioni (art. 2797 c.c.), in presenza di indizi gravi, precisi e concordanti: cfr. ABF, Coll. Milano, 3 novembre 2015, n. 8251, secondo cui, testualmente, «Contrariamente alla chiarezza che il dato testuale sembrerebbe mostrare prima facie, nel senso di escludere automaticamente qualsiasi presunzione al riguardo, deve infatti rilevarsi che l'espressa enunciazione del dettato normativo dispone che il solo compimento dell'operazione fraudolenta non costituisca "di per sé" e "necessariamente" prova della colpa grave dell'utilizzatore. L'unica presunzione che appare vietata dalla richiamata disposizione è quella relativa dell'affermazione della colpa grave esclusivamente collegata all'utilizzo della carta; da ciò ne discende, a contrario, che sia invece ammissibile tale presunzione, laddove sussista una serie di elementi di fatto univoca e convergente, sicché possa ragionevolmente ritenersi che l'uso fraudolento sia effettivamente riconducibile sul piano causale alla condotta dell'utilizzatore. Nel caso di specie sembrano emergere elementi di grave colpa, posto che il furto è collocato in un arco di tempo di oltre un giorno (tra le 13.00 del giorno 11.11.2013 alle ore 14.00 del giorno 12.11.2013, durante la pausa pranzo); che il ricorrente sembra essersi avveduto della sottrazione con due giorni di ritardo; che il frodatore ha compiuto un solo prelievo diretto, senza altri tentativi (comportamento anomalo per le frodi). Su questa linea, il ricorrente non sembra aver custodito con diligenza né la carta, né le credenziali»; ABF, Coll. Coord., 29 novembre 2013, n. 6198.

(17) Cfr., fra molti, E. Fusco, *Utilizzo improprio di un home banking da parte del rappresentante del correntista e perimetro della (ir)responsabilità dell'istituto di credito, tra legge antiriciclaggio, codice civile e disciplina sui servizi di pagamento*, in *Banca, borsa e tit. cred.*, 2021, II, 499 ss. e *ivi* ulteriori riferimenti.

(18) Secondo tale l'orientamento, il pericolo di utilizzi fraudolenti dello strumento di pagamento è riconducibile all'area dei rischi tipici connessi alla prestazione del relativo servizio di pagamento, rispetto al quale l'intermediario è tenuto a predisporre misure di sicurezza idonee a controllarlo, prevenirlo ed evitarlo. Se ne trae la conseguenza, sul piano probatorio, in virtù dei principi generali della responsabilità da inadempimento contrattuale, dell'allocazione a carico del prestatore di servizi di pagamento dell'onere di dimostrare di aver adempiuto tale obbligo con la diligenza tecnica e professionale dell'«accorto banchiere», ai sensi dell'art. 1176, comma 2, c.c. In tal senso, v. Cass. 12 giugno 2007, n. 13777, in *Banca, borsa, tit. cred.*, 2007, II, 21 ss.; Cass. 3 settembre 2015, n. 17547; Cass. 19 gennaio 2016, n. 806, in *Banca, borsa, tit. cred.*, 2016, II, 394 ss.; Cass. 3 febbraio 2017, n. 2950; Cass. 12 aprile 2018, n. 9158, in *Resp. civ.*, 2019, 622; Trib. Parma 6 settembre 2018, in particolare sul carattere oggettivo o semi-oggettivo della responsabilità della banca; da ultimo, v. Trib. Napoli Nord 2 luglio 2019, (inedita) in un caso di addebiti non autorizzati a valere su carta prepagata.

(19) Cfr. Ciraolo, *Pagamento fraudolento con carta di credito e ripartizione delle responsabilità. Dagli orientamenti attuali alla revisione della PSD*, cit.,156-157, secondo cui, resta comunque ferma la responsabilità del prestatore di servizi; Minneci, *Pagamenti elettronici non autorizzati: la tutela del cliente alla luce degli orientamenti dell'ABF*, in *Giur. comm.*, 2022, I, 1056. Tuttavia, Miotto - Speranzin, *I pagamenti elettronici*, in *Fintech*, a cura di Cian e Sandei, Padova, 2020, 188 ss., evidenziano come la tecnica delle frodi informatiche, sempre più evolute, comprometta notevolmente l'applicazione del concorso di colpa (art. 1227 c.c.), poiché la condotta dovuta dal cliente risulta sempre meno incidente sull'evento. E nella giurisprudenza di merito, tra molti, Trib. di Padova, 21 novembre 2023, n. 2309, in *ONE Legale*.

liberare fornendo la prova di un comportamento diligente, nella fattispecie, dell'adozione degli standard di sicurezza più elevati secondo lo stato dell'evoluzione tecnica. Si tratta di una diretta conseguenza immanente nel principio del rischio di impresa, secondo cui l'intermediario deve sopportare le conseguenze negative (non imputabili a terzi) dell'attività da cui trae utilità economica, potendo frazionare il relativo costo sulla totalità dei propri clienti, attraverso la determinazione dei prezzi di vendita dei propri beni e servizi (20).

Le soluzioni adottate dall'Arbitro Bancario Finanziario consegnano, tuttavia, all'interprete una vasta casistica, a dispetto delle vicende trattate innanzi alla giurisdizione ordinaria, probabilmente per via dell'esiguo costo d'accesso e della speditezza delle soluzioni adottate dal sistema alternativo di risoluzione delle controversie (21).

Per quanto qui d'interesse, con particolare riguardo agli obblighi di custodia dello strumento di pagamento e di riservatezza del PIN, l'ABF ha riconosciuto la colpa grave del cliente nei soli casi in cui questi abbia agito con macroscopica negligenza, lasciando incustoditi sia la carta, sia il relativo codice (22). Nei casi, come quello della sentenza in commento, nei quali i codici di accesso ai servizi di pagamento vengano sottratti con l'inconsapevole collaborazione del titolare dello strumento di pagamento, l'ABF ha statuito che il cliente risponde solo ove il raggiro sia stato attuato con modalità del tutto evidenti, come una mail dal contenuto sgrammaticato o non correlabile al sito della banca (23). Al contrario, laddove la frode sia compiuta con tecnologie e mezzi più sofisticati, come ad esempio, nel caso del cd. *man in the browser*, la responsabilità resta a carico del prestatore del servizio di pagamento (24). Essenzialmente, si tratta di valutare, caso per caso, le concrete modalità con cui il raggiro del cliente è stato realizzato, valutando anche l'attitudine a trarre in inganno una persona minimamente avveduta, ovvero se, in altri termini, l'uso di un grado elementare di prudenza e diligenza sarebbe valso ad evitare il danno (25).

Pertanto, qualora venga accertata la responsabilità del prestatore di servizi, questi è obbligato a restituire o risarcire il valore monetario indebitamente sottratto. Se si accetta l'interpretazione secondo cui l'ordine di pagamento rappresenta uno *iussum* del cliente diretto al PSP, secondo lo schema delegatorio, e se è proprio la fase di autorizzazione a risultare compromessa, con l'assenza di ogni connessione diretta dell'ordine al titolare dello strumento, allora tale operazione non dovrebbe riflettersi nel rapporto tra le parti. Di conseguenza, le registrazioni contabili del cliente necessitano di essere corrette, come previsto dall'articolo 25 d.lgs. n. 11/2010, attraverso un "rimborso", come se l'operazione di pagamento non fosse mai avvenuta (26). Diversamente, deve parlarsi di risarcimento allorché l'anomalia attenga alla fase esecutiva del procedimento, cioè nel trasferimento intermediato di fondi dal pagatore al beneficiario non correttamente eseguito. E solo in questa ipotesi che il rimedio va concettualmente ricercato nell'area del risarcimento del danno (27).

(20) Il costo del rischio correlativo che l'impresa assume su di sé si riverbererebbe, tendenzialmente, positivamente sul mercato: sul punto, cfr. Trimarchi, La *responsabilità civile: atti leciti, rischio, danno*, Milano, 2021, 301 ss.

(21) In particolare, sulle caratteristiche del procedimento innanzi all'ABF, v. Pagni, *L'arbitro bancario finanziario: natura e funzioni di uno strumento particolare per la risoluzione delle controversie*, in *Arbitro Bancario e Finanziario*, diretto da Conte, Milano, 2021, 8 ss.

(22) L'ABF, pronunciandosi su un furto di bancomat, ha negato che la prova della corretta digitazione del codice PIN al primo tentativo sia sufficiente a dimostrare la colpa grave del titolare della carta (ABF Milano, 9 ottobre 2018, n. 20897). Ha rilevato, in particolare, come il carattere sempre più sofisticato delle tecniche di sottrazione dei codici identificativi personali renda possibile che l'acquisizione avvenga a prescindere da qualsiasi colpa del cliente. Lo stesso Collegio di Coordinamento ABF (26 ottobre 2012, n. 3498) ha escluso ogni responsabilità a carico del cliente quando sia accertata un'aggressione informatica operata attraverso malware sofisticati, capaci di "sorprendere la buona fede anche di un pur normalmente attento fruitore del servizio. Ma per una presunzione di colpa grave nella conservazione dei codici unitamente alle carte, in ragione del breve lasso temporale tra il furto del bancomat e il primo dei prelievi abusivi, ritenuto incompatibile con la clonazione o autonoma estrazione di PIN da carte munite di chip", v. Trib. Milano, 27 settembre 2018, n. 9439; ABF Milano, 20 gennaio 2024, n. 908; ABF Milano, 20 gennaio 2024, n. 907, ABF Milano, 25 gennaio 2024, n. 1171.

(23) ABF Milano, 14 ottobre 2016, n. 9177, ABF Napoli, 20 ottobre 2016, n. 9322, ABF Napoli, 20 ottobre 2016, n. 9343, ABF Milano, 21 ottobre 2016, n. 9409. Si tratta, infatti, di un fenomeno «ormai del tutto noto con l'effetto che qualunque utente dotato di normale avvedutezza e prudenza è in grado di non farsi trarre in inganno anche per il risalto che viene dato al fenomeno in tutti i siti degli intermediari»: ABF Milano, 22 novembre 2016, n. 10306. ABF Milano, 24 gennaio 2024, n. 1032, ABF, Palermo, 22 gennaio 2024, n. 951.

(24) ABF Collegio di Coordinamento, 26 ottobre 2012, n. 3498; ABF Roma, 9 febbraio 2017, n. 1179; ABF Napoli, 25 luglio 2017, n. 9080.

(25) Cfr. ABF Bologna, 25 gennaio 2024, n. 1163, in particolare, sulla mancata prova della cattiva gestione delle credenziali da parte dell'utente, nonostante l'intermediario avesse implementato un processo di autenticazione che prevedeva l'uso di un PIN dispositivo e la possibilità di effettuare operazioni tramite un'applicazione mobile. La documentazione fornita, al riguardo, non ha chiarito con certezza l'utilizzo della procedura di SecureCall per l'autorizzazione dell'operazione fraudolenta. Nel dettaglio, non è emerso chiaramente se durante l'autorizzazione dell'operazione fraudolenta sia stata effettuata una chiamata SecureCall, un elemento chiave per la sicurezza dell'operazione.

(26) Sul rimborso integrale delle somme, senza applicazione della franchigia in caso di mancata produzione da parte dell'intermediario di documentazione idonea a dimostrare la corretta e regolare autenticazione della transazione contestata, fra molte, v. ABF Bologna, 24 gennaio 2024, n. 1042; ABF Bologna, 24 gennaio 2024, n. 1060; ABF Milano, 20 gennaio 2024, n. 905.

(27) De Stasio, *Riparto delle responsabilità e restituzioni nei pagamenti non autorizzati*, in *Attualità di Diritto bancario*, a cura di Minneci e Tina, Milano, 2021, 81.

# Sempre vietata la ripresa non casuale dell'immagine di un minore che ne consenta l'identificazione

Corte di Cassazione; sezione terza; ordinanza 1° febbraio 2024, n. 2978 – Pres. Travaglino – Rel. Spaziani.

*La ripresa non casuale avvenuta in pubblico che sia diretta espressamente alla identificazione del minore ed alla sua riconoscibilità costituisce un limite invalicabile che, a prescindere dalla effettiva lesione del decoro, della reputazione o dell'onore, rende inoperante la deroga al generale divieto di pubblicazione dell'immagine senza consenso in presenza di collegamento con eventi di interesse pubblico o comunque svolti in pubblico.*

*...Omissis...*

**Rilevato in fatto che**

Con sentenza 12 luglio 2022, n. 11113, il Tribunale di Roma ha rigettato la domanda proposta da B.B. e C.C., in qualità di genitori esercenti la responsabilità genitoriale sul minore A.A., avente ad oggetto, oltre l'inibizione della continuazione dell'illecito, il risarcimento dei danni patrimoniali e non patrimoniali subiti in conseguenza della non autorizzata pubblicazione della sua immagine dopo essere stato casualmente ripreso nel corso di un servizio di telegiornale effettuato in occasione dell'arresto di un latitante e successivamente diffuso mediante il mezzo televisivo e le piattaforme digitali.

2. Il Tribunale, pronunciando nel contraddittorio con il danneggiato, costituitosi personalmente in giudizio al raggiungimento della maggiore età, pur dando atto che nella citazione "si faceva riferimento al diritto all'immagine come espressione della riservatezza" (p. 5 della sentenza impugnata) – e pur qualificando, dunque, la domanda come di risarcimento del danno per lesione dei detti diritti della personalità, e non per illecito trattamento di dati personali – ha nondimeno ordinato il mutamento di rito, ai sensi dell'art. 10 del D. Lgs. n. 150 del 2011, disponendo procedersi con il rito speciale previsto per le controversie di cui all'art. 152 del D.Lgs. n. 196 del 2003, il quale, tra l'altro, non prevede la ricorribilità in appello.

Nel merito, il Tribunale, ritenuto di non dover provvedere sull'istanza di inibitoria (sul rilievo che non sarebbero state contestate, dalla parte attrice, le deduzioni svolte dalla convenuta in ordine all'avvenuta rimozione delle immagini da ogni piattaforma riferibile alla RAI), ha rigettato la domanda risarcitoria sulla base di una duplice *ratio decidendi*.

In primo luogo, ha escluso la stessa sussistenza dell'illecito, sul rilievo che, pur mancando il consenso dei genitori alla pubblicazione dell'immagine del minore, ai sensi dell'art. 96 della legge n. 633 del 1941, tuttavia ricorresse una delle ipotesi eccezionali di cui all'art. 97, primo comma, stessa legge, avuto riguardo, per un verso, al contenuto delle immagini divulgate, collegate ad un'esigenza informativa correlabile al diritto di cronaca, in quanto dirette a rappresentare l'arresto "in diretta" di un latitante, effettuato dalle forze dell'ordine sulla strada pubblica; e considerato, per altro verso, il carattere del tutto occasionale della presenza, nel servizio di informazione televisiva, dell'immagine del ragazzo, il quale si era venuto a trovare casualmente sulla strada al momento dell'arresto del latitante ed era stato quindi ripreso dalle telecamere unitamente ad una massa indistinta di persone, senza alcuna volontà di polarizzare l'attenzione sulla sua identità e sulla sua riconoscibilità.

In secondo luogo, il giudice del merito, ha escluso, in ogni caso, la sussistenza di conseguenze dannose, sia non patrimoniali che patrimoniali, osservando, quanto alle prime, che era rimasta sfornita di prova la deduzione attorea secondo cui, a causa dell'accostamento della sua immagine a quella di un delinquente, il minore era stato etichettato come tale nell'ambito dell'ambiente scolastico, con pregiudizio del suo rendimento; e rilevando, con riguardo alle seconde, la non configurabilità, nella fattispecie, di un pregiudizio correlato allo sfruttamento dell'immagine.

3. Propone ricorso per cassazione A.A. sulla base di tre motivi. Risponde con controricorso la RAI - Radiotelevisione Italia Spa.

La trattazione del ricorso è stata fissata in adunanza camerale, ai sensi dell'art. 380-*bis*.1 cod. proc. civ.

Il Procuratore Generale non ha depositato conclusioni scritte.
Entrambe le parti hanno depositato memoria.

**Considerato in diritto**
Con il primo motivo viene denunciata la "violazione e/o falsa applicazione dell'art. 10 D.lgs. 150/2021 in relazione all'art. 360 c.p.c., comma 1, n. 3".
Il ricorrente deduce che il Tribunale, pur riconoscendo che nell'atto di citazione si lamentava, non già la violazione del diritto alla protezione dei dati personali mediante l'illecita diffusione di essi, bensì la lesione dei diritti all'immagine e alla riservatezza, avrebbe, nondimeno, disposto il mutamento di rito ai sensi dell'art. 10 del D.Lgs. n. 150 del 2011 ed ordinato procedersi con il rito speciale lavoristico previsto per le controversie di cui all'art. 152 del D.lgs. n. 196/2003, sul presupposto che, nella comparsa di costituzione della RAI, si facesse, invece, riferimento alla capacità del minore di prestare consenso al trattamento dei propri dati personali.
Sostiene, dunque, il ricorrente che il mutamento di rito sarebbe stato erroneamente disposto, non già sulla base delle richieste formulate dalla parte attrice, ma sulla base delle difese svolte dalla parte convenuta e nonostante fosse stata proposta una ordinaria domanda risarcitoria.
1.1. Il motivo, censurando l'errore sul rito – in thesi – commesso dal giudice del merito per avere erroneamente adottato un rito diverso da quello previsto dalla legge in relazione al contenuto della domanda proposta, si palesa inammissibile, avuto riguardo al principio generale, desumibile dal consolidato orientamento di questa Corte, secondo cui l'errore sul rito può essere denunciato per cassazione come specifico *error in procedendo* da cui deriva la nullità del procedimento e della sentenza di merito impugnata soltanto ove sia dedotto e provato che tale errore abbia inciso sul contraddittorio o sull'esercizio del diritto di difesa o abbia comunque provocato alla parte deducente un pregiudizio processuale effettivamente apprezzabile (*ex multis*, Cass. 29/09/2005, n. 19136; Cass. 17/10/2014, n. 22075; Cass. 05/04/2018, n. 8422).
La mancata indicazione dello specifico pregiudizio processuale seguito alla adozione di un rito diverso da quello previsto dalla legge rende invece la doglianza inammissibile per difetto di interesse, poiché l'esattezza del rito non deve essere considerata fine a sé stessa, ma può essere invocata solo per riparare una precisa ed apprezzabile lesione che, in conseguenza del rito seguito, sia stata subìta sul piano pratico processuale (Cass., Sez. Un., 17/02/2009, n. 3758).
Nel caso di specie, il ricorrente non ha né dedotto né tanto meno provato il pregiudizio effettivo al proprio diritto di difesa che sarebbe seguito dal mutamento di rito erroneamente disposto dal giudice del merito.
In proposito, non rileva l'allegazione contenuta solo nella memoria illustrativa, diretta ad identificare il predetto pregiudizio con la negazione della facoltà di proporre appello, atteso che la memoria depositata ai sensi degli artt. 378 e 380-*bis*.1 cod. proc. civ. non può integrare i motivi del ricorso per cassazione, poiché assolve all'esclusiva funzione di chiarire ed illustrare i motivi di impugnazione che siano già stati ritualmente – ovverosia in maniera completa, compiuta e definitiva – enunciati nell'atto introduttivo del giudizio di legittimità, con il quale si esaurisce il relativo diritto di impugnazione (cfr. già, Cass.08/08/1986, n. 5000; più recentemente, Cass.20/12/2016, n. 26332; Cass. 30/03/2023, n. 8949).
Pertanto, il primo motivo di ricorso deve essere dichiarato inammissibile.
2. Con il secondo motivo viene denunciata la "violazione e/o falsa applicazione degli artt. 96 e 97 l. 633/41 e dell'art. 137 D.lgs. 196/2003, in relazione all'art. 360 c.p.c., comma 1, n. 3".
Il ricorrente, ricostruito il quadro normativo desumibile dagli artt. 96 e 97 della legge n. 633 del 1941 e dall'art. 137 del D.lgs. n. 196 del 2003 – ed evocate anche le disposizioni di diritto internazionale strumentali alla tutela della riservatezza della persona minore di età contenute negli artt.3 e 16 della Convenzione di New York del 1989 (ratificata con legge n. 176 del 1991) – sostiene che la sentenza impugnata conterrebbe "due affermazioni diametralmente opposte" (p. 17 del ricorso): la prima, compiuta reputando che la pubblicazione della sua immagine fosse fondata su una esigenza informativa, ritenuta correlabile al diritto di cronaca, emergente dall'intento di mostrare (anche) la reazione della comunità in cui si trovava il latitante, i cui membri, anziché prendere le distanze dall'arrestato, avrebbero assistito all'arresto e sarebbero persino andati a salutarlo; la seconda, compiuta qualificando come casuale la sua presenza in strada ed escludendo che la pubblicazione della sua immagine fosse stata posta in essere con la volontà di polarizzare l'attenzione sulla sua identità e riconoscibilità.
Le due affermazioni sarebbero in contrasto in quanto, se l'intento del giornalista fosse stato effettivamente quello di rappresentare un contesto sociale "malato" nel quale veniva reso omaggio ad un latitante arrestato, a tale intento non avrebbe potuto che corrispondere la volontà di polarizzare l'attenzione anche sull'identità dei soggetti coinvolti e sulla loro riconoscibilità.
La pubblicazione dell'immagine sarebbe stata quindi senz'altro illecita, sia perché sarebbe stata compiuta in pregiudizio all'onore, alla reputazione e al decoro della persona ritratta (art. 97, secondo comma, legge n. 633 del 1941), sia per l'avvenuta polarizzazione dell'attenzione sull'identità e riconoscibilità di un soggetto minorenne, indebitamente accostato ad un delinquente.

2.1. Anche questo motivo è inammissibile.
2.1.a. Il diritto all'immagine è tutelato nel nostro ordinamento nel codice civile (art. 10) e nella legge n. 633 del 1941 sulla protezione del diritto d'autore (artt. 96 e 97), che detta il completamento della disciplina codicistica.
Dal combinato disposto della disposizione del codice civile e delle disposizioni della legge speciale, si desume la regola che pone il divieto di esporre o pubblicare l'immagine di una persona.
Il divieto non è assoluto nell'ipotesi in cui l'esposizione o la pubblicazione non rechi pregiudizio all'onore, al decoro o alla reputazione della persona ritratta, perché in questa ipotesi l'esposizione o la pubblicazione è eccezionalmente ammessa quando sussista il consenso della persona medesima (art. 96 legge n. 633 del 1941) o quando ricorra una delle fattispecie tassativamente stabilite dalla legge in deroga al divieto stesso (notorietà della persona; ufficio pubblico da essa ricoperto; necessità di giustizia o di polizia; sussistenza di scopi scientifici, didattici o culturali; collegamento della riproduzione con fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico: art. 97, primo comma, l. n. 633 del 1941).
Il divieto è, invece, assoluto nella contraria ipotesi in cui l'esposizione o la pubblicazione rechi pregiudizio all'onore, al decoro o alla reputazione della persona ritratta, perché in questa ipotesi l'esigenza del rispetto dell'intimità della persona prevale sull'esigenza sociale di pubblica conoscenza della sua immagine, sicché non sono ammesse deroghe al divieto di divulgazione (art. 97, secondo comma, l. n. 633 del 1941).
2.1.b. Il diritto all'immagine – configurato in dottrina talora come manifestazione del più ampio diritto alla riservatezza, talaltra come autonomo diritto della personalità – ha un duplice contenuto, negativo e positivo.
Sotto il primo profilo, il diritto tutela l'interesse del titolare a che la sua immagine non venga diffusa o esposta in pubblico; la correlativa situazione giuridica soggettiva passiva posta in capo alla totalità (*erga omnes*) dei consociati consiste in un dovere di astensione.
Sotto il secondo profilo, il diritto tutela l'interesse del titolare ad apparire in pubblico nella misura in cui abbia interesse a farlo; la correlativa situazione giuridica soggettiva passiva posta in capo alla totalità (*erga omnes*) dei consociati consiste in un obbligo di *pati*.
Tanto il primo quanto il secondo aspetto del diritto hanno avuto, nell'elaborazione giurisprudenziale, una rilevante capacità espansiva, evolvendo verso forme di tutela più estese di quelle circoscritte dalle norme di diritto positivo dianzi ricordate.
Con riguardo al contenuto positivo del diritto, il crescente riconoscimento sociale della facoltà della persona di apparire in pubblico nella misura in cui abbia interesse a farlo, si è tradotto nel giudizio di meritevolezza di tutela (art. 1322, secondo comma, cod. civ.) dell'interesse patrimoniale del soggetto allo sfruttamento commerciale della propria immagine verso un corrispettivo, ponendo le basi, da un lato, per la diffusione del contratto atipico di sponsorizzazione (Cass. n. 9880 del 1997; Cass. n. 7083 del 2006; Cass. n.12801 del 2006; Cass. n.18218 del 2009); dall'altro lato, per il riconoscimento della risarcibilità del pregiudizio economico rappresentato dalla perdita del corrispettivo dell'utilizzazione della propria immagine a fini pubblicitari (Cass. n. 22513 del 2004; Cass. n. 1875 del 2019), così autorizzandosi la dottrina a ritenere esistente, anche nel nostro ordinamento, la figura, di derivazione americana, del right of publicity.
Con particolare riguardo al contenuto negativo del diritto – ovverosia l'aspetto che assume rilievo nella presente sede – deve osservarsi che nella giurisprudenza di questa Corte si è affermato, ed è andato consolidandosi, l'orientamento tendente ad operare una integrazione delle fonti della disciplina del diritto soggettivo in esame, individuandole, non più soltanto nella norma codicistica (art. 10 cod. civ.) e nelle disposizioni della legge sul diritto d'autore (artt. 96 e 97 della legge n. 633 del 1941), ma anche nel Codice in materia di protezione dei dati personali (D.Lgs. 30 giugno 2003, n. 196).
In tema di informazione fornita con il servizio televisivo (e con specifico riguardo al caso di diffusione dell'immagine di persone riprese di nascosto) è stato, ad es., ripetutamente affermato che la presenza delle condizioni legittimanti l'esercizio del diritto di cronaca non implica, di per sé, la legittimità della pubblicazione o diffusione anche dell'immagine delle persone coinvolte, la cui liceità è subordinata, oltre che al rispetto delle prescrizioni contenute negli artt. 10 cod. civ., 96 e 97 della legge n. 633 del 1941, anche all'osservanza di quelle contenute nell'art. 137 del D.lgs. n. 196 del 2003 e nell'art. 8 del codice deontologico dei giornalisti, nonché alla verifica in concreto della sussistenza di uno specifico ed autonomo interesse pubblico alla conoscenza delle fattezze dei protagonisti della vicenda narrata, nell'ottica della essenzialità di tale divulgazione ai fini della completezza e correttezza della informazione fornita (Cass. n. 15360 del 2015; Cass. n. 18006 del 2018).
Sempre in tema di attività giornalistica (con riguardo alla fattispecie di pubblicazione su quotidiano di fotografia di persona in stato di detenzione) è stato inoltre statuito che la pubblicazione è legittima se sia rispettosa, oltre che dei limiti, fissati dagli artt. 20 e 25 della legge n. 675 del 1996 (*ratione temporis* applicabili) e, comunque, riprodotti nell'art. 137 del D.lgs. n. 196 del 2003, di essenzialità per illustrare il contenuto della notizia e quelli dell'esercizio del diritto di cronaca, anche delle particolari cautele imposte a tutela della persona ri-

tratta, previste dall'art. 8 del codice deontologico dei giornalisti, che costituisce fonte integrativa; si è inoltre puntualizzato che l'osservanza dei suddetti limiti va accertata con maggior rigore rispetto alla semplice pubblicazione della notizia, per la maggiore potenzialità lesiva dello strumento visivo e la maggiore idoneità ad una diffusione decontestualizzata e insuscettibile di controllo da parte della persona ritratta (Cass. n. 12834 del 2014).
2.1.c. Il consolidarsi dell'orientamento giurisprudenziale tendente ad integrare le fonti regolatrici del diritto della personalità in esame, si è tradotto nel riconoscimento di una sua maggiore estensione e di una più penetrante e satisfattiva protezione in sede giudiziaria, comportando implicazioni sul giudizio di comparazione tra l'esigenza di tutela dell'interesse della persona a non veder diffusa o esposta in pubblico la propria immagine e l'esigenza di tutela del contrario interesse sociale di pubblica conoscenza dell'immagine medesima, che giustifica la deroga al divieto di esposizione o pubblicazione nelle specifiche ipotesi tassativamente indicate dalla legge.
L'individuazione della fonte regolatrice del diritto anche nelle norme del codice della privacy, implica, infatti, che nel giudizio di bilanciamento assuma un peso maggiore l'esigenza di protezione della sfera privata della persona rispetto alla contraria esigenza di consentirne l'esposizione e la diffusione dell'immagine in quelle tassative fattispecie in cui – escluso comunque il pregiudizio all'onore, al decoro o alla reputazione – sussista un interesse generale a renderla pubblica.
2.1.d. L'esigenza di protezione della sfera privata rispetto a quella di tutela dell'interesse pubblico alla diffusione della sua immagine assume particolare preminenza nell'ipotesi in cui si tratti di persona minore d'età.
Con riferimento a tale fattispecie, la Suprema Corte ha infatti affermato che anche quando non ricorra il caso limite della lesione del decoro, della reputazione o dell'onore della persona di cui all'art. 97, secondo comma, della legge n. 633 del 1941 e si integri, al contrario, in astratto, una delle fattispecie (in particolare il collegamento con un evento di interesse pubblico o comunque svoltosi in pubblico) indicate dal primo comma della detta disposizione, può nondimeno escludersi che operi, in concreto, la deroga legale al divieto di riproduzione dell'immagine prevista dalla stessa norma, allorché alla circostanza soggettiva della minore età della persona si accompagni quella, oggettiva, della non casualità della ripresa, espressamente diretta a polarizzare l'attenzione sull'identità del minore e sulla sua riconoscibilità (Cass. 13/05/2020, n. 8880).
2.1.e. Nella vicenda in esame, il Tribunale ha debitamente tenuto conto delle fonti regolatrici del diritto e dei limiti del divieto di pubblicazione dell'immagine della persona e ha debitamente svolto l'accertamento di merito alla luce degli illustrati principi di diritto.
Il giudice del merito, infatti, ha accertato, per un verso, la sussistenza di una delle tassative ipotesi in cui la pubblicazione dell'immagine della persona è consentita dalla legge a prescindere dal suo consenso, in quanto giustificata dal suo collegamento con un evento – l'arresto di un latitante nell'ambito del contesto sociale in cui si era nascosto – connotato dall'interesse pubblico all'informazione e, per di più, svoltosi in luogo pubblico; per altro verso, l'insussistenza delle circostanze obiettive che avrebbero escluso la liceità della pubblicazione dell'immagine di una persona minore di età, la quale era stata ripresa nell'ambito di un servizio di cronaca televisiva in modo del tutto casuale, all'interno di una massa indistinta di persone, senza alcun intento di renderla identificabile o riconoscibile da parte di chi avesse veduto il filmato.
Nell'obiettare a tale motivato accertamento l'opposto rilievo che, al contrario, la pubblicazione dell'immagine sarebbe stata compiuta in pregiudizio all'onore, alla reputazione e al decoro della persona minorenne e con l'intento di polarizzare l'attenzione sulla sua identità e riconoscibilità, il motivo di ricorso in esame, ad onta della formale intestazione, non denuncia un *error in iudicando* ma tende a suscitare dalla Corte di legittimità un nuovo giudizio di merito in contrapposizione a quello motivatamente formulato dal Tribunale nel rispetto dei principi di diritto applicabili alla fattispecie.
Pertanto, anche il secondo motivo di ricorso deve essere dichiarato inammissibile.
3. Con il terzo motivo viene denunciata la "violazione e/o falsa applicazione dell'art. degli artt. 10, 2043, 2059 e 2697 c.c., in relazione all'art. 360 c.p.c., comma 1, n. 3".
Il ricorrente censura la sentenza impugnata per avere escluso la prova del danno non patrimoniale e sostiene che, essendo stati da lui indicati chiaramente gli elementi indiziari di tale pregiudizio (con particolare riferimento al contesto sociale in cui egli viveva e all'ampia ampia diffusione del servizio giornalistico), il Tribunale avrebbe dovuto fare "ricorso alla prova presuntiva del turbamento dell'animo" (p.22 del ricorso).
3.1. Anche questo motivo è inammissibile, non solo perché diretto a censurare un motivato giudizio di merito, non sindacabile in sede di legittimità, ma anche – prima ancora – per difetto di interesse: invero, all'esito della reiezione del secondo motivo di ricorso, ha trovato conferma definitiva la statuizione del Tribunale diretta ad escludere il carattere illecito della pubblicazione, per modo che non assume rilevanza il giudizio sulla sussistenza del danno.
4. In definitiva, il ricorso proposto da A.A. deve essere dichiarato inammissibile.

5. Le spese del giudizio di legittimità seguono la soccombenza e vengono liquidate come da dispositivo.
8. Avuto riguardo al tenore della pronuncia, va dato atto – ai sensi dell'art. 13, comma 1-*quater*, del D.P.R. n. 115 del 2002 – della sussistenza dei presupposti processuali per il versamento, da parte del ricorrente, di un ulteriore importo a titolo contributo unificato, pari a quello previsto per la proposizione dell'impugnazione, se dovuto. P.Q.M. La Corte dichiara inammissibile il ricorso; condanna il ricorrente a rimborsare alla società controricorrente le spese del giudizio di legittimità, che liquida, in Euro 3.100,00 per compensi, oltre alle spese forfetarie, agli esborsi liquidati in Euro 200,00 ed agli accessori di legge.
*...Omissis...*

# IL COMMENTO

*di Massimiliano Marotta*

**Sommario:** 1. Il caso all'esame della Cassazione. – 2. L'evoluzione del diritto all'immagine ed il superamento di una concezione unicamente civilistica. –3. Il consenso quale primo limite alla divulgazione. – 4. L'equilibrio tra attività giornalistica, diritto di cronaca e tutela dell'immagine. – 5. L'individuazione del danno non patrimoniale e la difficoltà di una visione unanime. – 6. Brevi considerazioni conclusive.

Le previsioni normative tese a scongiurare che la pubblicazione dell'immagine di una persona possa recare pregiudizio al decoro ed alla reputazione della stessa trovano, quale unico limite, la riserva di legge in senso generale e, più nello specifico, la sussistenza di casi tali da escludere il consenso all'utilizzo, quali la notorietà o il ricoprire un pubblico ufficio ovvero il collegamento a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico. Tuttavia, anche in presenza delle citate circostanze "liberatorie", il divieto di riproduzione dell'immagine non legittimata da consenso permane laddove si tratti di soggetto minore d'età non ripreso per pura casualità e con lo scopo di consentirne l'identificazione e la riconoscibilità.

*The regulatory provisions aimed at preventing the publication of a person's image from causing damage to the decorum and reputation of the same find, as the only limit, the legal reservation in a general sense and, more specifically, the existence of cases such as to exclude consent to use for cases of notoriety or public office held or connection to facts, events, ceremonies of public interest or held in public. However, even in the presence of the aforementioned "liberating" circumstances, the prohibition on reproduction of the image not legitimized by consent remains where the subject is a minor and not filmed purely by chance and with the aim of allowing identification and recognisability.*

## 1. Il caso all'esame della Cassazione

Il ricorrente insorge contro la decisione del Tribunale di primo grado con la quale era stata rigettata la domanda avente ad oggetto, oltre l'inibizione della continuazione dell'illecito, il risarcimento dei danni patrimoniali e non subiti in conseguenza della non autorizzata pubblicazione dell'immagine di un minore casualmente ripreso nel corso di un servizio giornalistico.

Dopo aver dato atto all'attore di aver disegnato puntualmente la cornice normativa all'interno della quale collocare la tematica oggetto di ricorso, con particolare riferimento agli artt. 96 e 97 L. 633 del 1941 e dell'art. 137 D.Lgs. n. 196 del 2003 oltre che alla Convenzione di New York del 1989 ratificata in Italia nel 1991 in materia di salvaguardia della *privacy* dei minori, la Corte si dedica ad una vera e propria illustrazione della normativa applicabile, evidenziando come la protezione del diritto all'immagine, radicata sia nel codice civile (art. 10) che nella legge sulla protezione del diritto d'autore (artt. 96 e 97) (1), prenda forma nel divieto di divulgazione del ritratto di una persona senza il consenso che costituisce presupposto anche per il caso in cui la divulgazione non pregiudichi l'onore, la reputazione e il decoro del soggetto ritratto. Ricorda il Supremo Consesso come il divieto diventi assoluto quando la divulgazione danneggi l'onore o la reputazione dell'individuo, sottolineando come la tutela della sfera privata prevalga, in questo caso, sull'interesse pubblico alla conoscenza dell'immagine (art. 97, comma 2, L. n. 633 del 1941).

Il diritto all'immagine, che rappresenta espressione specifica del diritto alla riservatezza ma che viene, ormai, individuato come autonomo diritto della personalità a fronte di un processo di costituzionalizzazione, implica la tutela contro la diffusione non autorizzata quale proiezione del diritto di decidere quando e come apparire pubblicamente.

Tale diritto ha visto un'espansione significativa della sua protezione giurisprudenziale, evolvendo oltre i confini stabiliti dalla legge. L'approccio nomofilattico ha integrato le norme tradizionali con quelle del Codice in materia di protezione dei dati personali, sostenendo che la legittimità della diffusione dell'immagine richieda non solo il rispetto delle norme sul diritto d'autore e del codice civile, ma anche la verifica di un interesse pubblico specifico e autonomo alla divulgazione, al fine di garantire una informazione completa e corretta. Inoltre, il formante giurisprudenziale ha riconosciuto l'importanza di proteggere la sfera privata, soprattutto nel caso di minori, stabilendo che anche in presenza di un interesse pubblico alla divulgazione, si può escludere la riproduzione dell'immagine se questa è finalizzata a identificare il minore, sottolineando la necessità di un equilibrio tra la tutela della privacy individuale e l'interesse pubblico alla diffusione dell'immagine.

Il ragionamento del Giudice dell'impugnazione, tuttavia, non può non essere interpretato come la volontà di riaffermare e meglio precisare principi posti a governo del diritto all'immagine dell'individuo se si tiene conto che la formula utilizzata per respingere il secondo motivo di impugnazione – inammissibilità per inesistenza di profili di legittimità confusi con ragioni di merito – non avrebbe necessariamente richiesto un *excursus* normativo sulla tematica.

## 2. L'evoluzione del diritto all'immagine ed il superamento di una concezione unicamente civilistica

Col provvedimento che si annota il Giudice di legittimità conferma, nella sostanza, quella tendenza già pervicacemente intrapresa da dottrina e giurisprudenza diretta verso un'importante estensione dello spettro di protezione del diritto all'immagine sotto il profilo della meritevolezza (2). Nella pratica, infatti, si è dato corso ad una tanto evidente quanto crescente risposta all'esigenza di tutela dell'immagine vuoi come specifica manifestazione del diritto alla riservatezza (3), vuoi come vero e proprio diritto della personalità.

Il risultato è stato quello di una lettura costituzionalmente orientata del Giudice di legittimità che, sulla falsariga di ogni diritto di libertà, ha attribuito a quello all'immagine, contemporaneamente, un profilo c.d. positivo ("libertà di") (4) ed un profilo c.d. negativo ("libertà da"), di modo che in ossequio al primo il soggetto possa utilizzare come crede la propria immagine (quale proiezione del diritto alla libertà personale *ex* art. 12 Cost.), mentre grazie al secondo sia in grado di avvalersi del diritto alla riservatezza (5).

(1) In realtà, la Corte di Cassazione sostiene da tempo l'insufficienza degli artt. 10 c.c. e 97 L. n. 633 del 1941 per una compiuta disciplina del diritto all'immagine sollecitando un'autonoma e più rigorosa previsione.

(2) Diverse, nel tempo, sono le declinazioni assunte dal diritto all'immagine. Si pensi al *right to privacy*, al *right to be forgotten*, al *revenge porn* che impegnano la dottrina sull'essenza ultima di tali diritti, nonché sulla loro natura.

(3) Il ritrattato, in verità, è tutelato anche laddove non si riscontri violazione della riservatezza. Sul punto, Scognamiglio, *Il diritto alla utilizzazione economica del nome e dell'immagine delle persone celebri*, in *Dir. inf.*, 1988, 28.

(4) Affermazione non condivisa da prevalente dottrina secondo cui è possibile discorrere solo del profilo negativo, Mezzasoma, *Il diritto all'immagine fra Codice civile e Costituzione*, su *Revista Internacional de Doctrina y Jurisprudencia*, 2012, 13.

(5) Trib. Roma, 25 febbraio 1956, su *Foro it.*, 1956, spec. 1384, con nota di De Cupis, *Tutela giuridica contro le alterazioni della verità personale*. Concordemente, Schermi, *Considerazioni sulla tutela della riservatezza*, su *Giust. civ.*, 1958, 1811.

Al centro, la condivisibile ragione che riposa nella forza comunicativa proveniente dalla sola immagine che, senza alcun passaggio mediato, è in grado di generare quel convincimento pre-razionale nel terzo, difficilmente modificabile in prosieguo. Quanto basta, dunque, per considerare l'immagine un bene giuridico a carattere immateriale (6). L'inarrestabile evoluzione giurisprudenziale, di cui l'ordinanza oggetto di analisi dà conto, altro non è se non il frutto di una condivisibile integrazione tra fonti normative diverse che si è spinta ben oltre la disciplina codicistica (art. 10 c.c.) (7) e la legge sul diritto d'autore (artt. 96 e 97 L. 633 del 1941). Da ultimo, infatti, è sembrato obbligato un coinvolgimento, peraltro debitamente giustificato da un legame più che funzionale con la tutela del diritto all'immagine, sia del D.Lgs. 30 giugno 2003 n. 196 (di poi sostituito dal D.Lgs. 10 agosto 2018, n. 10) sia, in casi specifici, di ulteriori fonti secondarie come il codice deontologico dei giornalisti.
Tale essenziale dialogo tra fonti del diritto diventa indispensabile per valutare, in concreto, la sussistenza di presupposti tesi a consentire la pubblicazione del ritratto di un soggetto ovvero a negarla in presenza di condizioni specifiche. Peraltro, si tenga in debita considerazione come il corretto richiamo effettuato non permetta di chiarire se il legame tra le normative in questione sia caratterizzato da una relazione di norma generale rispetto a norma speciale o di eccezione a regola. La distinzione tra una norma speciale ed una eccezionale, infatti, non deriva dalla struttura della disposizione – che in entrambi i casi si distingue per determinati aspetti – ma si fonda sull'effetto prodotto: nell'ambito di una norma eccezionale tale effetto si oppone a quello previsto dalla norma generale; per una norma speciale, invece, l'effetto differisce da quello di una norma generale ma rimane in linea con la sua logica. Pertanto, è necessario valutare se, per quanto concerne l'uso dei segni evocativi dell'immagine personale, gli effetti giuridici delineati dal Codice della *privacy* siano semplicemente diversi o completamente incompatibili con quelli delineati dalla legge sui diritti d'autore.
In buona sostanza, si fuoriesce dall'orbita di un bieco assolutismo fatto di divieto e deroga per aprire le porte ad una valutazione molto penetrante che combini le varie prospettazioni offerte dai diversi contesti normativi col fine ultimo di stabilirne, volta per volta, la singola prevalenza (8).
Il concetto di trattamento dei dati personali, che rientra nell'ambito di applicazione del Codice della *privacy* (secondo la precedente formulazione), non si contrappone alle pratiche di mostrare, duplicare o vendere elementi che richiamano l'immagine personale. Al contrario, sembra che la gestione delle informazioni presenti nelle immagini rappresenti una forma di trattamento. Se l'operazione di selezione, utilizzo, divulgazione, o diffusione di dati personali rappresentati in forma iconica – o la realizzazione di altre azioni riguardanti tali dati – si accorda con l'esposizione, la riproduzione e la vendita di tali segni, allora l'obbligo di non elaborare i dati personali si allinea alla logica sottostante alle norme del diritto d'autore.
Di conseguenza, si può sostenere che le norme riguardanti l'immagine personale stabilite dalla legge sui diritti d'autore hanno un carattere più generale rispetto a quelle analoghe relative alla riservatezza e che, a causa di questa natura generale, esse trovano applicazione in tutti i casi in cui il trattamento di dati personali, inclusi in elementi che evocano l'immagine, non rientrino nell'ambito di applicazione delle norme in tema di *privacy*.
Finché i dati personali non sono diffusi tra il pubblico o comunicati in modo sistematico a determinati soggetti, la riproduzione, l'esposizione e la vendita degli elementi che li includono sono regolate dagli artt. 96 ss. della legge sui diritti d'autore concernenti i "*diritti sul ritratto*".
L'esigenza di tutela del diritto all'immagine, quale manifestazione di quello alla riservatezza ed il controllo sulla circolazione dei dati personali, hanno indotto, dunque, il legislatore a prevedere rimedi preventivi prima che risarcitori (9).
Per quanto sin qui detto, in presenza di una violazione del diritto di non vedere la propria immagine riprodotta o riprodotta in modo errato con pubblica diffusione, secondo quanto disposto dall'art. 10 c.c., saranno operativi tanto il Regolamento Generale sulla Protezione dei Dati, quanto la legge sui diritti d'autore. Quest'ultima, in particolare, identifica specifiche condizioni (come la fama della persona ritratta, il suo ruolo pubblico, le esigenze legali o di sicurezza, i fini scientifici, educativi o culturali, oltre agli eventi di interesse pubblico o svoltisi pubblicamente) che esonerano dall'obbligo di non divulgare, riprodurre o vendere l'immagine di una persona senza il suo consenso. Per converso, le norme

(6) Secondo qualcuno un diritto a carattere patrimoniale, Metafora, *Il mito di Narciso e la giurisprudenza*, in *Riv. crit. priv.*, 1990, 868 ss.

(7) Ferrara, *Il diritto sulla propria immagine nel nuovo Codice civile e nella nuova legge sul diritto d'autore*, Roma, 1942, 7. Sull'inquadramento civilistico del diritto all'immagine, Amar, *Dei diritti degli autori delle opere dell'ingegno*, Torino, 1874, 366; Allara, *Le nozioni fondamentali del diritto civile*, Torino, 1949, 161.

(8) Navarretta, *Bilanciamento di interessi costituzionali e regole civilistiche*, in *Riv. crit. dir. priv.*, 1998, 625.

(9) Thiene, *L'immagine fra tutela risarcitoria e tutela restitutoria*, in *Nuova giur. civ. comm.*, 2011, II, 356.

ricavate dal GDPR delineano un quadro più ampio per l'autorizzazione al trattamento dei dati personali legati all'immagine di un individuo per il quale, astrattamente, non basta il consenso dell'interessato, la sua notorietà o il fatto che ricopra un incarico pubblico.
La Suprema Corte coglie occasione, dunque, per una rapida scorsa dei momenti fondamentali della disciplina alla luce della elaborazione giurisprudenziale. Da una parte, la legge protegge il diritto dell'individuo ad evitare la divulgazione o l'esposizione pubblica della propria immagine instaurando un obbligo generale di non divulgazione (*erga omnes*) per tutti i cittadini, dall'altra, salvaguarda il diritto dell'individuo ad essere visibile pubblicamente secondo il proprio interesse, creando un generale obbligo di tolleranza (10).
In termini di diritto positivo, l'ampio riconoscimento sociale del diritto di una persona di apparire pubblicamente ha portato alla valutazione della tutelabilità dell'interesse economico nell'uso commerciale della propria immagine (11), gettando le basi per l'emergere di contratti di sponsorizzazione atipici e per il riconoscimento del danno economico legato alla perdita di compensi per l'uso dell'immagine a scopi pubblicitari, introducendo, così, nel nostro sistema giuridico, il concetto del diritto alla pubblicità di origine americana.
Diversamente, nel contesto della diffusione televisiva di immagini riprese segretamente, è stato chiarito che le condizioni che legittimano il diritto di cronaca non giustificano, automaticamente, la legittimità della pubblicazione delle immagini delle persone coinvolte che deve rispettare specifici canoni, nonché l'interesse pubblico alla conoscenza dell'evento. Ad esempio, nell'ambito del giornalismo, la pubblicazione di fotografie di persone detenute è considerata legittima solo se rispetta determinate condizioni, come l'essenzialità dell'immagine per illustrare la notizia e le cautele speciali a protezione dell'individuo ritratto, con una valutazione rigorosa della necessità della pubblicazione dell'immagine rispetto alla semplice divulgazione della notizia.

Il cammino giurisprudenziale, verso un'interpretazione più ampia e protettiva di tale diritto, dunque, ha portato ad una maggiore considerazione della *privacy* individuale nel bilanciamento con l'interesse pubblico alla divulgazione delle immagini, soprattutto in casi che non pregiudicano l'onore, il decoro o la reputazione, e ha acquisito particolare rilevanza nel caso di minori, dove la legge prevede limitazioni specifiche alla riproduzione delle loro immagini.
Più in dettaglio, l'art. 97 l. dir. aut. individua diverse condizioni in presenza delle quali è consentita la pubblicazione di immagini senza il consenso dell'individuo ritratto. La pubblicazione, infatti, è permessa a motivo di un interesse pubblico legato all'identità della persona (come la celebrità o il ruolo pubblico ricoperto) ovvero in quelle situazioni in cui prevale l'interesse pubblicistico della diffusione (ad esempio, per esigenze giudiziarie o di polizia, o per fini scientifici, educativi o culturali); infine, vengono ricompresi i casi in cui la pubblicazione è giustificata da specifiche circostanze di tempo e di luogo che generano, di per sé, un interesse pubblico alla diffusione.
Il Supremo Consesso, tuttavia, tiene a rimarcare il fattore più rilevante di cui si deve tener conto nello scrutinio del caso concreto: non è sufficiente identificare una di queste condizioni per giustificare la pubblicazione, in quanto occorre valutare, caso per caso, se essa sia effettivamente lecita.

## 3. Il consenso quale primo limite alla divulgazione

La concessione da parte di un individuo del permesso di pubblicare il proprio ritratto è atto negoziale, che può essere manifestato anche attraverso una dichiarazione unilaterale. Ciò vale anche nel caso in cui tale permesso venga concesso dopo una pubblicazione non autorizzata al fine di legittimarla (12). Esiste un dibattito sul se e come questo consenso, che può essere fornito gratuitamente o a pagamento (come indicato negli articoli 17, 96, 97 e 98 della legge sui diritti d'autore), possa essere integrato in un accordo contrattuale (13), nonché sulla possibilità, per la persona ritratta, di revocare tale

(10) Vercellone, *Il diritto sul proprio ritratto*, Torino, 1953, 8 ss.; Scalisi, *Il diritto alla riservatezza,* in *Il diritto privato oggi*, a cura di Cendon, Milano, 2002, 41 ss.; Sirena, *La tutela inibitoria e cautelare del diritto all'immagine*, in *Riv. critica dir. priv.*, 1996, 334; De Vita, *sub art. 10 c.c.*, in *Comm. cod. civ.* a cura di Scialoja - Branca - Galgano, *Delle persone Fisiche*, *artt. 1-10*, Bologna-Roma, 1988, 570; Bavetta, *Immagine (diritto alla)*, in *Enc. dir.*, XX, Milano, 1970, 145, 148 ss.; De Cupis, *I diritti della personalità*, in *Tratt. Dir. civ. e comm.*, Cicu-Messineo, IV, t. 1, Milano, 1973, 273; Ansalone, *Il diritto all'immagine*, in *Nuova giur. comm.*, 1990, II, 235 ss.; Albertini, *L'abusivo sfruttamento (in particolare come marchio) del nome e dell'immagine altrui*, in *Giust. civ.*, 1997, II, 494 ss.; Alpa - Resta, *Le persone fisiche e i diritti della personalità*, in *Tratt. Sacco*, I, *Le persone e la famiglia*, Torino, 2006, 534 ss.

(11) Il cd. "*right of publicity*" di matrice anglosassone che attribuisce il diritto esclusivo di sfruttare commercialmente l'immagine di una persona.

(12) Zeno Zencovich, *Profili negoziali degli attributi della personalità*, in *Dir. inf. e inform.*, 1993, 553 ss.

(13) Sulla indisponibilità ed intrasmissibilità del diritto all'immagine quale diritto della personalità si veda De Cupis, *I diritti della personalità*, cit., 85 ss.; Galgano, *Diritto civile e commerciale*, Padova, 2004, I, 181; Di Nicola, *L'atto di disposizione del diritto all'immagine ha, dunque, natura non patrimoniale*, in *Cont. Imp.*, 2005, 463 ss. In senso contrario, Vercellone, *Il diritto sul proprio ritratto*, cit., 112 ss.; Zeno Zencovich, *Profili negoziali degli attributi della personalità*, cit., 549; Albertini, *L'abusivo sfruttamento (in particolare come marchio) del nome e dell'immagine altrui*, cit., 499; Alpa - Resta, *Le persone fisiche e i diritti della personalità*, cit., 631; nonché Cass. civ., 10 novembre 1979, n. 5790, in *Giust. civ.*, 1980, I, 1377.

consenso in ogni momento. Le posizioni finora assunte concentrano il fuoco su due fondamentali concetti.
La prima interpretazione, supportata da diverse decisioni della Corte di Cassazione (14), vede il consenso come un atto relativo non tanto al diritto all'immagine in sé, ma al proprio utilizzo. Anche se questo consenso viene inserito in un contratto, è considerato distinto ed indipendente da questo e, quindi, revocabile in qualsiasi momento dal soggetto ritrattato, anche se è stato pagato un corrispettivo. In questo scenario, se la revoca risulta essere un abuso del diritto della personalità, si ritiene che la persona ritrattata debba versare un indennizzo a chi aveva ottenuto, originariamente, il permesso di diffondere l'immagine.
Il secondo approccio, sostenuto da sentenze più datate della Cassazione e da parte della dottrina (15), accoglie la concezione di un diritto all'immagine, almeno sotto il profilo del suo esercizio, che possa costituire oggetto di contratti validi. Secondo tale impostazione, si applicherebbero le regole generali del codice civile sul recesso contrattuale, escludendo, dunque, la possibilità di revoca del consenso da parte della persona ritrattata a piacimento.
Per quanto riguarda la forma ed il contenuto del consenso, né il codice civile né la legge sui diritti d'autore forniscono indicazioni specifiche, lasciando agli interpreti il compito di definire le norme applicabili. Tuttavia, l'art. 23, comma 3, del decreto legislativo n. 196/2003, nella propria formulazione ante Regolamento (16), stabiliva che il consenso al trattamento dei dati personali, ivi compresa l'immagine, dovesse assumere la forma espressa senza che, come sostenuto da giudici di merito, potesse ammettersi una manifestazione di volontà tacita od implicita (17).
Si aggiunga che allorquando un individuo conceda il permesso alla pubblicazione del proprio ritratto, normalmente, ne definisce anche i limiti ed eventuali restrizioni. Oltrepassare tali limiti rende, parimenti, la diffusione dell'immagine illegittima.
In realtà, l'art. 6 del Regolamento Generale sulla Protezione dei Dati (GDPR) stabilisce che il consenso al trattamento dei dati personali deve essere specifico per il tipo di trattamento previsto. Questo implica che, nell'autorizzare la pubblicazione del proprio ritratto, una persona non solo può, ma deve definire i confini entro cui la pubblicazione è consentita (18).
La dichiarazione con cui si rinuncia al diritto all'immagine o si cede in modo illimitato, ponendo in essere una volontà di fatto abdicativa verso tale diritto, è considerata nulla alla stregua di un atto di rinuncia alla propria libertà personale. Questa interpretazione è conseguenza di quanto previsto dagli artt. 1343 e 1346 c.c. che invalidano i contratti con causa o oggetto contrari all'ordine pubblico, estendendo tale patologia anche agli atti unilaterali.
Un consenso prestato, dunque, che non specifichi l'ambito di diffusione dell'immagine, potrebbe, nondimeno, essere considerato non validamente formato; tuttavia, va precisato come i limiti di tale consenso possano essere determinati interpretativamente, basandosi sull'uso prevedibile al momento del consenso. Se questa analisi non riesce a definire chiaramente i confini di legittima diffusione, il consenso è nullo per indeterminatezza dell'oggetto, secondo quanto disposto dall'art. 1346 c.c.
Concedendo l'autorizzazione per la presentazione, la duplicazione, la distribuzione (secondo l'art. 96 della legge sui diritti d'autore) e, in termini più ampi, per la gestione dei segni che richiamano la propria immagine (art. 23 del codice sulla privacy), ogni persona disegna, quindi, i confini della propria *privacy*. L'interesse protetto è strettamente legato all'individuo che ne detiene il governo e si manifesta attraverso un diritto che, per sua natura, non può essere ceduto – quindi può essere trasferito solo se espressamente consentito dalla legge – dato che la sua protezione richiede un continuo adeguamento alle decisioni variabili dell'individuo a cui è attribuito. D'altra parte, considerando l'interesse pubblico (19), in certe circostanze il legislatore può decidere, in modo eccezionale, di ridurre o addirittura eliminare il livello di *privacy* che la persona ritratta è in grado di mantenere riservato, comprimendo l'estensione del diritto alla riservatezza e permettendo che l'immagine

(14) Cass. civ., 19 novembre 2008, n. 27506, in *Giust. civ.*, 2009, 2, 313 ss.; Cass. civ.,17 febbraio 2004, n. 3014, in *Dir. giust.*, 2004, 107 ss.

(15) Cass. civ., 29 maggio 2009, n. 12801, in *Resp. civ. e prev.*, 2007, 3, 554 ss.; Cass. civ., 21 maggio 1998, n. 5086, in *Dir. inf. e inform.*, 1998, 227 ss.; Cass. civ., 11 ottobre 1997, n. 9880, in *Dir. inf. e inform.*, 1998, 279; Cass. civ., 16 aprile 1991, n. 4031, in *Giur. it.*, 1991, 976 ss.

(16) Il contenuto dell'art. 23, comma 3, del decreto legislativo n. 196/2003, che riguardava le condizioni per il consenso al trattamento dei dati personali, è stato sostituito nel contesto dell'adeguamento della normativa italiana al Regolamento (UE) 2016/679 (GDPR) con il Decreto Legislativo 10 agosto 2018, n. 101. Il decreto ha introdotto importanti novità per allineare la legislazione italiana alle disposizioni del GDPR, che stabilisce norme dettagliate sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati.

(17) Sulla necessità del consenso alla diffusione dell'immagine quale dato sensibile, MONTALDO, *Il ritratto fotografico digitale tra diritto d'autore, diritti della persona e tutela della privacy*, su *Resp. civ. prev.*, 2010, 2369.

(18) Trib. Roma, 12 marzo 2004, in *Danno e resp.*, 2005, 879 ss., con nota di TASSONE, *Diritto all'immagine fra uso non autorizzato del ritratto e lesione della privacy*, 2005, 885 ss.

(19) FERRI, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, 1990, I, 801 ss. L'Autore evidenzia come la compressione del diritto alla riservatezza sia il frutto della prevalenza di un corrispondente interesse collettivo.

possa essere utilizzata senza il consenso dell'individuo raffigurato attraverso la valorizzazione di limiti oggettivi e soggettivi.
I limiti oggettivi riguardano la scelta delle modalità e dei contesti specifici in cui l'immagine può essere divulgata, includendo considerazioni sia quantitative (ad esempio, il tempo e il luogo della diffusione) che qualitative (il mezzo, lo scopo o la modalità specifica di diffusione).
I limiti soggettivi, invece, attribuiscono il potere divulgativo a soggetti specifici con esclusione di tutti gli altri, con ciò evidenziando l'importanza dell'identità del divulgatore nella tutela del diritto all'immagine.
Nel caso che ci occupa, l'assenza di consenso da parte degli esercenti la potestà genitoriale sul minore (20), così come ritualmente evidenziata nell'atto introduttivo, impone, quindi, una verifica sull'esistenza di presupposti legittimanti la divulgazione al di fuori della esplicita manifestazione di volontà dell'avente diritto (21). Non v'è dubbio, infatti, che non solo si versi in una ipotesi di assenza di preventivo consenso espresso ma di assoluta impossibilità di ricavare tale manifestazione di volontà da condotta concludente avente genesi nella sequela degli accadimenti.
Più nello specifico, la ripresa televisiva o fotografica dei minori costituisce un aspetto puntuale su cui l'ordinamento ha concentrato la propria attenzione. L'esigenza di protezione della dignità del minore, infatti, trova risposta nel Codice in materia di protezione dei dati personali (così come sostituito dal Regolamento Generale sulla Protezione dei Dati, applicabile dal 25 maggio 2018), nonché nella Convenzione sui diritti dell'infanzia e dell'adolescenza ratificata in Italia con la legge 27 maggio 1991, n. 176, peraltro invocata dal ricorrente (22).

Anche se la Convenzione non tratta specificamente la protezione dei dati personali, i principi in essa contenuti si applicano indirettamente attraverso l'obbligo degli Stati di adottare tutte le più adeguate misure legislative e amministrative per proteggere i diritti dei bambini.
La sinergia tra il Regolamento e la Convenzione crea un quadro robusto per la tutela dei minori, imponendo ai responsabili del trattamento dei dati e ai fornitori di servizi la responsabilità di adottare misure appropriate per proteggere la *privacy* e i dati personali dei minori, garantendo, così, il loro benessere e sviluppo in un ambiente sicuro.
Per quanto concerne il consenso nel trattamento dei dati personali dei minori, l'Italia ha fatto uso della facoltà concessa dall'art. 8 del GDPR di stabilire un'età inferiore ai 16 anni per il consenso fornito direttamente dai minori nell'ambito dei servizi offerti da società di informazione. L'età stabilita dall'ordinamento italiano per fornire validamente il consenso al trattamento dei dati personali, senza il bisogno del consenso dei genitori o dei tutori legali, è di 14 anni. Pertanto, per i minori di età inferiore a 14 anni, è necessario ottenere il consenso dai titolari della responsabilità genitoriale per poter trattare legalmente i loro dati personali in relazione ai servizi offerti direttamente al minore, come i social media, le *app* e altri servizi *on-line* (23).
*Il Garante per la Protezione dei Dati Personali, quale autorità di controllo, ha anche emesso linee guida e chiarimenti su come le organizzazioni dovrebbero gestire il consenso per il trattamento dei dati dei minori, nonché su come dovrebbero essere implementate adeguatamente misure per verificare l'età e il consenso dei genitori in maniera efficace. Anche l'Autorità per le Garanzie nelle Comunicazioni* (AGCOM) *ha emanato il "Testo unico dei servizi di media audiovisivi e radiofonici"* che, tra l'altro, stabilisce linee guida per la partecipazione dei minori a programmi televisivi e radiofonici, mirando a proteggere la loro immagine e dignità (24).

(20) Per Cass. civ., 25 novembre 2021, n. 36754, in *Resp. civ. e prev.*, 2022, 1217 "*in mancanza di un esplicito consenso, costituiscono violazione del diritto all'immagine le riprese effettuate in pubblico, per fini commerciali*".

(21) Cass. civ., ord., 19 febbraio 2021, n. 4477, in *Studium juris*, 2021, 9, 1100, con nota di Zanovello. Spetta al rappresentante legale del minore o della persona comunque incapace di agire, nel rispetto dei limiti posti dalle comuni norme in materia, di dare il consenso alla diffusione dell'immagine del soggetto sottoposto a tutela, purché ciò determini una qualche utilità per l'incapace e, in ogni caso, senza pregiudizio per il medesimo.

(22) La Convenzione sui diritti dell'infanzia e dell'adolescenza, meglio conosciuta come la Convenzione sui Diritti del Fanciullo (CRC), è un trattato internazionale adottato dalle Nazioni Unite il 20 novembre 1989. L'Italia ha ratificato la Convenzione con la legge 27 maggio 1991, n. 176, impegnandosi, così, a rispettare i diritti ivi sanciti e a garantire la loro applicazione all'interno del proprio ordinamento giuridico.
La Convenzione rappresenta il primo trattato internazionale che riconosce i bambini come portatori di diritti propri, indipendentemente da quelli dei loro genitori o tutori. Essa stabilisce una serie di diritti universali per tutti i bambini e gli adolescenti (persone di età inferiore ai 18 anni), tra cui il diritto alla vita, alla salute, all'istruzione, al gioco, alla protezione dalla violenza e dall'abuso, e il diritto di esprimere la propria opinione e di essere ascoltati in tutte le questioni che li riguardano. Vie-ne, in particolare, valorizzato l'interesse superiore del bambino (articolo 3) onde per cui ogni decisione concernente il bambino deve considerare tale profilo. La ratifica della Convenzione implica l'obbligo per gli Stati Parti di adottare tutte le misure legislative, amministrative e giudiziarie necessarie per darvi effettiva attuazione. Inoltre, gli Stati devono presentare periodicamente rapporti al Comitato sui diritti del fanciullo delle Nazioni Unite, un organo di esperti incaricato di monitorare l'attuazione della Convenzione. La legge italiana n. 176/1991, ratificando la Convenzione, ha introdotto nell'ordinamento giuridico nazionale i principi e le disposizioni in essa contenuti, impegnando l'Italia a garantire e tutelare i diritti dell'infanzia e dell'adolescenza in conformità agli standard internazionali.

(23) In questa ***Rivista***, Trib. civ. Bari, ord. 7 novembre 2019, con nota di Maggi, *Consenso e tutela del diritto all'immagine del minore: tra diritto della personalità e protezione dei dati personali*, 87 s.

(24) Il "*Testo unico dei servizi di media audiovisivi e radiofonici*" è conosciuto come il Testo Unico dei Servizi di Media Audiovisivi e Radiofonici (TUSMAR), ed è stato introdotto per regolamentare in maniera organica i

Ordunque, non esiste una singola specifica disposizione normativa che vieti, categoricamente, la ripresa di minori, bensì diverse previsioni in diversi contesti legislativi che impongono limitazioni e condizioni al fine di tutelare la *privacy* e l'integrità psicofisica dei minori. L'utilizzo di immagini o video raffiguranti soggetti minori deve essere preceduto dal consenso informato dei genitori o dei tutori legali e deve essere gestito in modo da rispettare i diritti del minore. Tanto, non è avvenuto nel caso di specie. L'assenza di un consenso validamente prestato, quindi, apre le porte alla verifica sulla sussistenza di ipotesi derogatorie.

## 4. L'equilibrio tra attività giornalistica, diritto di cronaca e tutela dell'immagine

Non v'è dubbio sul fatto che il ricorrente, nel caso in esame, abbia ricondotto nell'alveo dell'art. 10 c.c. e degli artt. 96 e 97 l. dir. aut. la domanda di tutela rassegnata nel proprio atto introduttivo. Tuttavia, anche sulla scorta di quanto osservato in precedenza in merito alla interoperabilità delle fonti, non v'è, parimenti, dubbio sul fatto che il tema del trattamento dei dati personali non possa essere emarginato sullo sfondo. Tanto più che, gravitando, il giudizio *de quo,* intorno all'orbita della delicata materia della deontologia giornalistica e del suo connubio col diritto alla riservatezza, non può non sentirsi forte il richiamo della disciplina del trattamento dei dati personali.

Ricordando che oggetto di giudizio è il caso del minore ripreso nel corso di un servizio televisivo raffigurante l'arresto di un latitante (25), appare opportuna qualche considerazione. Al centro della disputa si colloca la valutazione esperita dai genitori del minore che conclude per un servizio televisivo finalizzato, non solo alla rappresentazione visiva dell'arresto di un latitante, bensì alla veicolazione della notizia di un contesto sociale ambiguo ed opaco tale da rendere l'informazione screditante se non, addirittura, infamante.

Tale premessa stimola, nell'immediato, una prima riflessione. Il quadro fattuale, infatti, costituisce, in astratto, presupposto vuoi per un indebito utilizzo dell'immagine scaturente da atto illecito non giustificabile, vuoi, sempre in forma astratta, una lesione della reputazione provocata da attività legittima. Due alternative, quindi, potenzialmente riscontrabili. In concreto, però, la valutazione del giudice del merito, non scalfita dal giudizio di legittimità (per motivazioni che di qui a poco si esamineranno), condivide l'assunto difensivo di parte convenuta che ripara il servizio giornalistico sotto l'ombrello protettivo dell'attività informativa (*rectius* di cronaca) concernente un fatto caratterizzato da spiccato interesse pubblico. Tale argomentazione, quanto ai fini dell'operatività del combinato disposto di cui agli artt. 10 c.c. e 96 e 97 l. dir. aut., porta a ritenere come ci si trovi al cospetto di una condotta che, sebbene per diversi aspetti potenzialmente idonea ad arrecare nocumento alla reputazione del minore, non appare, nello specifico, affetta da capacità diffamatoria (26), destinata, in ogni caso, a rimanere assorbita dal legittimo esercizio del diritto di cronaca. L'operazione di *balance,* dunque, obbligatoria per una compiuta qualificazione giuridica, consente il prevalere, nel caso in questione, del diritto all'informazione.

Una lettura attenta, inoltre, mette in luce come la notizia dell'arresto del latitante, non abbia, di fatto, travalicato i confini della essenzialità (con ogni più ovvia conseguenza per l'opponibilità del diritto di cronaca) (27) a poco valendo che, nell'economia generale della ripresa televisiva, l'inquadratura abbia immortalato varie persone presenti sul luogo dell'arresto tra le quali il minore. Nondimeno, non muta il quadro fenomenico il fatto che la contestata condotta lesiva non trovi giustificazione alcuna in una posizione attiva del danneggiante che, sotto tale aspetto, resta privo di un interesse meritevole di tutela da opporre al soggetto leso. Si aggiunga, inoltre, che la lamentata polarizzazione dell'attenzione del servizio sulla figura del minore non può essere ricavata, quasi mediante sovrapposizione, dalla ulteriore denun-

servizi di media audiovisivi e la radiodiffusione in Italia, in linea con le direttive europee, in particolare la Direttiva 2010/13/UE del Parlamento Europeo e del Consiglio del 10 marzo 2010, conosciuta come Direttiva sui servizi di media audiovisivi (*SMAV o AVMSD - Audiovisual Media Services Directive*).

(25) Sui limiti del diritto di cronaca, sulla essenzialità della notizia e sulla possibilità di ritrarre un soggetto in stato di arresto, si veda il provvedimento del Garante della *privacy* (25 febbraio 2021) e la giurisprudenza (Cass. civ., 18 marzo 2008, n. 7261 in *Giust. civ.*, 2008, 7-8, I, 1664). L'enfatizzazione dell'immagine di un soggetto ristretto nella propria libertà costituisce potenziale lesione della dignità della persona anche in ragione della capacità comunicativa dello strumento visivo capace di una diffusione decontestualizzata e insuscettibile di controllo da parte della persona ritratta.

(26) Nell'ipotesi in esame non pare versarsi nemmeno in una di quelle ipotesi di giornalismo contestate per metodo.

(27) Per quanto riguarda la libertà di espressione e il diritto di cronaca, l'art. 85 del GDPR, prevede che gli Stati membri debbano conciliare la protezione dei dati personali con il diritto alla libertà d'espressione e d'informazione, incluso il trattamento a scopi giornalistici. Ciò implica che in determinate circostanze possano essere applicate esenzioni o deroghe alle norme sulla protezione dei dati, a condizione che siano necessarie per conciliare il diritto alla vita privata con le norme sulla libertà di espressione. Il "*limite dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico*" era espressamente previsto dall'art. 137, comma 3, del Codice della Privacy" (cioè il divieto di "divulgare dati, immagini e dettagli non strettamente necessari per dare conto di fatti di cronaca e vicende giudiziarie", Garante Privacy, 10 ottobre 2002), principio confermato dalle norme deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica, pubblicate ai sensi dell'art. 20, comma 4, del decreto legislativo 10 agosto 2018, n. 101. Si veda Sica, *Danno morale per lesione della privacy: domicilio ed essenzialità della notizia*, in *Dir. inf.*, 2000, 371 ss.

ciata finalità del servizio televisivo consistente nel mostrare all'opinione pubblica un contesto sociale contiguo al latitante o di favore per quest'ultimo.
Le due affermazioni, infatti, non legano e l'esistenza dell'una non prova automaticamente l'altra. In buona sostanza, si tratta di comprendere, alla luce dei criteri offerti dal dato positivo, se l'interesse leso possa considerarsi prevalente rispetto a quello del danneggiante, in guisa tale da qualificare come risarcibile l'eventuale consequenziale danno.
In verità, non sembra fuor di luogo, per il caso esaminato, un richiamo al cd. concetto di "ritratto collettivo" dal momento che ad essere oggetto di divulgazione è l'immagine ritraente una pluralità di soggetti (non solo del minore) quale somma di ritratti individuali. Ordunque, anche laddove possa ritenersi soddisfatto l'ineliminabile requisito della riconoscibilità del ritrattato (28), è comunque necessario valutare se l'immagine della moltitudine di individui, tra cui il minore, possa costituire uno sfondo inevitabile e, per l'effetto, casuale in modo tale da essere percepito come elemento meramente accidentale nell'economia globale dell'integrale servizio giornalistico. Sul punto, pare che il primo Giudice si sia rifatto all'interpretazione secondo cui debba considerarsi giustificata la diffusione del ritratto allorquando la notorietà (non voluta dal soggetto ripreso) sia – come conseguenza di un evento specifico – interamente coperta dal pubblico interesse conoscitivo (29). Quanto detto, nella misura in cui risulti effettivamente possibile un collegamento oggettivo tra l'evento che genera notorietà del soggetto ripreso ed il soggetto medesimo come accaduto nel caso di specie, in cui l'inquadratura del minore presente sui luoghi diviene ineliminabile cornice dell'evento fondamentale costituito dall'arresto del latitante che resta il nucleo della notizia.
Secondo la prospettazione spiegata nell'atto di impugnazione, peraltro, l'autore del servizio giornalistico, da un lato, avrebbe opposto la mera casualità della ripresa del minore, giudicata inevitabile a fronte della presenza del medesimo sui luoghi, dall'altro, avrebbe tentato di immunizzare, attraverso il diritto di cronaca, il servizio televisivo finalizzato, tra l'altro, ad evidenziare lo scarso senso civico dei concittadini dell'arrestato, dediti, per lo più, a dare conforto e saluto a quest'ultimo.
Su tale aspetto, appare necessario, in primo luogo, evidenziare come i fatti posti a base di un giudizio vanno qualificati nella loro oggettività e non per il senso che una delle parti intenda attribuirgli. In secondo luogo, sul piano squisitamente processuale, non può non evidenziarsi come il motivo di censura, per come articolato, sembri stigmatizzare più la contraddittorietà della difesa di controparte che un vizio di motivazione. Di qui, un ulteriore ragione di condivisione dell'ordinanza in commento.
Tuttavia, e questo potrebbe apparentemente sembrare paradossale, la Corte, sebbene concluda per un giudizio di complessiva inammissibilità del ricorso (ovviamente per ragioni processuali che esonerano da qualsivoglia più penetrante valutazione) non pare dar torto, in linea di principio, ai rilievi del ricorrente. Ed infatti, l'ordinanza esaminata scolpisce nella pietra il principio, non nuovo, secondo cui "*anche quando non ricorra il caso limite della lesione del decoro, della reputazione o dell'onore della persona di cui all'art. 97, secondo comma, della legge n. 633 del 1941 e si integri, al contrario, in astratto, una delle fattispecie (in particolare il collegamento con un evento di interesse pubblico o comunque svoltosi in pubblico) indicate dal primo comma della detta disposizione, può nondimeno escludersi che operi, in concreto, la deroga legale al divieto di riproduzione dell'immagine prevista dalla stessa norma, allorché alla circostanza soggettiva della minore età della persona si accompagni quella, oggettiva, della non casualità della ripresa, espressamente diretta a polarizzare l'attenzione sull'identità del minore e sulla sua riconoscibilità*".
Tra l'altro, il Supremo consesso già aveva avuto modo di valorizzare quel canone a tenor del quale "*non ogni vicenda che coinvolga un personaggio noto (nella specie un calciatore) giustifica la conclusione della legittimità, in ogni caso, della diffusione di immagini anche di soggetti terzi che con questi vengano in contatto ove ne manchi una specifica necessità (...). Si tratta di fattispecie nelle quali la riproduzione e la diffusione del ritratto sono ritenute lecite, anche in assenza del consenso dell'effigiato, se ed in quanto miranti a soddisfare soprattutto esigenze pubbliche e sociali tali da giustificare il sacrificio del singolo in funzione del preminente interesse del singolo individuo di fronte ad esigenze della collettività, tale sacrificio non deve estendersi otre i limiti idonei a soddisfare queste esigenze*".
In altri termini, si legittima la pubblicazione dell'immagine in ragione di fattuali "*circostanze in presenza delle quali il soggetto si è fatto ritrarre*". Tale approccio non può non essere che fondato sulla scelta di graduare l'esercizio del diritto di cronaca e tanto sull'ulteriore presupposto che l'interesse generale alla conoscenza di una notizia non presuppone *ex se* l'interesse a conoscere il contesto nel quale quella notizia si è sviluppata, ivi comprese le fattezze della persona.
Orbene, il Giudice di legittimità conferma l'orientamento già assunto in precedenza, ricordando che per considerare illegittima la riproduzione dell'immagine di una persona non è indispensabile l'effetto di una lesione alla reputazione ovvero all'onore allorquando siano

(28) Che non coincide con l'identificabilità del soggetto, D'URSO, *Tutelabilità dell'immagine e limiti della tutela inibitoria* in *Riv. trim. dir. proc. civ.*, 1979, 391.

(29) In merito alle caratteristiche dell'evento, DE CUPIS, *I diritti della personalità*, cit., 307.

compresenti l'elemento della minore età e la non casualità della ripresa. Tuttavia, ricorda sempre il Supremo Giudice, una diversa valutazione in tal senso avrebbe importato un giudizio sul fatto da sovrapporsi a quello del giudice di merito e per forza di cose teso ad un diverso apprezzamento del materiale probatorio non praticabile in sede di legittimità. La decisione che si annota, tra l'altro, costituisce spunto per un esame del profilo del danno risarcibile con particolare riferimento alla possibilità che una condotta possa, indipendentemente dal classico danno alla reputazione o all'onore, essere caratterizzata da una carica di lesività propria ed originaria generata dalla presenza di requisiti oggettivi e soggettivi come nel caso in esame.

## 5. L'individuazione del danno non patrimoniale e la difficoltà di una visione unanime

Il principio informatore, dapprima adottato dalla Suprema Corte nell'ordinanza in commento e mutuato quale direttrice per l'elaborazione del presente contributo, impone, in continuità, l'esame incrociato delle diverse fonti per analizzare il tema del danno generato dalla violazione del diritto all'immagine. Secondo la prospettazione del ricorrente, il pregiudizio arrecato al bene immateriale troverebbe fonte nell'abusiva divulgazione dell'immagine del minore accostata a quella di un delinquente, dalla quale sarebbe scaturito un peggioramento reputazionale nel contesto scolastico con ulteriore decremento del rendimento studentesco.

Invero, per quanto sin qui riferito, il danno presunto, in via meramente astratta, potrebbe ricavarsi sia dalla gestione illecita di un dato personale e sensibile (come l'immagine) che quale violazione espressa della disciplina civilistica e del diritto d'autore che tra loro, peraltro, appaiono perfettamente coniugabili. Nello specifico, infatti, il danno non patrimoniale, il cui mancato riconoscimento costituisce specifico motivo di impugnazione, implica, obbligatoriamente, un richiamo normativo agli artt. 82 GDPR e 2059 c.c. alla luce degli approdi delle Sezioni Unite in tema di danno non patrimoniale (30). Le due disposizioni richiamate, nonostante l'eccessiva genericità della prima, non risultano incompatibili col risultato dell'interpretazione giurisprudenziale sfociata nelle cd. sentenze di San Martino (31) che hanno puntellato i profili applicativi dell'art. 2059 c.c., se si pone mente al risultato finale consistente nella valorizzazione dei due fondamentali canoni ermeneutici: inesistenza di un danno intrinsecamente connaturato alla violazione del diritto all'immagine (32) e doppio requisito di gravità dell'illecito e serietà del pregiudizio.

Orbene, il danno all'immagine, costituzionalmente protetto quale diritto della personalità, è senz'altro un danno risarcibile purché esistente ovvero caratterizzato (non solo) da un rapporto di causalità diretta con l'illecito trattamento connotato, a propria volta, da una significativa intensità della violazione foriera di un pregiudizio alieno alla sfera della normale tollerabilità. Conseguenza di ciò è che la violazione di tale diritto, astrattamente inidonea a generare un danno non patrimoniale in *re ipsa* (33) – anche alla luce dei significativi precedenti richiamati – rileva, ai fini risarcitori, solo ove comporti una lesione della reputazione (34).

In verità, come si dirà a breve, l'esistenza di un danno non patrimoniale, diverso dal canonico pregiudizio all'onore o alla reputazione è, da qualcuno, ammessa e costituisce, di fatto, il nodo nevralgico della questione (35). Diversamente, altro orientamento interpreta l'ingiustizia richiesta dall'art. 2043 c.c. come una sorta di contenitore adatto ad ogni stagione e suscettibile di essere colmato, di volta in volta e nel corso dei tempi, con nuove ipotesi di illeciti (36).

(30) Sull'estensione del danno non patrimoniale, Busnelli, *Il "trattamento dei dati personali" nella vicenda dei diritti alla persona: la tutela risarcitoria*, in *Trattamento dei dati e tutela della persona* a cura di Cuffaro - Ricciuto – Zeno-Zencovich, Torino, 1998, 185; Sica, *Art. 18*, in *Commentario alla legge 31 dicembre 1996, n. 675*, a cura di Giannantonio - Losano - Zeno-Zencovich, Padova, 1997, *passim*.

(31) Per un commento a Cass. civ., sez. un., 11 novembre 2008, n. 26972 si vedano Sica, *"In danno di nessuno". Ciò che è vivo e ciò che è morto del danno esistenziale*, in Aa.Vv., *Il danno non patrimoniale. Guida commentata alle decisioni delle S.U., 11 novembre 2008 nn. 27972/3/4/5*, Torino, 2009; Ponzanelli, *Certezze e incertezze nel risarcimento del danno alla persona*, in *Danno e resp.*, 2020, 103 ss. Ancora, Mazzamuto, *Il rapporto tra gli artt. 2059 e 2043 c.c. e le ambiguità delle Sezioni unite a proposito della risarcibilità del danno non patrimoniale*, in *Contr. e impr.*, 2009, 589 ss., 614 s., secondo cui il procedimento inferenziale parte dalla natura dell'interesse leso, dalla intensità della lesione oltre che dalle modalità concrete della condotta.

(32) Tassone, *Danno in re ipsa, cerchi concentrici e funzioni della responsabilità civile*, in *Resp. civ. e prev.*, 2022, 1187 ss.

(33) Cass. civ., ord., 18 novembre 2022, n. 34026, in *Nuova giur. civ. comm.*, 2023, 3, 598, con nota di Mezzanotte - Parisi. La Cassazione ha chiarito due principi fondamentali riguardanti il risarcimento del danno non patrimoniale: primo, sottolinea l'importanza per la parte lesa di provare le conseguenze subite a seguito del danno, evidenziando un ruolo cruciale per le prove presuntive che possono diventare determinanti per il giudizio; secondo, una volta stabilita l'esistenza del danno, l'ammontare del risarcimento viene fissato attraverso la valutazione equitativa del giudice, processo considerato essenziale nella quantificazione del risarcimento. In dottrina, Zeno Zencovich - Sammarco, *La quantificazione del danno alla reputazione; ricognizione su 620 sentenze del Tribunale civile di Roma (2015-2020)*, in *Dir. inf.*, 2021, 663.

(34) Tosi, *Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE*, in *Danno e resp.*, 2020, 433 ss.

(35) Bianca, *La responsabilità*, Milano, 2021, 558 s. e 561. Il danno ingiusto integra il fatto illecito in quanto lesione di un interesse giuridicamente tutelato nella vita di relazione (danno evento) mentre il danno-conseguenza integra l'evento lesivo costituendo una forma di ulteriore aggravamento.

(36) Alpa, *Il problema dell'atipicità dell'illecito*, Napoli, 1979, *passim*.

La Suprema Corte, proprio su tali alternativi filoni di pensiero, ha rimarcato la differenza tra le due concezioni di danno individuandola nella coincidenza, dell'una, con la lesione della sfera giuridica e, dell'altra, con la diminuzione patrimoniale (37). In realtà, pur respingendo la sovrapposizione piena e totale tra violazione e danno, si ammette l'ipotesi, così individuando un punto di accordo tra le contrapposte teorie, di un danno che possa ritenersi presunto in ragione della particolarità dell'evento. Il danno patrimoniale (pur domandato nel caso di specie), invece, è legato alla esistenza di una specifica perdita economica e comporta la necessità del nesso causale da valutarsi, tuttavia, in sede di merito e non di legittimità.

Non può ravvisarsi danno patrimoniale quale effetto di una condotta che, pur non generando una conseguenza pregiudizievole a carattere economico, possa comportare, comunque, un danno diverso dalla classica lesione del diritto alla reputazione ovvero alla onorabilità meritevole di risarcimento (38). Il tema è, quantomai, interessante, alla luce delle ultime tendenze giurisprudenziali nell'ottica di un ampliamento dello spettro dell'illecito trattamento dei dati personali (39).

Orbene, la valutazione del danno non patrimoniale si basa generalmente su giudizi presuntivi relativi, ad esempio, al disagio psicologico subito dall'individuo ritratto, mentre il danno patrimoniale segue un percorso diverso, orientandosi verso il cd. "prezzo del consenso" in assenza di altre specifiche perdite dimostrabili. Non v'è dubbio sul fatto che l'individuazione del danno non patrimoniale e la sua consequenziale stima pongano maggiori difficoltà operative e, infatti, proprio sotto tale aspetto, la giurisprudenza tenta di superare tali problematiche attraverso il meccanismo delle presunzioni, consentendo ai giudici di inferire l'esistenza e l'entità del danno da elementi indiziari (40). Tuttavia, l'uso di tale metodo solleva preoccupazioni riguardo alla possibilità che la semplice dimostrazione di un comportamento dannoso da parte del responsabile possa, automaticamente, portare alla conclusione che sia stato provocato un danno. In particolare, nel contesto dei danni non patrimoniali, è evidente la difficoltà di fondare le decisioni su fatti che, pur essendo dimostrabili, offrono solo una descrizione più dettagliata delle circostanze in cui si è verificato il danno, piuttosto che fornire una prova concreta della sua effettiva esistenza. Sotto tale aspetto, l'importo che la persona avrebbe probabilmente richiesto per autorizzare l'uso della propria immagine, può costituire un parametro adeguato.

La notorietà della persona gioca un ruolo fondamentale nella stima del danno patrimoniale che diviene più complessa nell'ipotesi di persone comuni; a tal fine soccorre, spesso, il vantaggio economico ottenuto dall'autore dell'illecita pubblicazione così mutuando parametri di tutela predisposti per la riproduzione non autorizzata di opere creative. Proprio in tale cornice, l'abuso dell'immagine di persone non celebri assume, maggiormente, i tratti della violazione dei dati personali, sebbene in entrambi i casi si rileva una mescolanza di interessi collettivi e diritti della personalità che merita di essere presa in considerazione (41).

Sotto il diverso profilo dell'illecito trattamento dei dati personali, è possibile, invece, inventariare una serie di pregiudizi minori che, pur non superando le soglie giurisprudenziali per il danno non patrimoniale, si legano a un modello economico che sfrutta la raccolta e l'analisi di dati personali attraverso l'intelligenza artificiale per fini commerciali (42). Nell'economia di tutto quanto brevemente esposto, va, nondimeno, ricordato come qualsivoglia ragionamento presuntivo posto a base del

(37) Cass. civ., Sez. Un., 15 novembre 2022, n. 33645, in *Urbanistica e appalti*, n. 2, 2023, 198, con nota di Cippitani - Langella, *La rilevanza del danno-evento nell'attuale applicazione della responsabilità civile*. Gli autori rilevano che "*le Sezioni Unite aprono al danno in re ipsa per occupazione illegittima dal momento che quest'ultima incide di per sé, intaccandolo, sul diritto di godimento del proprietario e da ciò consegue che quel danno può essere presunto in ragione delle particolari caratteristiche dell'evento dal quale origina. Ma, ed in ciò sta la "moderazione" tra i due orientamenti, non si consente di prescindere da un danno-conseguenza. È necessario perché si configuri la responsabilità civile che vi sia stata nel concreto l'impossibilità di godere direttamente o indirettamente (mediante concessione del godimento ad altri dietro corrispettivo) della proprietà. Tale perdita deve essere provata e qualora sia difficile quantificarla si può ricorrere (secondo principio di diritto) alla liquidazione del giudice con valutazione equitativa, se del caso mediante il parametro del canone locativo di mercato*".

(38) Cass. civ., ord., 23 gennaio 2023, n. 2685, in *Nuova giur. civ. comm.*, 2023, 3, 651, con nota di Brutti, *Indebito utilizzo dell'immagine quale dato personale e tutela risarcitoria*.

(39) Cass. civ., 15 luglio 2014, n. 16133, in *Danno e resp.*, 2015, 343 ss., con nota di Ceccarelli, *La soglia di risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali*.

(40) In questa ***Rivista***, Tribunale di Napoli Nord, ord. 30 luglio 2020, n. 6090, con nota di Di Ciommo, *Lesione del diritto all'immagine dell'impresa causata da un comunicato stampa diffuso online dell'Agcm, giurisdizione ordinaria e danno in re ipsa,* 115.

(41) Cass. civ., 25 novembre 2021, n. 36754, in *Resp. civ. prev.*, 2022, 1217, sul danno non patrimoniale derivante dalla violazione del diritto all'immagine di persona non famosa da determinarsi in via equitativa, in misura pari al presumibile prezzo del consenso; Cass civ., 11 maggio 2010, n. 11353, in *Foro it.*, 2011, 2, 540 ss., pt. 1 con nota Pardolesi, *Abusivo sfruttamento d'immagine e danni punitivi*.

(42) Esistono danni non patrimoniali minori e tollerabili che, sebbene indubbiamente esistenti, il GDPR considera, a fronte di una verifica nel caso concreto, riconducibili all'orbita della normale tollerabilità. Perviene alla medesima conclusione anche il Giudice di legittimità che ha proposto applicazione del principio di solidarietà anche per negare richieste risarcitorie legate a danni non patrimoniali, tuttavia lievi o per condotte non gravi, per fatti illeciti effettivamente accertati. Cfr. Cass. civ. sez. un., 11 novembre 2008, n. 26972, in *Giur. it.*, 2009, 2, 317 con nota di Tomarchio, *L'unitarietà del danno non patrimoniale nella prospettiva delle Sezioni unite*.

riconoscimento del danno non patrimoniale (43), può costituire oggetto di sindacato di legittimità solo nella misura in cui assuma determinate forme: a) errore nella valutazione della gravità, precisione e concordanza dei fatti considerati per le presunzioni semplici secondo l'art. 2729 c.c.; b) omissione di esame di fatti pertinenti che avrebbero potuto supportare una presunzione semplice; c) motivazioni apparenti che presentano logiche fallaci o conclusioni errate; d) interpretazioni errate di prove relative a fatti minori che potevano generare una presunzione semplice (44). Solo tale scrutinio consente alla Cassazione di verificare se i giudici di merito hanno correttamente ravvisato i caratteri della gravità, precisione e concordanza negli elementi a loro disposizione trattandosi, questo, questo non di un giudizio di fatto, ma piuttosto di una valutazione giuridica.

Il caso scrutinato, per la verità, resta, sotto il profilo risarcitorio, scarsamente approfondito. Nello specifico la Suprema Corte, da un lato, commina la "sanzione" dell'inammissibilità affermando come la valutazione sul motivo, dal carattere inevitabilmente controfattuale, implichi un giudizio sul fatto non censurabile e, dall'altro, riconduce la formula di rito utilizzata anche ad un difetto di "*interesse*" legato al giudizio del Giudice del merito sulla liceità della condotta del resistente tale da rendere superfluo qualsivoglia giudizio sull'eventuale danno.

Orbene, mentre si condivide pienamente il primo dei due assunti, dal momento che la valutazione operata dal primo Giudice non è in alcun modo sindacabile in sede di legittimità se si esclude l'ipotesi dell'omesso esame di un fatto decisivo oggetto di discussione tra le parti, si fatica, maggiormente, a comprendere appieno la seconda delle affermazioni. Invero, mentre immune da vizi appare il criterio di assorbenza che, di fatto, ha reso superfluo una valutazione sulla sussistenza del danno, del tutto dubbio appare la contemporanea ritenuta "*carenza di interesse*" opposta dalla Corte. I motivi di impugnazione, infatti, devono essere sì autonomi, sebbene sia consentito il criterio dell'assorbenza, ma pare difficile considerare inammissibile per carenza di interesse, *prima facie*, un motivo di impugnazione legato alla valutazione di inesistenza del danno operata dal primo Giudice sulla scorta di un giudizio, *ex post*, di un diverso motivo di impugnazione considerato presupposto. In altre parole, la mancata valutazione in termini presuntivi del danno non può, in astratto, essere considerata di per sé inammissibile per carenza di interesse sul presupposto di una negativa valutazione del precedente e preliminare motivo di impugnazione concernente la violazione delle norme sulla tutela di diritto all'immagine. Il difetto di interesse, che per natura affligge geneticamente una ragione di doglianza, non è da confondersi con il criterio dell'assorbenza che rende un giudizio superfluo in quanto "assorbito" da quello precedente. E ciò a tacere del fatto che, in ogni caso, l'autonomo motivo di impugnazione sulla sussistenza del danno avrebbe potuto essere vagliato anche al cospetto di una condotta scriminata ma ugualmente produttiva di danno.

Nel caso in questione, quindi, la legittimità del servizio giornalistico esclude il danno anche se appare chiaro come il Giudice del merito, a prescindere dalla evidenziata liceità, si sia posto il problema di un pregiudizio subito dal minore a fronte di una condotta giustificata; tuttavia, egli conclude per l'inesistenza di una prova in tale senso. Quanto al danno patrimoniale, in ultimo, è stato escluso a fronte dei rammentati più semplici criteri di individuazione che ne hanno decretato l'inesistenza.

## 6. Brevi considerazioni conclusive

L'ordinanza che si annota si colloca nel solco ormai tracciato di una vera e propria costituzionalizzazione del diritto all'immagine. Conseguenza immediata di tale percorso è l'inevitabile estensione dell'applicazione più ampia dei principi relativi al diritto della personalità e un distacco, ormai importante, da precedenti concezioni troppo restrittive ed ai limiti di una conclamata insufficienza.

La natura del consenso, ad esempio, si è evoluta sino a rendere l'espressione di volontà richiesta anche allorquando non si producano danni all'onore o alla reputazione, segnando, con ciò, un cambiamento rispetto alla pratica precedente che, indissolubilmente, legava la tutela della *privacy* ad un danno concreto alla reputazione. Non a caso il maggior rigore che caratterizza la manifestazione di volontà che deve essere, ora, esplicita e mai implicita, è indice di una chiara sovrapposizione tra la tutela dell'immagine ed il trattamento dei dati personali. Anche un consenso validamente prestato non legittima, automaticamente, ogni tipo di pubblicazione, specialmente se destinata ad un uso privato.

La Suprema Corte, dunque, ripropone una visione in cui la violazione dell'onore non è più l'unico criterio per determinare la violazione un diritto della personalità ma diviene elemento sintomatico di esistenza ed entità del danno. Vi è, in buona sostanza, piena consapevolezza della complessità e delle implicazioni trasversali del diritto all'immagine, considerando anche l'impatto potenzialmente offensivo dei ritratti e la loro capacità di replicazione su vari media nel tempo.

Una protezione rafforzata, quindi, del diritto all'immagine, che passa non solo attraverso la considerazione

(43) Ponzanelli, *Avanti con la presunzione: per una ricostruzione unitaria dell'onere della prova del danno patrimoniale e non patrimoniale*, in *Riv. it. med. leg.*, 2022, 1155 ss.

(44) Patti, *Le presunzioni semplici: rilievi introduttivi*, in *Il ragionamento presuntivo. Presupposti, struttura, sindacabilità*, a cura di Patti - Poli, Torino, 2022, 3 ss.

dell'interesse pubblico ma anche attraverso un esame del contesto specifico e delle emozioni personali degli individui coinvolti, che meritano di rimanere nella sfera privata dell'individuo e della famiglia.
Tuttavia, affermare con certezza, anche in riferimento al provvedimento esaminato, quale porzione del diritto all'immagine (riservatezza o pubblicità) sia, in assoluto, prevalente resta operazione difficile di certo non agevolata dal comune rimando compiuto dall'art. 10 c.c. alla legge speciale e viceversa e dalla non coincidente ampiezza dell'interesse tutelato dalle due fonti.

# Criptofonini: prime applicazioni dei principi enunciati dalle Sezioni Unite

Corte di Cassazione; sezione quarta; sentenza 4 aprile 2024; Pres. Francesco Maria Ciampi; Rel. Eugenia Serrao; Ga.Ma (Avv. Mercurelli).

*In ordine all'ammissibilità ed utilizzabilità, ai sensi dell'art. 191, comma 1 c.p.p. e 132, comma 3-bis, d.lg. 30 giugno 2003, n. 196 e della direttiva 2014/41 del Parlamento Europeo e del Consiglio, delle prove acquisite da Autorità estere a seguito di attività di cooperazione internazionale vi è la necessità di un controllo giurisdizionale circa la natura dell'attività svolta da queste ultime, nonché il rispetto del principio di equivalenza sancito dall'art. 6 par. 1 lett. b) direttiva 2014/41, ai fini del rispetto dei diritti fondamentali e di difesa.*

*...Omissis...*

**Svolgimento del processo**

1. Il Tribunale di Bari, in funzione di giudice del riesame ai sensi dell'art.309 cod. proc. pen., ha rigettato l'istanza proposta nell'interesse di A.A. avverso l'ordinanza emessa dal Giudice per le indagini preliminari del Tribunale di Bari il 17/10/2023 applicativa della custodia cautelare in carcere in relazione ai reati di cui agli artt.74, commi 1, 2 e 5, (capo 1) e 81,110 cod. pen. e 73, comma 1, 80, comma 2, d.P.R. 9 ottobre 1990, ri.309 (capi 6 e 8) commessi in Andria in epoca antecedente l'ottobre 2019 fino all'attualità (capo 1), il 12 agosto 2020 (capo 6) e in epoca compresa tra il 2 dicembre 2020 e il 19 febbraio 2021 (capo 8).

*...Omissis...*

2.2. Con il terzo motivo deduce violazione degli artt. 178, lett. c) e 181, comma 1, cod. proc. pen. nonché difetto di motivazione in ordine alla mancata declaratoria di nullità dell'O.I.E. n. 13/21 e dei suoi esiti, Sulla base della mancata messa a disposizione della difesa delle stringhe alfanumeriche dalle quali erano stati convertiti i contenuti delle chat dopo la loro captazione, senza peraltro che fosse nota la modalità con la quale era stata eseguita l'operazione di decrittazione, il Tribunale ha mostrato di non comprendere i termini reali della questione sollevata, avente a oggetto il diritto della difesa di accedere ai dati acquisiti prima della loro decrittazione con rinvio alle sentenze della Cassazione n. 49896 del 15 ottobre 2019 e della Corte EDU Grande Camera del 26 settembre 2023 Yuskel c. Turchia. Il Tribunale era stato sollecitato a pronunciarsi, alla stregua dell'ordinamento interno e della CEDU come interpretata dalla Corte di Strasburgo, sulla mancata messa ci disposizione della difesa delle stringhe alfanumeriche e delle chiavi di decrittazione in quanto lesiva del diritto di difesa e valutare quali ne fossero le conseguenze sull'acquisizione dei dati già in chiaro acquisiti attraverso la cooperazione dell'autorità giudiziaria francese. Il Tribunale, tuttavia, ha replicato affermando che "il diritto straniero è un fatto e spetta a chi eccepisce il difetto di compatibilità dimostrare il contrario", peraltro richiamando una decisione della Corte Suprema dei Paesi Bassi senza confrontarsi con la sentenza della Cassazione n.49896/2020 concernente un caso sovrapponibile a quello in esame.

2.3. Con il quarto motivo ha dedotto l'inutilizzabilità, ai sensi dell'art. 191, comma 1, cod. proc. pen. e 132, comma 3-*bis*, d.lgs. 30 giugno 2003, n.196 come modificato dal d.l. 30 settembre 2021, n. 132 conv. dalla legge 23 novembre 2021, n. 178 in riferimento all'art. 6 par. 1 lett. b) Direttiva 2014/41 del Parlamento Europeo e del Consiglio del 3 aprile 2014, dei messaggi inviati e ricevuti da e sull'apparecchio user (...*Omissis*...). Il Tribunale ha respinto l'eccezione di inutilizzabilità con un ragionamento costellato da gravi errori di diritto e fondato sul travisamento del contenuto degli atti trasmessi dall'autorità giudiziaria francese. Secondo la difesa, contrariamente a quanto affermato nell'ordinanza impugnata, i dati trasmessi alla Procura di Bari erano stati acquisiti solo in esecuzione dell'O.I.E. emesso dall'autorità italiana, come si evince dal provvedimento del 20 ottobre 2021 adottato dal giudice Madame Brice Hansemann delegata all'esecuzione della rogatoria, contenente l'ordine alla polizia giudiziaria di procedere a qualsiasi attività necessaria per l'accertamento della verità. Secondo quanto si desume dai verbali della polizia giudiziaria francese del 20 dicembre 2021 e del 6 gennaio 2022, i dati sono stati estratti mediante interfaccia di ricerca neozelandese. Secondo la difesa, questi documenti dimostrano che i dati trasmessi in Italia non fossero già nella disponibilità dell'autorità giudiziaria francese, che li aveva acquisiti solo a seguito della rice-

zione dell'O.I.E. dalla Procura di Bari per dare esecuzione a quest'ultimo. Il Tribunale, per confutare tale dato, ha attribuito rilievo a una nota prot. n. 197/21 del 3 dicembre 2021 sottoscritta dal Membro Nazionale per l'Italia presso Eurojust e trasmessa con la precisazione che il documento non fosse destinato all'inserimento in procedimenti penali, essendo inviato a soli fini informativi e conoscitivi dell'autorità giudiziaria e di polizia giudiziaria, con divieto di divulgazione a terzi. Trattasi, in ogni caso, si assume, di una nota che non ha alcuna attinenza al caso in esame in quanto vi si fa menzione di una squadra comune franco-belga-olandese, mentre nel presente procedimento le attività di acquisizione dei dati sono state svolte unicamente dalla polizia francese. La difesa aveva, dunque, posto questioni di diritto interno relative al regime di utilizzabilità degli esiti dell'O.I.E.: secondo il sistema processuale nazionale. Facendo riferimento all'art. 6 par. 1 lett. b) Direttiva del Parlamento Europeo, che individua nella proporzionalità della richiesta istruttoria il criterio di validità, ravvisando la proporzionalità nell'attività di prosecuzione delle indagini, e considerando l'attuazione nell'ordinamento interno di tale principio con art. 1 D.Lgs. 21 giugno 2017, n. 108, come peraltro applicato da Sez.6 n. 44154 del 26 ottobre 2023, la difesa evidenzia come sia stato riconosciuto dallo stesso Tribunale che l'iscrizione della notizia di reato nei confronti del A.A. fosse stata eseguita solo l'8 febbraio 2023, cosicché prima della ricezione degli esiti dell'O.I.E., avvenuta il 4 febbraio 2023, nessun elemento utile fosse stato acquisito dalla Procura per giustificare l'avvio di indagini nei suoi confronti; a maggior ragione non esistevano elementi utili il 5 ottobre 2021, quando l'O.I.E. era stato emesso. Ma il Tribunale ha ritenuto del tutto corretto l'operato della Procura affermando che l'iscrizione del A.A. nel registro delle notizie di reato fosse stata determinata dall'espletamento degli approfonditi accertamenti sul materiale trasmesso dalla Francia. La difesa evidenzia come ciò che rileva sia la constatazione obiettiva che l'O.I.E. sia stato ordinato nei confronti del A.A. non per proseguire le indagini ma per avviarle, dunque fuori dei casi consentiti dalla legge e dalla Direttiva del Parlamento Europeo. Inconferente risulta la distinzione tra indizi di colpevolezza e semplici indizi di reità per giustificare l'attivazione nei confronti del A.A. dell'O.I.E. pur in mancanza della formale iscrizione della notizia di reato a suo carico. Tanto più che all'epoca dell'emissione dell'O.I.E., il 5 ottobre 2021, vigeva il principio definitivamente consacrato dalle Sezioni Unite n. 40538/2008 secondo il quale il pubblico ministero ha l'obbligo di iscrivere immediatamente la notizia di reato con riferimento alla componente soggettiva quando sia superata la soglia del mero sospetto e l'attribuibilità del reato all'indagato assuma una certa pregnanza. Il Tribunale, ritenendo corretto l'operato del pubblico ministero, ha implicitamente affermato che nei confronti dell'attuale indagato non fosse stata superata la soglia del mero sospetto, pur parlando di indizi di reità. A differenza dei casi esaminati nell'ordinanza impugnata, nel caso in esame, secondo la difesa, non sussiste alcuna incertezza circa il fatto che l'autorità francese sì sia attivata solo e unicamente all'esito dell'ordine di indagine italiano. Con riguardo alla natura dei contenuti delle conversazioni sulle chat su piattaforme informatiche, la Corte Costituzionale con sentenza n. 170 del 2023 ha ricondotto tali comunicazioni alla nozione di corrispondenza estendendo a esse la tutela di cui all'art. 15 Cost. Ciò comporta che l'acquisizione all'estero di documenti e dati informatici inerenti a corrispondenza o ad altre forme di comunicazione debba essere sempre autorizzata da un giudice. L'operatività e l'ambito di applicazione dell'art. 234-*bis* cod. proc. pen. risultano, quindi, circoscritti ai casi in cui l'autorità giudiziaria straniera, all'esito di sue attività svolte autonomamente prima e a prescindere dalla ricezione dell'ordine di indagine europeo, si trovi già in possesso dei dati richiesti. Considerato che l'acquisizione dall'estero di dati probatori dal punto di vista giuridico-formale ha natura di procedimento, il vizio dell'atto iniziale, ossia l'ordine di indagine non formulato dal Giudice per le indagini preliminari, comporta la nullità dell'intero procedimento in quanto originatosi da un atto illegittimo perché emesso da un soggetto privo *ex lege* della competenza a emetterlo.

*...Omissis...*

3. Il difensore del ricorrente ha depositato in data 4 marzo 2024 memoria insistendo per l'annullamento anche alla luce dell'informazione provvisoria relativa alla sentenza delle Sezioni Unite n. 3 del 29 febbraio 2024.

*...Omissis...*

**Motivi della decisione**

*...Omissis...*

3. Il terzo motivo di ricorso pone il tema del diritto della difesa di acquisire i dati c.d. grezzi, prima della loro decrittazione, inviati dall'autorità francese in esecuzione di O.I.E. n.13/2021.

Va evidenziato in primo luogo che, contrariamente a quanto allegato nel ricorso, il Tribunale ha fornito espressa motivazione sul punto. In particolare, con riguardo al diritto della difesa di ottenere i dati sui quali si fonda il provvedimento cautelare per come acquisiti prima della loro decrittazione unitamente alle chiavi di decrittazione, il Tribunale ha ribadito, a pag. 50 nota 27, come l'obbligo di trasmissione degli atti abbia ad oggetto gli atti presentati al Giudice per le indagini pre-

liminari con la richiesta cautelare nonché gli elementi sopravvenuti a favore dell'indagato; si aggiunge che il diritto della difesa ad accedere ai dati per come acquisiti prima della loro decrittazione non è desumibile dalla pronuncia della Corte EDU Grande Camera del 26 settembre 2023 Yuskel Yalcinkaya c. Turchia, che ha ritenuto violato il diritto a un equo processo in un caso ben diverso dal presente, in cui la prova decisiva del giudizio di colpevolezza si identificava nella mera constatazione dell'utilizzo da parte dell'indagato di un sistema criptato di messaggistica telefonica, equiparato in via presuntiva dai giudici nazionali alla adesione consapevole e volontaria dello stesso a un'organizzazione terroristica, a prescindere dal contenuto dei messaggi e dalla identità delle persone con cui erano stati scambiati (Sez. 6, 26/10/2023, n. 46833, Bruzzaniti, in motivazione). E se i princìpi convenzionali giocano un ruolo importante nell'interpretazione del diritto nazionale, non bisogna trascurare che, secondo quanto espresso dalla Corte Costituzionale con sentenza n. 49 del 14 gennaio 2015, per attribuire valenza generale vincolante alle decisioni della Corte EDU, rispetto alle quali si è detto che hanno come punto di riferimento imprescindibile il caso concreto specificamente trattato e che solo rispetto a casi analoghi potrebbero assumere il valore di affermazione di un principio generale, si debba tener conto tanto delle peculiarità del caso deciso quanto del fatto che la decisione adottata deve essere espressione di un orientamento definitivo, che costituisce "diritto consolidato" generato dalla giurisprudenza europea.

Giova, per altro verso, evidenziare che si tratta di censura aspecifica in quanto priva dell'allegazione della non corrispondenza al vero dei dati decrittati posti a base del provvedimento cautelare. Si è, in più occasioni, evidenziato che l'algoritmo che consente la decrittazione dei messaggi non altera il contenuto del dato, essendo nozione acquisita alla scienza informatica che in assenza dell'algoritmo necessario alla decodificazione è impossibile ottenere un testo intellegibile con contenuto in lingua italiana difforme dal reale, potendosi al più avere una sequenza alfanumerica o simbolica priva di alcun senso. La pronuncia risulta esente da vizi e conforme alla logica secondo la quale la decrittazione del dato informatico è attività distinta dalla captazione e le operazioni di decodificazione del significato delle comunicazioni intercettate sono da tenere distinte dai requisiti di utilizzabilità della prova. Le incertezze circa la correttezza della decodificazione delle intercettazioni utilizzabili attengono al valore e alla portata probatoria delle comunicazioni decrittate e quindi non possono avere ingresso nel giudizio ove la difesa non alleghi argomenti a sostegno di errori nella lettura e/o nella interpretazione dei messaggi captati (Sez. 1, n. 6364 del 13/10/2022, dep. 2023, Calderon, in motivazione; Sez. 4, n. 29866 del 08/07/2022, Adenni, in motivazione).

4. Il quarto motivo di ricorso è fondato nei termini che seguono.

Sul tema inerente al fatto che l'autorità francese si sia attivata solo e unicamente all'esito dell'ordine di indagine italiano, i giudici del merito cautelare hanno fornito una risposta che deve essere ora riesaminata alla luce delle recenti pronunce delle Sezioni Unite. Il verbale del 6 gennaio 2022 redatto dalla polizia giudiziaria francese dà atto dell'avvenuta "estrazione" delle informazioni relative ai Conti Sky ECC tramite interfaccia di ricerca neozelandese. Tale operazione è stata interpretata dai giudici del merito cautelare come indicativa della acquisizione di dati già in possesso dello Stato di esecuzione; a pag. 54 dell'ordinanza impugnata si fa riferimento alla nota prot. 197 del 3 dicembre 2021 di Eurojust, che nel ricorso si afferma essere afferente a procedimenti inconferenti rispetto a quello in esame. Il riferimento alle polizie di Stati membri ulteriori rispetto a quella francese, che ha curato il procedimento di estrazione dei dati, non risulta però sufficiente a dare conto della provenienza dei dati da una più ampia attività investigativa inerente a un procedimento penale estero preesistente all'ordine di indagine europeo emesso dalla Procura italiana, elemento necessario secondo quanto si dirà in seguito.

4.1. Sul tema della disciplina di garanzia che afferisce a tali acquisizioni, va ricordato che l'Ordine Europeo d'Indagine deve aver a oggetto una prova acquisibile nello Stato di emissione e deve essere eseguito in conformità a quanto previsto nello Stato di esecuzione per il compimento di un analogo atto di acquisizione probatoria, dovendosi certamente presumere il rispetto di tale disciplina e dei diritti fondamentali, salvo una concreta verifica di segno contrario che, allo stato, non risulta allegata. Deve essere, poi, ricordato che, secondo un consolidato orientamento della giurisprudenza di legittimità, gli artt. l e 9 della Direttiva 2014/41/UE implicano che l'utilizzazione degli atti trasmessi a seguito di attività di cooperazione internazionale (come più volte affermato in tema di rogatoria attiva) non sia condizionata a un accertamento dei parte del giudice dello Stato di emissione concernente la regolarità delle modalità di acquisizione esperite dall'autorità straniera, in quanto vige la presunzione di legittimità dell'attività svolta e spetta al giudice straniero la verifica della correttezza della procedura e l'eventuale risoluzione di ogni questione relativa alle irregolarità lamentate nella fase delle indagini preliminari (Sez. l, n. 2312 del 2/02/2023, Demce, in motivazione; Sez. 5, n. 1405 del 16/11/2016, dep. 2017, Ruso, Rv. 269015; Sez. 2, n. 24776 del 18/05/2010, Mutari, Rv. 247750; Sez. I, n. 21673 del 22/01/2009, Pizzata, Rv. 243796).

4.2. Occorre, inoltre, osservare come l'art. 1 d.lgs. 21 giugno 2017, n. 108, secondo quanto chiarito da Sez. 6 n. 44154 del 26 ottobre 2023, consenta secondo il principio di proporzionalità che una richiesta istruttoria venga eseguita attraverso l'ordine di investigazione europeo purché essa sia necessaria per la prosecuzione delle indagini, in tal modo rispettando quanto affermato dalla Corte di Giustizia Europea laddove ha imposto la verifica in concreto dell'effettiva necessità di un intervento acquisitorio. La censura evidenzia che, all'atto della emissione il 5 ottobre 2021 da parte della Procura della Repubblica di Bari dell'ordine di esecuzione europeo n. 13/21, non fosse stato acquisito alcun elemento utile a giustificare l'avvio di indagini nei confronti del A.A. A tanto la difesa giunge osservando come l'iscrizione della notizia di reato nei confronti del A.A. sia avvenuta solo l'8 febbraio 2023, cosicché sarebbe provato che, prima della ricezione degli esiti dell'ordine di esecuzione, non esistessero elementi utili a giustificare l'emissione di tale ordine.
4.3. A pag. 50 dell'ordinanza impugnata si è, però, chiarito che, sebbene l'iscrizione del A.A. nel registro delle notizie di reato fosse avvenuta solo quando, dopo l'esecuzione dell'ordine di indagine, erano emersi elementi sufficienti a collegare la posizione del A.A. al traffico di sostanze stupefacenti, tuttavia nella stessa richiesta di ordine di indagine il A.A. era indicato quale persona interessata all'atto di indagine e al contempo erano indicati come indiziati di traffico di sostanze stupefacenti i soggetti che avevano in uso gli apparecchi cellulari con predeterminati user ID e nickname, tra i quali risultava il criptofonino abbinato alla user ID (...*Omissis*...) con nickname GM (verosimilmente le iniziali del prevenuto), poi risultato in uso al A.A. . Anche sotto il profilo della regolare selezione dei dati utili alle indagini, nel rispetto del principio di proporzionalità, sono stati indicati plurimi elementi a disposizione degli inquirenti al momento dell'emissione dell'O.I.E. (emergenti dal monitoraggio operato tramite videoripresa nei pressi dell'impresa MG-Pro gestita dal A.A., servizi di o.c.p. che avevano verificato alcuni incontri tra il A.A. e uno dei principali indagati, B.B., pag. 26 e nota n. 18 pag. 28, da intercettazioni dell'utenza (...*Omissis*...)intestata e in uso al A.A., cfr. nota n.19 pag. 33, in occasione dell'arresto con sequestro di kg. 3 di cocaina di C.C. con la quale il A.A. pacificamente intratteneva una relazione sentimentale, dalla geolocalizzazione della predetta utenza, pag. 44).
4.4. Non si tratta, dunque di una richiesta di indagine europea finalizzata ad avviare le indagini nei confronti del A.A., quanto piuttosto ad approfondirle. L'interpretazione seguita nell'ordinanza in merito alla disciplina di cui agli artt. 132, comma 3-*bis*, 1.178/2021 e 6 par. 1 lett. b) della Direttiva 2014/41/UE si fonda sul concetto che il pubblico ministero si possa avvalere dello strumento di collaborazione giudiziaria con uno Stato membro sulla base di semplici indizi della sussistenza di un fatto reato delineato sufficientemente senza che ne siano individuati i responsabili. Tale presupposto, ritenuto logicamente sussistente nel caso in esame, è stato contrapposto all'assunto difensivo secondo il quale per il ricorso alla procedura dell'ordine di indagine europeo sarebbe necessario che l'autore del reato sia stato già identificato e come tale già iscritto nel registro ai sensi dell'art. 335 cod. proc. pen.
4.5. Il tema proposto dalla difesa circa il rapporto tra i presupposti per l'emissione dell'ordine di indagine europeo e i presupposti per l'iscrizione di una persona nel registro delle notizie di reato sii fonda sul principio espresso dalla sentenza Sez. U, n. 40538 del 24/09/2009 (Lattanzi, Rv. 244378 - 01) circa l'obbligo di iscrizione della notizia di reato quando si è superata la soglia del mero sospetto e l'attribuibilità del reato all'indagato assuma una certa pregnanza. Ma il presupposto del ragionamento difensivo non è pregnante in quanto inidoneo a incidere sull'utilizzabilità degli atti acquisiti mediante O.I.E., dato lo stato delle indagini alla data in cui l'ordine fu emesso, posto che trova qui applicazione, ratione temporis (Sez. 6, ord. n. 2329 del 15/01/2024, in motivazione), il principio secondo il quale "Il termine di durata delle indagini preliminari decorre dalla data in cui il pubblico ministero ha iscritto, nel registro delle notizie di reato, il nome della persona cui il reato è attribuito, senza che al giudice per le indagini preliminari sia consentito stabilire una diversa decorrenza, sicché gli eventuali ritardi indebiti nella iscrizione, tanto della notizia di reato che del nome della persona cui il reato è attribuito, pur se abnormi, sono privi di conseguenze agli effetti di quanto previsto dall'art. 407, comma 3, cod. proc. pen." (Sez. 6, n. 4844 del 14/11/2018, dep. 2019, Ludovisi Rv. 275046 - 01).
4.6. Considerato, però, che l'acquisizione delle chat da parte della Procura della Repubblica presso il Tribunale di Bari è avvenuta con lo strumento di collaborazione giudiziaria internazionale rappresentato dall'Ordine Europeo d'Indagine, disciplinato dal D.Lgs. 27 giugno 2017, n. 108, emanato per dare attuazione alla direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014, occorre rilevare che in relazione al contrasto inerente all'individuazione dello strumento processuale interno da porre a parametro per l'importazione delle chat decrittate e richieste con O.I.E. le Sezioni Unite hanno recentemente affermato (notizia provvisoria di decisione n.4/2024) che l'acquisizione di atti di altro procedimento penale non deve essere oggetto di verifica giurisdizionale preventiva della sua legittimità nello Stato di emissione dell'O.I.E.
4.7. Riprendendo, dunque, il tema della previa acquisizione dei dati trasmessi dall'autorità di altro Stato

membro, il pubblico ministero italiano è legittimato, ai sensi dell'art. 27, comma 1, del D.Lgs. n. 108 del 2017 a emettere, nell'ambito delle proprie attribuzioni nella fase delle indagini preliminari, un ordine europeo di indagine volto all'acquisizione di una prova "già disponibile" e a trasmetterlo direttamente all'autorità di esecuzione (CGUE del 8/12/2020, C584/19 a proposito delle condizioni in virtù della quali un ufficio di Procura sia qualificabile come "Autorità di emissione"). La Corte di giustizia ha, a tale proposito, statuito che, una volta che la prova è stata acquisita nello spazio comune europeo e in conformità al diritto dell'Unione, la sua ulteriore circolazione, con trasferimento ad altro procedimento, non richiede una nuova autorizzazione del giudice, ma solo che sia rispettato il limite della utilizzabilità per ragioni di sicurezza pubblica e repressione di gravi reati (Corte di giustizia, sentenza 7 settembre 2023, A.G. - C-162/22, relativa all'utilizzazione della documentazione acquisita dal giudice presso gli operatori di telecomunicazioni in processi diversi da quello originario; sentenza 16 dicembre 2021, H.P., C-724/19, 10 in tema di ordine europeo di indagine emesso da un pubblico ministero per l'acquisizione in altro Paese di dati dagli operatori di telecomunicazione).

4.8. Tale profilo di censura dovrà, dunque, essere nuovamente esaminato e approfondito dal giudice del rinvio in ragione delle carenze motivazionali indicate al precedente par. 4.

5. Quanto all'ammissibilità dell'acquisizione degli atti mediante ordine europeo di indagine penale, l'art. 6, par. 1 lett. b), Direttiva 2014/41/UE, prescrive che "l'autorità di emissione può emettere un ordine europeo di indagine solamente quando l'atto o gli atti di indagine richiesti nell'ordine europeo di indagine avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo". L'art. 10, par. 5, di tale direttiva sancisce, inoltre, che "ove, conformemente al paragrafo 1, l'atto di indagine richiesto nell'ordine europeo di indagine non sia previsto dal diritto dello Stato di esecuzione o non sia disponibile in un caso interno analogo, e ove non vi siano citati atti di indagine che consentano di ottenere lo stesso risultato dell'atto di indagine richiesto, l'autorità di esecuzione informa l'autorità di emissione che non è stato possibile fornire l'assistenza richiesta". L'autorità giudiziaria dello Stato di emissione non può, pertanto, demandare all'autorità giudiziaria dello Stato di esecuzione il compimento di un atto di indagine che non sia contemplato dalla *lex fori*, né tantomeno richiedere la trasmissione di prove che non avrebbero potuto formare di acquisizione in un procedimento penale interno. La disposizione intende, infatti, evitare che le prove raccolte dall'autorità giudiziaria dello Stato di esecuzione, in conformità al proprio ordinamento, possano eludere i divieti di acquisizione probatoria stabiliti dalla legge processuale dello Stato di emissione, divenendo utilizzabili ai fini decisori. È, dunque, necessario verificare se il principio di equivalenza sancito dalla 6, par. 1 lett. b), Dir. 2C14/41/UE sia stato rispettato nel caso di specie e, segnatamente, se le chat acquisite dall'autorità giudiziaria francese fossero acquisibili nell'ordinamento italiano.

5.1. Il Collegio ritiene che, alla luce dei recenti arresti della Corte Costituzionale e delle Sezioni Unite, l'orientamento interpretativo, sposato nell'ordinanza impugnata, secondo il quale le chat intervenute sulla piattaforma Sky Ecc avrebbero natura di "documenti di dati informatici", debba essere rivisitato. Nella giurisprudenza costituzionale si è ampliato il concetto di "corrispondenza" con argomentazioni inerenti a qualunque flusso di comunicazioni, ancorché esaurito (Corte Cost. 7 giugno 2023 n. 170, in cui si afferma che "Il concetto di "corrispondenza" è ampiamente comprensivo, atto ad abbracciare ogni comunicazione di pensiero umano: idee, propositi, sentimenti, dati, notizie, tra due o più persone determinate, attuata in modo diverso dalla conversazione in presenza; in linea generale, pertanto, lo scambio di messaggi elettronici – e-mail, SMS, WhatsApp e simili – rappresenta, di per sé, una forma di corrispondenza agli effetti degli artt. 15 e 68, terzo comma, Cost."; già in tal senso Sez. 4, n. 40903 del 2:8/06/2016, Gras; si, Rv. 268228-01; Sez. 3, n. 50452 del 10/11/2015, Guarnera, Rv. 265615-01). Tale definizione è da porre in correlazione con le posizioni assunte in materia dalla Corte Europea dei diritti dell'uomo, che ha ricondotto "sotto il cono di protezione dell'art. 8 CEDU", ove pure si fa riferimento alla "corrispondenza" tout court, i messaggi di posta elettronica (Corte EDU, sent. 5/09/20:17, Barbulescu c. Romania, par. 72; Corte EDU, sent. 3/04/2007, Copland c. Regno Unito, par. 41), gli SMS (Corte EDU, sent. 17/12/2020, Saber c. Norvegia, par. 48) e la messaggistica istantanea inviata e ricevuta tramite internet (Corte EDU, sent. Barbulescu, cit., par 74).

5.2. Risulta inoltre decisivo, sul punto, il dictum di SSUU Gjuzi e Giorgi (informazioni provvisorie di decisione nn. 3 e 4 del 29 febbraio 2024), da cui si evince che il trasferimento all'Autorità giudiziaria italiana, in esecuzione di ordine europeo di indagine, del contenuto di comunicazioni effettuate mediante criptofonini e già acquisite e decrittate dall'Autorità giudiziaria estera in un proprio procedimento penale rientra nell'acquisizione di atti di un procedimento penale, che rispetta l'art.6 della Direttiva 2014/41/UE in quanto, secondo la loro natura, trova il suo fondamento negli artt.78 disp. att. cod. proc. pen., 238, 270 cod. proc. pen.

5.3. Ove si riconosca natura captativa alle comunicazioni effettuate mediante criptofonini, e si accerti che i flussi di comunicazione, al momento in cui tali dati sono stati

richiesti dall'Autorità giudiziaria italiana, non erano più in corso, il relativo trasferimento tra due procedimenti penali è ammesso a opera del pubblico ministero nell'ordinamento italiano alle condizioni previste dall'art.270 cod. proc. pen., da considerare il "caso interno analogo" al quale fa riferimento la disposizione eurounitaria (rilevanza e indispensabilità per l'accertamento dei delitti per i quali è obbligatorio l'arresto in flagranza) e secondo i criteri di bilanciamento degli opposti interessi indicati dalle Sezioni Unite nella sentenza Cavallo (Sez. U, n. 51 del 28/11/2019, dep.2020, Rv. 277395 - 01) e recentemente da Corte E.D.U., Sezione Terza, del 13 febbraio 2024, nel procedimento Podchasov c. Russia (n. 33696/19); ferma restando l'inconferenza delle censure inerenti alle modalità di acquisizione dei dati già valutate dall'Autorità giudiziaria di altro Stato membro secondo la *lex loci*, come già detto al par.4.1.

6. Considerato, dunque, che appare necessario riesaminare la natura dell'attività svolta all'estero e attribuire alla stessa la corretta qualificazione giuridica, l'ordinanza impugnata deve essere annullata con rinvio affinché il Tribunale verifichi nuovamente l'utilizzabilità, nel presente giudizio cautelare, delle suindicate chat. Tale disamina è funzionale a consentire alla difesa di contestare la necessità e la regolarità dell'O.I.E. (CGUE 11/11/2021, C 852/19 Gavanozov, par. 54) sotto il profilo del rispetto elei diritti fondamentali dell'indagato ai sensi degli artt. 6 e 14 par. 7 Direttiva 2014/41/UE.

6.1. Il tema centrale sul quale il Tribunale del riesame si deve pronunciare, resta, dunque, il controllo giurisdizionale successivo all'acquisizione dei dati, sul punto se si tratti di chat già acquisite dall'Autorità giudiziaria estera in un proprio procedimento penale e se siano state rispettate le specifiche modalità processuali la cui osservanza ne rende acquisibili e utilizzabili nello Stato italiano i contenuti, in ossequio alla previsione degli artt. l par. l, 10 par. 2 lett. a), 13 par. l della Direttiva e art. 2, comma 1 lett. a), 9, comma 5 lett. a), 10, comma 1, 12, comma 1, d.lgs. 27 giugno 2017, n.108, in altre parole la legittimità della trasposizione dei risultati delle intercettazioni alla luce della disciplina processuale italiana. La difesa aveva, infatti, contestato l'utilizzabilità dei dati per mancanza di controllo giurisdizionale e, sul punto, il Tribunale del riesame si è limitato ad affermare (pagg. 54-56) che, applicando il principio di equivalenza, se ne deve desumere che per le comunicazioni non più in corso di svolgimento, e già in possesso dell'autorità straniera, non opererebbe alcun divieto probatorio connesso alla mancanza di un'autorizzazione giudiziale. Tale assunto, se condivisibile con riferimento al controllo preventivo, non risulta satisfattivo, alla luce delle recenti pronunce delle Sezioni Unite (secondo le quali "l'Autorità giurisdizionale dello Stato di emissione dell'ordine europeo di indagine deve verificare il rispetto dei diritti fondamentali, comprensivi del diritto di difesa e della garanzia di un equo processo"), in assenza di un controllo successivo circa l'utilizzabilità dei dati secondo l'ordinamento interno.

6.2. In merito alla rilevanza e indispensabilità delle chat per l'accertamento di reati per i quali è previsto l'arresto in flagranza si osserva, da un lato, che si procede in relazione al reato di cui all'art. 74 T.U. Stup. e, dall'altro, che è stato già affermato il principio secondo il quale "In fase di indagini preliminari, non è necessario che nel provvedimento che utilizza, ai sensi dell'art. 270 cod. proc. pen., i risultati di intercettazioni effettuate in procedimento diverso sia espressamente motivata l'indispensabilità di tali risultati ai fini dell'accertamento dei delitti per cui si procede e per i quali è previsto l'arresto in flagranza, potendo la valutazione di indispensabilità essere compiuta anche implicitamente, mediante l'attribuzione agli elementi utilizzati di specifica rilevanza ai fini della decisione adottata" (Sez. 3, n. 5821 del 18/0:1/2022, Napolitano, Rv. 282804 -01).

6.3. Resta, quindi, da assicurare, come richiesto dall'art. 14 par.7 Direttiva 2014/41/UE (che così recita "Lo Stato di emissione tiene conto del fatto che il riconoscimento o l'esecuzione di un OEI sono stati impugnati con successo conformemente al proprio diritto nazionale. Fatte salve le norme procedurali nazionali, gli Stati membri assicurano che nei procedimenti penali nello Stato di emissione siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove acquisite tramite l'OEI") il pieno esercizio del diritto di difesa. Sul punto, occorre che la decisione inerente alle condizioni di ammissibilità dei dati così acquisiti sia rimessa al giudice del merito cautelare onde assicurare il contraddittorio (Sez. 6, n. 44155 del 26/10/2023 Kolgjokaj, in motivazione), anche perché le valutazioni circa l'utilizzabilità del materiale captativo proveniente dal procedimento in cui sono state disposte le relative operazioni, non vincolano il giudice del diverso procedimento, che conserva piena autonomia decisoria e deve procedere ad autonomo apprezzamento (Sez. 1, n. 42006 del 28/10/2010, Tavelli, Rv. 249109 - 01).

*...Omissis...*

8. Tali sono le ragioni per le quali l'ordinanza deve essere annullata, con rinvio per nuovo esame al Tribunale di Bari.

*...Omissis...*

# IL COMMENTO

*di Gaetano Ancona*

**Sommario:** 1. Una premessa sui fatti. – 2. La decisione alla luce dell'evoluzione giurisprudenziale: verso un rispetto dei diritti del prevenuto? – 2.1. Le indagini francesi. – 2.2. (*Segue*) La normativa di riferimento. – 2.3. (*Segue*) Le modalità di emissione e l'utilizzabilità del materiale probatorio. – 3. Le questioni ancora irrisolte. – 4. Spunti di riflessione alla luce della Sentenza della Corte di Giustizia C-670/22.

La sentenza in esame rappresenta un'importante tappa nell'interpretazione normativa relativa all'emissione degli Ordini Europei di Indagine (O.E.I.), per l'acquisizione di prove da sistemi di messaggistica cifrata come Sky Ecc e Encrochat. Analizzando i principi ivi esposti, il contributo esplora le sfide ancora presenti, concentrandosi sul delicato equilibrio tra investigazioni penali e tutela dei diritti fondamentali. Infine, prova a prospettare delle soluzioni alla luce della decisione dalla Corte di Giustizia dell'UE sul caso Encrochat.

*The judgment represents an important milestone in interpreting the European Investigation Orders (EIOs) for acquiring evidence from encrypted messaging systems such as Sky ECC and Encrochat issued by Italian judicial authorities. By analysing the principles outlined therein, the contribution explores the challenges still present, focusing on the delicate balance between criminal investigations and the protection of fundamental rights. Finally, it seeks to propose solutions in light of the decision of the Court of Justice of the EU on the Encrochat case.*

## 1. Una premessa sui fatti

La decisione in commento si inserisce all'interno di un lungo filone giurisprudenziale volto ad individuare la normativa interna di riferimento per l'emissione di un Ordine Europeo di Indagine, diretto ad acquisire messaggistica scambiata su sistemi cifrati come *Sky Ecc* e *Encrochat*. Nello specifico, la presente sentenza costituisce la prima applicazione dei principi enunciati dalle Sezioni Unite in merito alla corretta sussunzione normativa degli elementi ottenuti tramite O.E.I. (1).

La vicenda processuale sottesa alla decisione è piuttosto intricata. Essa trae origine dall'applicazione, da parte del g.i.p. presso il Tribunale di Bari, di una misura privativa della libertà personale nei confronti dell'indagato, per reati di associazione finalizzata allo spaccio di sostanze stupefacenti (2). La decisione è fondata, principalmente, su messaggi privati scambiati dall'indagato con altri presunti membri della cosca criminale, ottenuti dalla Procura della Repubblica per il tramite di un O.E.I. trasmesso all'autorità giurisdizionale francese. La messaggistica in questione era stata scambiata su telefonini criptati che utilizzavano la tecnologia *Sky Ecc* (piattaforma di messaggistica crittografata che garantiva ai propri clienti un elevatissimo grado di riservatezza) (3), il cui *server* era ubicato a Roubaix in Francia.

La misura custodiale era poi stata confermata dal Tribunale del Riesame di Bari, decisione avverso la quale la difesa ha proposto ricorso per Cassazione, lamentando, *inter alia*, l'incorretta applicazione della normativa di matrice eurounitaria per la circolazione di prove di cui alla dir. UE 3 aprile 2014, n. 41 (4), così come implementata dal d.lgs. 21 giugno 2017, n. 108 (5). In particolare, il ricorrente denunciava l'incongruenza delle modalità con cui i dati sono stati raccolti dall'autorità estera, l'impossibilità della difesa di contestare ed analizzare le modalità di estrazione, l'inconferenza del riferimento normativo italiano sulla base del quale la procura ha emesso l'O.E.I., e la competenza stessa della procura ad emettere la richiesta.

(1) Cfr. Cass., sez. un., 29 febbraio 2024, informazioni provvisorie n. 3 e 4, disponibili su <www.giurisprudenzapenale.com>.

(2) Artt. 73 e 74, d.P.R. n. 309 del 1990.

(3) Per una completa ricostruzione del funzionamento dell'applicativo *Sky Ecc* si rimanda a Morcella, *Le due mosse, con cui l'AG francese ha "hackerato" Sky ECC*, in *Dir. pen. e proc.*, 2023, 1378.

(4) Per un commento alla direttiva, si vedano, per tutti, Caianiello, *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove*, in *Proc. pen. e giust.*, 2017, 1 ss.; Daniele, *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, in *Riv. trim. Dir. pen. cont.*, 2015, 86 ss.; Marafioti, *Orizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento*, in *L'ordine europeo di indagine: criticità e prospettive* a cura di Bene, Lupària e Marafioti, Torino, 2017, 9 ss.

(5) Per un commento alla normativa di attuazione, Mangiaracina, *L'acquisizione "europea" della prova cambia volto: l'Italia attua la Direttiva relativa all'ordine europeo di indagine penale*, in *Dir. pen. e proc.*, 2018, 158 ss.; Trogu, *Ordine europeo di indagine penale*, in *Cooperazione giudiziaria europea in materia penale* a cura di Marandola, Milano, 2018, 1004 ss.; Caianiello, *L'attuazione della direttiva sull'ordine europeo di indagine penale e le sue ricadute nel campo del diritto probatorio*, in *Cass. pen.*, 2018, 2197 ss.

## 2. La decisione alla luce dell'evoluzione giurisprudenziale: verso un rispetto dei diritti del prevenuto?

La definizione dei confini della questione non è operazione semplice. In effetti, si intrecciano tra loro diverse tematiche di fondamentale importanza. *In primis*, ad intrecciarsi sono gli ordinamenti giuridici di due Stati. La transnazionalità della prova richiede il ricorso ai mezzi di cooperazione tra Stati membri dell'Unione. Il riferimento normativo è, in questo caso, la direttiva sull'O.E.I., che garantisce la possibilità alle autorità giudiziarie di uno Stato membro di richiedere l'acquisizione di una prova o il trasbordo di prove già ottenute in uno Stato diverso. Dunque, risultano di estrema rilevanza le modalità con cui le attività investigative sono state espletate nello Stato di esecuzione.

*In secundis*, l'emissione di un ordine d'indagine europeo è subordinata al rispetto di alcuni requisiti. La richiesta deve essere necessaria per la prosecuzione delle indagini, proporzionata, e rispettare il principio di equivalenza: gli atti di indagine richiesti nell'O.E.I. dovrebbero poter essere emessi "alle stesse condizioni in un caso interno analogo" (6). Le modalità di acquisizione seguite dall'autorità estera, determinano la definizione della categoria processual penalistica di riferimento per l'emissione dell'ordine di indagine (7).

Infine, sia le procedure di assunzione che la normativa interna di riferimento influiscono inevitabilmente sulle garanzie di cui la difesa ha il diritto di beneficiare. (8)

L'analisi delle questioni giuridiche coinvolte richiede un approccio graduale. Il primo quesito da porsi attiene alla definizione delle attività di indagine svolte dall'autorità giudiziaria d'oltralpe. In seguito, vi è da chiedersi quale sia, alla luce del principio di non sostituibilità (9), la norma o le norme che permetterebbero lo svolgimento di attività simili in un procedimento domestico. Infine, andrebbero approfondite le modalità di emissione e di eventuale utilizzazione degli elementi acquisiti.

### *2.1. Le indagini francesi*

L'attività investigativa svolta dalle autorità d'oltralpe è stata caratterizzata da un elevato grado di complessità tecnica. I criptofonini e la piattaforma *Sky Ecc* rappresentavano, allo stato dell'arte, le più avanzate tecnologie di criptatura della messaggistica e dei dati forniti solitamente da dispositivi mobili (traffico dati, localizzazione GPS, ecc.). Infatti, si tratta di apparecchi a cui sono state apportate diverse modifiche per garantirne l'impenetrabilità. Nei criptofonini risultavano disattivati i servizi Google, la videocamera, il microfono, il sistema Bluetooth, la porta USB e il sistema di geolocalizzazione. In più, essi non si agganciavano alle tradizionali reti di telecomunicazioni, ma utilizzavano piattaforme, anch'esse criptate, con *server* gestiti da privati localizzati in paesi esteri. Nello specifico, la piattaforma *Sky Ecc* era una piattaforma di messaggistica "coperta" da quattro distinte chiavi di cifratura (10). Alcuni di questi algoritmi di cifratura erano locati nel *server*, per permettere il flusso di chat, mentre le restanti erano contenute nei criptofonini in possesso ai singoli utilizzatori. Inoltre, oltre alla protezione offerta dalle chiavi di cifratura, i messaggi inviati per il tramite della piattaforma, si cancellavano automaticamente nel corso di 48 ore. Sky Ecc non conservava i contenuti dei messaggi, né tanto meno le informazioni ad essi legati.

Come è facilmente intuibile, ottenere accesso alla corrispondenza scambiata su Sky Ecc non è stato un compito agevole. Per poter decifrare il contenuto delle *chat*, scambiate per il tramite della piattaforma, gli inquirenti dovevano entrare in possesso di tutte e quattro le chiavi cifrate, oltre alla necessità di intercettare la messaggistica nel momento di passaggio attraverso il *server*, essendovi il concreto rischio di perdere l'occasione di conoscerne il contenuto.

Le autorità francesi hanno installato, all'insaputa del gestore del *server*, dei *malawere* che permettevano di intercettare il flusso di dati intercorrente sul *server* stesso. Inoltre, nonostante il governo francese abbia posto il segreto di stato su come sia stato possibile ottenere le chiavi di cifratura, si ritiene che questo *malawere* fosse in grado di inviare delle notifiche *push* sui singoli criptofonini per ottenere le *passwords* in possesso a ciascun utilizzatore (11).

Dunque, l'attività svolta in Francia sembrerebbe rientrare nel concetto di intercettazioni. Attraverso l'installazione di un *trojan* su un dispositivo fisso (il *server*), è stato possibile captare in tempo reale le conversazioni e

(6) Art. 6, paragrafo 1, lett. b), dir. UE n. 41 del 2014; art. 27, comma 1, d.lgs. n. 108 del 2017.

(7) Parla di «garanzie a geometria variabile» DANIELE, *Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky Ecc/Encrochat in attesa delle Sezioni Unite*, in *Sistema Penale*. Il testo è disponibile al seguente link <https://www.sistemapenale.it/it/scheda/daniele-ordine-europeo-di-indagine-penale-e-comunicazioni-criptate-il-caso-sky-ecc-encrochat-in-attesa-delle-sezioni-unite>.

(8) FILIPPI, *Criptofonini e diritto di difesa*, in *Pen. dir. e proc.*, 2023, 322. Sul punto, si veda anche LORENZETTO, *L'acquisizione all'estero di comunicazioni digitali criptate nella fucina dell'ordine europeo di indagine penale*, in *Cass. pen.*, 2024, 185.

(9) CONTI, *Il principio di non sostituibilità: il sistema probatorio tra costituzione e legge ordinaria*, in *Cass. pen.*, 2024, 451 ss.

(10) MORCELLA, *op. cit.*, 1378.

(11) LUDOVICI, *I criptofonini: sistemi informatici criptati e server occulti*, in *penaledp*. Il testo è disponibile al seguente link <https://www.penaledp.it/i-criptofonini-sistemi-informatici-criptati-e-server-occulti/>.

i flussi comunicativi gestiti dalle piattaforme crittografate. È probabile che le attività di captazione e quelle di decriptazione siano avvenute in momenti distinti, ma la natura del flusso comunicativo ne imponeva l'intercettazione contestuale. Tuttavia, a causa delle poche informazioni disponibili, non si può del tutto escludere che il *server* e i criptofonini potessero registrare i messaggi (12).

### *2.2. (***Segue***) La normativa di riferimento*

La natura delle attività di indagine svolte in Francia costituiscono il punto di partenza per l'individuazione del corrispettivo normativo domestico, che dovrebbe costituire l'elemento giustificativo per l'emissione di un ordine d'indagine europeo. Il recente susseguirsi di sentenze di legittimità ha dimostrato la complessità dell'operazione tassonomica. Infatti, nel corso di pochi mesi, la Suprema Corte ha proposto tre diverse soluzioni al medesimo problema. Secondo un primo filone interpretativo (13), le *chat* in possesso dell'autorità estera costituivano documenti e dati informatici, il cui riferimento normativo nazionale è da individuare nell'art. 234-*bis* c.p.p. Tuttavia, la prospettata soluzione è stata messa in crisi dallo sviluppo della giurisprudenza costituzionale in tema di corrispondenza. Il giudice delle leggi, infatti, con la sentenza n. 170 del 2023 ha ampliato, e non di poco, il concetto di corrispondenza. Ad avviso della Corte Costituzionale, il concetto di corrispondenza, tutelato dall'art. 15 Cost., è «ampiamente comprensivo» ricomprendendovi la corrispondenza elettronica, anche a seguito della ricezione da parte del destinatario (14). Dunque, lo scambio di messaggi su *app* di messaggistica, anche se archiviati, rientra nell'alveo dell'art. 15 Cost., determinando una tutela maggiore della limitazione della libertà e segretezza dello stesso, che può essere attuato unicamente per atto motivato dell'autorità giudiziaria e con le garanzie stabilite dalla legge.

Alla luce di tali novità, i successivi interventi del supremo consesso si sono orientati verso una soluzione (parzialmente) differente. La Corte Suprema, con due sentenze gemelle (15), ha ritenuto che il corretto riferimento normativo nazionale dovesse rinvenirsi negli artt. 254-*bis* o 266-*bis* c.p.p., a seconda delle modalità acquisitive poste in essere dall'autorità estera. A ben vedere, i giudici di legittimità, valorizzando i principi enunciati dalla Consulta, hanno sostenuto che qualora l'attività investigativa si traduca nell'accesso occulto al contenuto archiviato nel *server* durante l'indagine, tale acquisizione deve essere considerata ai sensi dell'art. 254-*bis* c.p.p. D'altro canto, se, invece, l'attività consiste nell'intercettazione e nella registrazione del messaggio cifrato mentre è in transito dall'apparecchio del mittente a quello del destinatario, il mezzo più appropriato per la ricerca della prova è l'intercettazione telematica, come previsto dall'art. 266-*bis* c.p.p. (16).

Ciononostante, il contrasto tra le sezioni "semplici" della Cassazione non si è risolto. Pertanto, è stato rimesso alle Sezioni Unite il compito di comporre le diversità di vedute. Nello specifico, con l'ordinanza 30 novembre 2023, n. 47798, la terza sezione ha riferito la seguente questione: se «l'acquisizione di messaggi su chat di gruppo scambiati con sistema cifrato, mediante OEI, presso autorità giudiziaria straniera che ne ha eseguito la decrittazione costituisca acquisizione di documenti e di dati informatici ai sensi dell'art. 234 bis c.p.p. o di documenti *ex* art. 234 c.p.p. o sia riconducibile in altra disciplina relativa all'acquisizione di prove» (17). Sul punto, il Supremo Collegio, nella sua composizione più autorevole, ha provvisoriamente risposto al quesito sostenendo che la corretta disciplina interna di riferimento è da individuare negli artt. 78 disp. att. c.p.p., 238 c.p.p. e 270 c.p.p. (18). Ancorché non specificato dalle Sezioni Unite, essendo ancora attese le motivazioni della decisione, si può ritenere che l'inquadramento in una delle due fattispecie, trasbordo di prove assunte in un altro procedimento o trasbordo di intercettazioni assunte in un procedimento diverso, dipenda dal momento in cui l'autorità italiana richiede la trasmissione delle prove. Invero, qualora lo scambio di conversazioni di cui si faccia richiesta sia già stato assunto all'interno di processo estero, sarà applicabile il combinato disposto degli artt. 78 disp. att. c.p.p. e 238 c.p.p. Mentre, nel caso in cui il procedimento estero si trovi ancora nella fase delle indagini preliminari o, quanto meno, manchi ancora il vaglio di un magistrato decidente, norma interna, ai fini della richiesta di un O.E.I. ai sensi dell'art. 6, paragrafo

(12) Filippi, *op. cit.*, 324.

(13) Cass. 5 aprile 2023, n. 16347 in C.*E.D. Cass.*, n. 284513; Cass. 13 gennaio 2023, n. 19082, in C.*E.D. Cass.*, n. 284440; Cass. 13 ottobre 2022, n. 6364, in C.*E.D. Cass.*, n. 283998; Cass. 20 aprile 2021, n. 18907, in C.*E.D. Cass.*, n. 281819.

(14) Corte cost. 27 luglio 2023, n. 170, in questa ***Rivista***, 2023, 669 con nota di Foderini, *E-mail e messaggi di whatsapp del "parlamentare"*, 675. Si veda, anche, Fontani, *La svolta della Consulta: la "corrispondenza telematica" è pur sempre corrispondenza*, in *Dir. pen. e proc.*, 2023, 1312 ss.

(15) Cass. 26 ottobre 2023, n. 44154, in C.*E.D. Cass.*, n. 285284; Cass. 26 ottobre 2023, n. 44155, in C.*E.D. Cass.*, n. 285362.

(16) Nocerino, *Ancora in tema di criptofonini: nuovi arresti giuridprudenziali in attesa delle Sezioni Unite*, in *penaledp*. Il testo è disponibile al seguente link <https://www.penaledp.it/criptofonini-nuovi-arresti-giurisprudenziali-in-attesa-delle-sezioni-unite/>.

(17) Cass. 30 novembre 2023, ord. n. 47798, reperibile su <www.sistemapenale.it>.

(18) Cass., sez. un., 29 febbraio 2024, informazione provvisoria n. 3, *cit.*

1, lett. b), dir. UE n. 41 del 2014, è la disciplina *ex* art. 270 c.p.p. (19).
A tal riguardo, è il caso di soffermarsi sulla decisione in commento, poiché fornisce delle importanti chiavi interpretative in merito alla determinazione dell'istituto giuridico più confacente. Prima di tutto, in motivazione la Corte ha ribadito che le *chat* intervenute sulla piattaforma *Sky Ecc* hanno natura di corrispondenza, tenuto conto dei recenti approdi della giurisprudenza costituzionale e di quella sovranazionale (20). Infatti, le limitazioni alla corrispondenza sono tutelate dall'art. 15 Cost., a livello nazionale, e dall'art. 8 della Conv. eur. dir. umani, nonché, verrebbe da aggiungere, dall'art. 7 della Carta dei diritti fondamentali dell'Unione Europea (Carta di Nizza), a livello sovranazionale. Perciò, nonostante non prenda una posizione definitiva (21), la Corte ritiene che il trasferimento dei flussi di comunicazioni dall'autorità francese verso quella italiana debba avvenire secondo le modalità dell'art. 270 c.p.p., da considerarsi «il caso interno analogo».

### *2.3. (***Segue***) Le modalità di emissione e l'utilizzabilità del materiale probatorio*

L'inquadramento della vicenda nell'art. 270 c.p.p. ha delle importanti ricadute in tema di autorità competenti ad emettere un O.E.I. e di utilizzabilità del materiale probatorio.
L'individuazione dell'istituto probatorio applicabile non è un mero esercizio di stile. Infatti, ciascun istituto probatorio definisce delle regole ben precise riguardo le modalità di assunzione del materiale probatorio, che ne determina anche l'utilizzabilità nel processo (22).
Dunque, il primo aspetto riguarda l'autorità competente ad emettere un O.E.I. volto ad ottenere, si è chiarito, il materiale di intercettazioni svolte all'estero. Su questo punto, infatti, gravitavano altre incertezze giurisprudenziali. Il nodo della questione aveva a che fare con la titolarità del pubblico ministero a richiedere ed ottenere materiali con un potenziale afflittivo nei confronti dell'indagato particolarmente elevato. In effetti, si riteneva fosse sproporzionato e, a tratti anche irragionevole (23), che l'accusa potesse ottenere materiale probatorio dall'estero, che non avrebbe potuto ricercare sul territorio nazionale secondo le regole del codice di procedura penale. L'equivoco è sorto a causa del silenzio della direttiva e, conseguentemente, della legge di implementazione, rispetto alle autorità competenti e alle modalità da seguire nel caso in cui la richiesta contenuta nell'ordine europeo d'indagine abbia a che fare con prove già in possesso dell'autorità di esecuzione (24).
A questo riguardo, le Sezioni Unite hanno chiarito come l'autorità predisposta a richiedere l'acquisizione di conversazioni, captate all'estero per il tramite di un O.E.I. sia il *dominus* dell'indagine penale. Effettivamente, secondo il diritto nazionale, è il pubblico ministero l'autorità competente a richiedere il trasbordo di intercettazioni avvenute in altro procedimento. Una tale soluzione appare in linea con il rispetto della riserva di giurisdizione imposta dall'art. 15 Cost., in quanto l'art. 270 c.p.p. prevede un contraddittorio differito, durante il quale è data alle parti private la possibilità di intervenire sulla selezione dei materiali da far confluire nel procedimento (25).
La norma prevede che i risultati delle attività di intercettazione possano essere utilizzati in un procedimento diverso, qualora queste siano rilevanti ed indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza (26). Inoltre, il comma 2 della disposizione disciplina le regole riguardo l'utilizzabilità dei materiali assunti in questo modo: deve essere dato

(19) A questa soluzione era arrivato anche Spangher, *Criptofonini: sono "in gioco" diritti fondamentali*, in *Cass. pen.*, 2024, 179.

(20) C. eur. dir. umani 5 settembre 2017, *Barbulescu c. Romania*, app. n. 61496/08, 74; più recentemente, in merito a messaggi di testo scambiati sulla piattaforma *telegram*, C. eur. dir. umani 13 febbraio 2024, *Podchasov c. Russia*, app. n. 33696/19, 76.

(21) L'*incipit* della Suprema Corte sul punto è il seguente: «ove si riconosca natura captativa alle comunicazioni effettuate mediante criptofonini, e si accerti che i flussi di comunicazione, al momento in cui tali dati sono stati richiesti dall'Autorità giudiziaria italiana, non erano più in corso, il relativo trasferimento [..]».

(22) Conti, *op. cit.*, 460.

(23) Dinacci, *I modi acquisitivi della messaggistica chat o e-mail: verso letture rispettose dei principi*, in *Arch. pen.*, 2024, 7 ss. L'Autore rileva come in materia di acquisizione dei dati "esteriori" delle conversazioni sia necessaria l'autorizzazione di un giudice. Questa tecnica di indagine è sicuramente meno incisiva dell'assunzione dei contenuti "interiori" delle conversazioni, per le quali, invece, l'autorizzazione non sarebbe richiesta.

(24) Gallo, *Un altro tassello giurisprudenziale in tema di Ordine Europeo d'Indagine penale (OEI) per l'acquisizione della digital evidence dal server estero*, in *Arch. pen.*, 2023, 15.

(25) De Leo, *Vecchio e nuovo in materia di intercettazioni telefoniche riguardanti reati non previsti nel decreto di autorizzazione*, in *Foro it.*, 1989, 26. Sul punto, anche Corte cost. 23 luglio 1991, n. 366, in *Cass. pen.*, 1991, 914.

(26) Art. 270, c. 1, c.p.p., così come modificato dall'art. 1, commi 2-*quater* e 2-*quinquies*, d.l. n. 105 del 2023, convertito con modificazioni dalla l. 9 ottobre 2023, n. 137. Per una approfondita disamina della norma si rimanda a Griffo, *Non c'è pace per l'art. 270: un recente contrasto in ordine ai presupposti di applicabilità della "nuova" disciplina*, in *Arch. pen.*, 2024, 1 ss. Sulla pregnanza del significato di "indispensabilità" si veda Cass. 18 febbraio 2022, n. 5821, in *C.E.D. Cass.*, n. 282804. La Suprema Corte ha ritenuto che «non è necessario che nel provvedimento che utilizza, ai sensi dell'art. 270 cod. proc. pen., i risultati di intercettazioni effettuate in procedimento diverso sia espressamente motivata l'indispensabilità di tali risultati ai fini dell'accertamento dei delitti per cui si procede e per i quali è previsto l'arresto in flagranza, potendo la valutazione di indispensabilità essere compiuta anche implicitamente, mediante l'attribuzione agli elementi utilizzati di specifica rilevanza ai fini della decisione adottata».

avviso ai difensori; i verbali e le registrazioni delle intercettazioni devono essere depositati presso l'autorità procedente; le parti hanno il diritto a consultare i verbali, ad ascoltare i nastri, e ad estrarre copia; è possibile instaurare il contraddittorio nella c.d. udienza di stralcio (27).
Quindi, sarebbe garantito, in questo modo, il coinvolgimento del giudice, anche se *ex post*, nella valutazione degli elementi ottenuti tramite un ordine europeo d'indagine. Non solo, si garantisce alla difesa l'occasione di contestare la rilevanza e la correttezza degli elementi probatori ottenuti. Tuttavia, è il caso di sottolineare che opera in questo contesto l'art. 271 c.p.p., norma speciale che disciplina le regole d'esclusione dei risultati delle intercettazioni. Il divieto di utilizzazione deve intendersi sussistente unicamente quando queste siano state eseguite fuori dai casi consentiti dalla legge e nell'eventualità in cui non siano state rispettate le disposizioni degli artt. 267 e 268, commi 1 e 3 c.p.p. (28). Non costituirebbe, invece, causa di inutilizzabilità l'eventuale violazione dei commi 6, 7 e 8 dell'art. 268 c.p.p., commi che regolano il "contraddittorio differito" in caso di trasbordo di intercettazioni (29).
La prospettata soluzione avrebbe il pregio di fornire maggiori tutele ai soggetti coinvolti e, sembrerebbe, maggiormente aderente al dettato costituzionale e al diritto dell'Unione. Ciononostante, queste maggiori garanzie sembrano comunque non pienamente efficaci. Rimane aperto il dubbio su quali siano le conseguenze del mancato deposito, da parte del pubblico ministero richiedente, dei risultati delle intercettazioni operate all'estero. Il controllo giurisdizionale successivo potrebbe esserne compromesso, lasciando la difesa senza un'occasione effettiva di partecipare al momento acquisitivo del materiale probatorio.

## 3. Le questioni ancora irrisolte

Al netto delle problematiche sopra sollevate, i nuovi approcci giurisprudenziali hanno il merito di aver individuato una strada maggiormente rispettosa dei diritti della difesa. Infatti, anche nella scongiurabile ipotesi in cui venisse a mancare il momento del contraddittorio disciplinato dall'art. 268, comma 6 c.p.p., le difese potrebbero far valere l'inutilizzabilità degli atti assunti tramite O.E.I. in sede di contestazione dell'applicazione di misure cautelari (come è avvenuto nel caso di specie), ovvero nell'atto di formazione del fascicolo per il dibattimento ai sensi dell'art. 431 c.p.p. (30).
Resta, però, da affrontare un tema di centrale importanza: in che modo si declina la possibilità per la difesa di interloquire sulle modalità di acquisizione dei materiali probatori assunti all'estero. Si è detto in precedenza che vi è un velo di mistero sulle modalità con cui sono state svolte le attività di indagine in Francia. Questo comporta che ciò che arriva all'autorità italiana sono conversazioni già decriptate, delle quali non è possibile conoscere le modalità di decriptazione e gli strumenti utilizzati. Ci si chiede, dunque, come una difesa possa rilevare segni concreti di inaffidabilità nel modo in cui sono state condotte le indagini.
A questo interrogativo, la giurisprudenza di legittimità tende a rispondere in modo semplicistico. Infatti, le contestazioni, sollevate sinora dalle difese sulla possibile mancanza di corrispondenza tra le comunicazioni intercettate e quanto trascritto, sono sempre state respinte dalla Corte di Cassazione. A fondamento dei rigetti vi sono principalmente due argomentazioni. In primo luogo, viene richiamato il principio del *mutual trust* (31), su cui si fonda la cooperazione tra Stati membri dell'Unione nell'Area di Libertà, Sicurezza e Giustizia. In virtù di tale principio, i giudici di legittimità ritengono che sussiste una presunzione, ancorché relativa (32), sulla correttezza delle indagini svolte dall'autorità francese. In secondo luogo, viene chiamata in causa la tecnologia con cui sono state ottenute le conversazioni. A più riprese, infatti, la Suprema Corte ha evidenziato che «l'algoritmo che consente la decrittazione dei messaggi non altera il contenuto del dato, essendo nozione acquisita alla scienza informatica che in assenza dell'algoritmo necessario alla decodificazione è impossibile ottenere un testo intellegibile con contenuto in lingua italiana difforme dal reale, potendosi al più avere una sequenza alfanumerica o simbolica priva di alcun senso» (33).

(27) Le definisce «regole d'uso» CORDERO, *Procedura penale9*, Milano, 2012, 856.

(28) Cass. 28 settembre 2005, n. 47331, in C.*E.D. Cass.*, n. 232777.

(29) Cass. 31 luglio 2008, n. 27042, in C.*E.D. Cass.*, n. 240972; Cass. 21 dicembre 2009, n. 48968, in C.*E.D. Cass.*, n. 245542; Cass. 18 gennaio 2016, n. 1801, in C.*E.D. Cass.*, n. 266410.

(30) SPANGHER, *op. cit.*, 178.

(31) Per una disamina del concetto si rimanda a KLIP, *European Criminal Law. An integrative approach4*, Antwerp, 2021, 473 ss; MITSILEGAS, *EU criminal law2*, Oxford, 2022, 196 ss.

(32) MITSILEGAS, *The limits of Mutual Trust in Europe's Area of Freedom, Security and Justice: From Automatic Inter-State Cooperation to the Slow Emergence of the Individual*, in *Yearbook Eur. Law*, 2012, 319 ss; MANCANO, *The Systemic and the Particular in European Law – Judicial Cooperation in Criminal Matters*, in *GLJ*, 2023, 962 ss. Cfr. alla giurisprudenza della Corte di Giustizia dell'Unione Europea che a partire da CGUE 5 aprile 2016, cause riunite C-404/15 e C-695/15 PPU, resa nel caso *Aranyosi and Căldăraru*, in *Dir. pen. e proc.*, 2016, 1240, ha messo in discussione la necessità di avere fiducia "cieca" nei confronti degli ordinamenti giuridici degli Stati membri.

(33) Cfr. Cass. 13 maro 2024, n. 13819, in *Dir. gius.*, 2024. Nello stesso senso, Cass. 13 ottobre 2022, n. 6364, *cit.*

L'impossibilità di accedere ai mezzi investigativi dovrebbe avere delle conseguenze nell'ordinamento interno. Si è di fronte ad una chiara violazione del diritto ad un processo equo, così come tutelato e garantito dalla Costituzione (artt. 24, comma 2 e 111), dalla Conv. eur. dir. umani (art. 6 par. 2) e dalla Carta di Nizza (artt. 47 e 48), in quanto la difesa non è messa nelle condizioni di poter confutare il contenuto degli atti di indagine. Ciò comporterebbe l'applicazione della sanzione della nullità a regime intermedio di cui all'art. 178 comma 1, lett. c) c.p.p. (34). Tuttavia, in termini simili, sarebbe configurabile anche l'inutilizzabilità ai sensi degli artt. 191 e 271 c.p.p., in quanto intercettazioni assunte in violazione dei principi fondamentali dell'ordinamento, come stabilito dall'art. 1, paragrafo 4, dir. UE n. 41 del 2014 e dall'art. 1, d.lgs. n. 108 del 2017 (35).
È anche vero che le ragioni della mancata *discovery* delle modalità d'indagine giacciono nell'esigenza di non disvelare al pubblico mezzi d'indagine particolarmente efficienti, che sono in grado di "bucare" sistemi chiusi come i criptofonini. Andrebbe, dunque, individuato il corretto bilanciamento tra le esigenze di prevenzione e repressione del crimine, specialmente organizzato, e la tutela delle prerogative dei soggetti coinvolti in indagini penali.
Ciò non toglie che, impedire alla difesa di accedere ai dati "grezzi" costituisce un severo *vulnus* ai diritti della difesa. L'importanza di una maggiore tutela non risiede soltanto nell'esigenza di garantire lo svolgimento di un *fair trail*, ma anche di rafforzare la fiducia tra gli Stati e favorire, in questo modo, la circolazione delle prove. L'effettiva tutela delle prerogative della difesa, infatti, costituisce il mezzo principe per promuovere il mutuo riconoscimento tra gli Stati dell'Unione Europea (36).

## 4. Spunti di riflessione alla luce della Sentenza della Corte di Giustizia C-670/22

All'interno dell'evoluzione giurisprudenziale finora prospettata, si inserisce, da ultimo, la Corte di Giustizia dell'UE, con una recentissima decisione su un caso simile (37). Difatti, benché i fatti del giudizio *a quo* riguardano l'assunzione in un procedimento penale, in questo caso tedesco, di conversazioni intercettate sulla piattaforma *Encrochat*, i principi di diritto enunziati dalla CGUE sono traslabili anche ai casi che riguardano *Sky Ecc* (38).
Senza entrare nel dettaglio della decisione dei giudici di Lussemburgo, che esula dallo scopo di questo contributo, è interessante menzionare le soluzioni adottate in merito alle problematiche che sono state sollevate, essendo, potenzialmente, di portata rivoluzionaria. Inoltre, è il caso di ricordare, che le decisioni della Corte hanno efficacia vincolante, diretta e prevalente all'interno dell'ordinamento nazionale (39).
In primo luogo, la Corte ha ritenuto che, ai sensi dell'art. 1, paragrafi 1 e 2, lett. c), dir. UE n. 41 del 2014, autorità competente ad emettere un O.E.I. per l'acquisizione di prove già in possesso delle autorità competenti dello Stato di esecuzione è il pubblico ministero, a condizione che, secondo il diritto dello Stato di emissione, esso sia autorità competente ad ordinare l'acquisizione di dette prove in un procedimento domestico (40). Inoltre, l'autorità inquirente è anche legittimata a richiedere prove che nello Stato di esecuzione siano state acquisite a seguito di intercettazione di telecomunicazioni, sempre sotto la condizione che la pubblica accusa possa esercitare i medesimi poteri in un procedimento puramente interno (41).
In secondo luogo, la CGUE, attraverso un'interpretazione sistematica dell'art. 31, dir. UE n. 41 del 2014, ha elaborato un nuovo concetto autonomo di diritto dell'Unione (42), quello di «intercettazione di telecomunicazioni». Secondo la Corte, in assenza di una definizione esplicita del concetto all'interno della direttiva, e di un rinvio espresso al diritto degli Stati membri, la lacuna va colmata tramite elaborazione giurisprudenziale. Nell'interpretazione fornita dai giudici di Lussemburgo, la formula «intercettazione di telecomunicazioni» non deve ricomprendere unicamente il contenuto delle te-

(34) Lorenzetto, *op. cit.*, 185; Daniele, *Ordine europeo di indagine penale*, cit.

(35) Barbieri, *I limiti di utilizzabilità dei messaggi crittografati scaricati da un server estero ed acquisiti mediante ordine europeo di indagine*, in *Giurisprudenza penale*. Il testo è disponibile al seguente link <https://www.giurisprudenzapenale.com/wp-content/uploads/2023/02/Barbieri_gp_2023_2.pdf>.

(36) Lorenzetto, *I diritti della difesa nelle dinamiche dell'ordine europeo di indagine penale*, in *La nuova cooperazione giudiziaria penale. Dalle modifiche al Codice di Procedura Penale all'Ordine europeo di indagine* a cura di Marchetti e Selvaggi, Milano, 2019, 340.

(37) CGUE 30 aprile 2024, C-670/22, resa nel caso M.N. (*Encrochat*), disponibile su <www.sistemapenale.it>.

(38) Sulle similitudini delle due piattaforme, Daniele, *Ordine europeo di indagine penale*, cit.

(39) Sugli effetti delle pronunce della Corte di Giustizia, cfr. Corte cost. 8 giugno 1984, n. 170, in *Foro it.*, 1984, I, 2062.

(40) CGUE 30 aprile 2024, C-670/22, resa nel caso M.N. (*Encrochat*), para 77, *cit.*

(41) CGUE 30 aprile 2024, C-670/22, resa nel caso M.N. (*Encrochat*), para 106, *cit.*

(42) Per una disamina dell'evoluzione dei concetti autonomi di diritto dell'Unione nell'ambito del diritto penale si veda Mitsilegas, *Autonomous concepts, diversity management and mutual trust in Europe's area of criminal justice*, in *CMLR*, 2020, 45 ss.

lecomunicazioni, ma anche la raccolta dei dati relativi al traffico e all'ubicazione associate a tali telecomunicazioni. Questo implica che l'infiltrazione nelle apparecchiature terminali per estrarre dati di comunicazione, così come informazioni sul traffico o sulla posizione, da servizi di comunicazione basati su Internet, costituisce a tutti gli effetti una intercettazione di telecomunicazioni (43).

Infine, la Corte di Giustizia, pur affermando che non rientra nelle competenze della Corte stessa definire le norme relative all'ammissibilità e alla valutazione di informazioni ed elementi di prova, individua una causa di inutilizzabilità di un mezzo di prova. All'interno di un procedimento penale nazionale, nel quale si è fatto ricorso all'O.E.I., il giudice è tenuto ad escludere dal procedimento ogni informazione ed elemento di prova, che potrebbe influire in modo preponderante sulla valutazione dei fatti, sul quale la persona indagata o accusata non sia stata in grado di svolgere efficacemente le proprie osservazioni (44).

La portata di questa decisione potrebbe essere dirompente. Infatti, la CGUE ha aperto le porte verso la definizione di un diritto probatorio di matrice unionale.

Oltre al potenziale impatto sulle regole probatorie, la Corte sembra aver risolto i dubbi concernenti le conseguenze giuridiche derivanti dal mancato accesso ai dati "grezzi" estratti dalle autorità investigative da parte della difesa. L'impossibilità di accedere ed esaminare le informazioni e le prove raccolte determina un *vulnus* eccessivo ai diritti del prevenuto, tale da giustificare l'espugnazione dal compendio probatorio di quegli elementi.

Dunque, nei processi nazionali, in cui si è fatto ricorso ad un ordine europeo di indagine per ottenere informazioni e prove estrapolate tramite l'impiego di algoritmi secretati, il giudice è tenuto ad escluderle qualora alle difese non sia data la possibilità di analizzare le modalità con cui le prove a loro carico sono state ottenute.

(43) CGUE 30 aprile 2024, C-670/22, resa nel caso M.N. (*Encrochat*), para 113 e 114, *cit.*

(44) CGUE 30 aprile 2024, C-670/22, resa nel caso M.N. (*Encrochat*), 130 e 131, *cit.*

# Accesso abusivo a sistema informatico di interesse pubblico: il punto della cassazione sul caso del P.R.A.

Corte di Cassazione; sezione quinta; sentenza 10 gennaio 2024, n. 1161; Pres. Pezzullo; Rel. Cuoco; con l'intervento del Sost. Proc. Gen. Epidendio.

*L'utilizzo delle credenziali proprie dell'agente e l'assenza di divieti espressi non escludono di per sé il carattere abusivo dell'accesso o del mantenimento nel sistema informatico dell'ufficio, che può comunque essere qualificato "abusivo", quando, pur formalmente corretto, risulti effettuato per finalità estranee a quelle proprie della funzione esercitata.*

*Integra l'aggravante di cui al comma 3 dell'art. 615-ter c.p. l'accesso abusivo al P.R.A. come sistema informatico di interesse pubblico, vista la destinazione di questo sistema informatico al servizio di una collettività indifferenziata e indeterminata di soggetti.*

*...Omissis...*

**Motivi della decisione**

1. Il dato fattuale non è in contestazione: il B.B., nella sua qualità di pubblico ufficiale in servizio presso la sezione di polizia giudiziaria della Procura della Repubblica di Avellino, si è ripetutamente introdotto all'interno del Pubblico Registro Automobilistico, per effettuare ricerche nell'interesse di A.A., suo investigatore, al quale gli esiti venivano comunicati.

2. La Corte territoriale ha ritenuto l'accesso abusivo (in quanto realizzato per una finalità estranea alla funzione svolta in ragione del suo ufficio) e il PRA un servizio d'interesse pubblico.

La difesa del B.B. contesta (con il primo motivo) tale assunto, ritenendo, invece, che l'accesso fosse giustificato dai rapporti professionali esistenti tra il B.B., in servizio presso la Procura della Repubblica di Avellino, e il A.A., suo storico informatore e, quindi, il potere fosse stato esercitato in coerenza con i doveri e gli interessi inerenti all'ufficio ricoperto.

La censura è infondata.

Va premesso che, secondo l'insegnamento delle Sezioni Unite (Sez. U., n. 41210 del 18/05/2017, Savarese, Rv. 271061), l'utilizzo di credenziali proprie dell'agente e l'assenza di espressi divieti, non escludono la possibilità che l'accesso o il mantenimento nel sistema informatico dell'ufficio possa comunque essere qualificato "abusivo", quando, pur formalmente corretto, risulti effettuato per finalità estranee a quelle proprie della funzione esercitata. In altri termini, per giudicare della liceità dell'accesso, occorre aver riguardo non solo alla titolarità astratta del potere esercitato, ma (anche) al suo concreto esercizio e, quindi, alla finalità perseguita dall'agente, che deve essere confacente alla ratio sottesa al potere di accesso. Cosicché, anche in assenza di violazione di specifiche disposizioni regolamentari e organizzative, l'accesso può essere ugualmente abusivo ove si concretizzi in un reale sviamento del potere (Sez. 5, n. 26530 del 17/05/2021, non massimata), che ricorre non solo quando l'attività concreta del pubblico ufficiale sia svolta in contrasto con le norme che regolano l'esercizio del potere, ma anche quando la stessa risulti formalmente corretta, ma orientata alla realizzazione di un interesse collidente con quello per il quale il potere è attribuito (Sez. U, n. 155 del 29/09/2011, Rossi, dep. 2012, Rv. 251498, in tema di abuso d'ufficio).

Parallelamente, il Pubblico Registro Automobilistico, nel quale il B.B. si è introdotto avvalendosi delle sue credenziali, è un registro, nazionale (introdotto con il regio decreto-legge 15 marzo 1927, n. 436, convertito dalla legge 19 febbraio 1928, n. 510), gestito dall'ACI, nel quale vanno registrate tutte le operazioni che riguardano le vicende circolatorie (come, ad esempio, l' immatricolazione, la compravendita, la demolizione, il leasing, i fermi amministrativi o i pignoramenti) o gli elementi identificativi riguardanti un veicolo.

Ebbene, i dati riportati all'interno del registro, coerentemente con la funzione di pubblicità (notizia) svolta dal registro, sono pubblici (attenendo il pagamento del corrispettivo dovuto per l'accesso alla sola gestione economica del servizio), ma l'accesso e la relativa gestione, proprio in ragione della funzione pubblicistica svolta dal registro, è rimesso a soggetti qualificati, in quanto tali titolari del riconosciuto potere di accesso.

Ciò premesso, nella gestione del rapporto con il suo informatore, il ricorrente ha offerto l'accesso al PRA (*rectius*, il mancato pagamento della somma prevista per l'accesso pubblico) a titolo di corrispettivo per le informazioni in precedenza ricevute, acquisendo e comunicando le notizie richieste evitandogli un pagamento.
Ebbene, è pur vero che la figura dell'informatore non è estranea al nostro ordinamento (tant'è che il codice di procedura penale legittima gli ufficiali e gli agenti di polizia giudiziaria a non rivelarne i nomi: art. 203), ma la gestione del (pur legittimo) rapporto con l'informatore non può giustificare, in assenza di una specifica regolamentazione, l'esercizio di un potere e un connesso atto di disposizione delle entrate pubbliche a titolo di corrispettivo per le informazioni dovute.
Cosicché, l'accesso, avvenuto pacificamente nell'interesse del A.A., deve ritenersi abusivo, proprio perché avvenuto per finalità estranee a quelle proprie dell'ufficio.
Su tali premesse, può darsi conto anche dell'infondatezza della connessa censura sollevata dal A.A. ed afferente, per come si è detto, alla sussistenza di una condotta di partecipazione a lui ascrivibile e alla piena consapevolezza del carattere abusivo dell'accesso. Se, infatti, per come si è detto, l'abusività dipende anche dalla finalità per la quale il potere viene esercitato e se, parallelamente, utilizzare il sistema informatico per soddisfare interessi diversi da quelli proprio dell'amministrazione ne sostanzia la condotta, la relativa consapevolezza è ontologicamente presupposta nella stessa richiesta di acquisizione delle informazioni e nella successiva comunicazione dei dati e la richiesta di informazioni, da acquisire nell'interesse privato del richiedente, rappresenta una chiara condotta concorsuale nella successiva esecuzione materiale del reato, che della richiesta ne è l'attuazione.
3. Ugualmente infondate sono, poi, le residue censure (sollevate con il secondo motivo di entrambi i ricorsi) afferenti alla sussistenza in concreto dell'aggravante contestata e alla legittimità della sua contestazione.
Va premesso che non esiste una definizione normativa di "sistema d'interesse pubblico", tant'è che la dottrina, in più occasioni, ha posto l'accento sull' indeterminatezza della fattispecie, diretta a ricomprendere ipotesi non chiaramente definite nella loro perimetrazione.
Ebbene, proprio in ragione del principio di tassatività delle norme penali, fra le varie opzioni ermeneutiche, questa Corte ha aderito a una interpretazione restrittiva, fondata su criteri oggettivi, connessi all'effettivo interesse (pubblico) al quale l'attività (e, con essa, il sistema informatico) è finalizzata, indipendentemente dal soggetto che la espleta o al quale questa è istituzionalmente collegata. Ed in questi termini, quindi, deve leggersi la locuzione: come connessa "alla destinazione del sistema informatico al servizio di una collettività indifferenziata e indeterminata di soggetti" (Sez. 5, n. 24576 del 16/03/2021, Specchiatilo, Rv. 281320).
È pur vero che tutte le precedenti elencazioni sembrano riferirsi alle sole ipotesi in cui emergono le " infrastrutture critiche dello Stato" (traffico aereo, navale o ferroviario, rete elettrica o idrica, ecc.), ma proprio il carattere aperto della previsione (con l' inserimento di una clausola di chiusura) permette d ricomprendere anche attività diverse, esse stesse funzionali al perseguimento di un generale interesse di rilevanza pubblicistica, a prescindere dal carattere riservato dei dati contenuti nel sistema informativo (in sé estraneo alla previsione normativa). Rilevanza della cui sussistenza non può dubitarsi in relazione al registro automobilistico, ontologicamente destinato, proprio in ragione della sua funzione di pubblicità, all'intera collettività.
In ultimo, è pur vero che tale circostanza, presentando innegabili caratteri valutativi, necessita di una chiara esplicitazione nella relativa imputazione (Sez. 5, n. 7541 del 25/11/2021, dep. 2022, Mezzina, Rv. 282982). Ma, in concreto, tale esplicitazione c'è stata, attraverso l'indicazione degli elementi fattuali (il riferimento al registro automobilistico) e normativi (art. 615-ter, comma 3).
La rilevata sussistenza dell'aggravante esclude l'invocato decorso del termine prescrizionale.
4. In conclusione, i ricorsi devono essere rigettati e i ricorrenti condannati al pagamento delle spese processuali....*Omissis...*
8. Tali sono le ragioni per le quali l'ordinanza deve essere annullata, con rinvio per nuovo esame al Tribunale di Bari.
**P.Q.M.**
Rigetta i ricorsi e condanna i ricorrenti al pagamento delle spese processuali.
*...Omissis...*

# IL COMMENTO

*di Simone Tarantino*

**Sommario:** 1. Le questioni sottese al caso di specie. – 2. Sul concetto di abusività dell'accesso e del mantenimento in un sistema informatico o telematico. – 3. La nozione di sistemi informatici o telematici di interesse pubblico. – 4. Brevi riflessioni conclusive.

La Cassazione ribadisce i limiti del potere d'accesso – e di mantenimento – del pubblico ufficiale in un sistema informatico o telematico, precisando altresì la nozione di interesse pubblico del sistema, che aggrava la condotta dell'agente.
L'accesso ad un sistema informatico o telematico è abusivo, quando è finalizzato al raggiungimento di un interesse collidente con quello per cui il titolo è invece lecitamente attribuito.
Pertanto, l'accesso al P.R.A, quale sistema informatico di interesse pubblico, naturalmente destinato al servizio di una collettività indifferenziata ed indeterminata di soggetti, integra l'aggravante di cui al comma 3 dell'art. 615-*ter* c.p.

*The Italian Supreme Court reiterates the limits of the public official's power to access – and maintain the said access – a computer or telematic system. It also specifies the concept of public interest of the system, which aggravates the agent's conduct.*
*The access to a computer or telematic system by a public official is illicit when it is aimed at the achievement of an interest that is colliding with the one for which the title is instead lawfully conferred.*
*Therefore, this access to the P.R.A. (Public Vehicle Register), as it is a computer system of public interest, in view of the fact that this computer system is naturally destined to serve an undifferentiated and indefinite group of people, constitutes the aggravating circumstance referred to in paragraph 3 of Article 615-ter of the Criminal Code.*

## 1. Le questioni sottese al caso di specie

La pronuncia *de qua* del Supremo Collegio suscita particolare interesse poiché torna ad affrontare due nodi interpretativi di cruciale rilevanza, già consolidati in materia di accesso abusivo a sistemi informatici o telematici, riaffermando gli insegnamenti, dottrinali e giurisprudenziali, tanto in punto di abusività dell'accesso da parte di un pubblico ufficiale, quanto in punto di interesse pubblico qualificato del sistema stesso nell'aggravante prevista dal terzo comma dell'art. 615-*ter* c.p.
L'art. 615-*ter* è stato topograficamente collocato nel libro secondo del Codice penale ed annoverato tra i «*delitti contro la inviolabilità del domicilio*» con la l. del 23 dicembre 1993, n. 547 che, in tema di criminalità informatica, ha dato attuazione alla c.d. "*lista minima obbligatoria*" in ossequio alla Raccomandazione del Consiglio d'Europa n° 9/1989, che esortava gli Stati ad introdurre incriminazioni penali per contrastare fatti commessi a mezzo computer.
Tale delitto punisce, al primo comma, la condotta di «*chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero ivi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo*».
L'innesto normativo ha tradotto nella sfera immateriale e telematica il disvalore sociale del delitto di violazione di domicilio, di cui all'art. 614 c.p. A partire da questo, il legislatore ha trasposto, nel sistema informatico o telematico, la condotta tipica alternativa di «*introduzione abusiva o di mantenimento*» contro la volontà del titolare dello *ius excludendi*, apprestando così tutela al nuovo bene giuridico, denominato «*domicilio informatico*». Esso viene inteso come spazio ideale (anche fisico) comprensivo dei dati informatici di pertinenza della sfera individuale della persona, che assurgono al rango – per la prima volta – di bene giuridico costituzionalmente protetto (1).
Tanto brevemente premesso, e venendo al caso di specie, ai ricorrenti veniva contestata l'ipotesi aggravata prevista dal comma terzo dell'art. 615-*ter* c.p., identificata quale tipizzazione dell'accesso abusivo commesso a danno di un sistema di «*interesse militare*» relativo «*all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico*», commesso da un «*pubblico ufficiale, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio*».
I ricorsi innanzi alla Suprema Corte sono stati proposti dagli imputati a censura della sentenza della Corte d'Appello, che li aveva condannati, accertando la loro penale responsabilità, per aver commesso il delitto di accesso abusivo *ex* art. 615-*ter* c.p., aggravato ai sensi del suo comma terzo alla luce della connotazione pubblica del Pubblico Registro Automobilistico, in concorso tra loro: l'uno, quale informatore della Polizia Giudiziaria,

(1) Cass. 04 ottobre 1999, n. 3067; Cass. 04 ottobre 1999, n. 3065. Per un approfondimento dottrinale si veda: Picotti, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di Internet*, a cura di Picotti, Padova, 2004, 21 ss.; Flor, *Riservatezza informatica e sicurezza informatica quali nuovi beni giuridici penalmente protetti*, in *Mobilità, sicurezza e nuove frontiere tecnologiche* a cura di Militello e Spena, Torino, 2018, 463 ss.

nelle vesti di istigatore dell'azione delittuosa; l'altro, quale pubblico ufficiale in servizio presso la Sezione di Polizia Giudiziaria della Procura della Repubblica di Avellino, nelle vesti di materiale esecutore dell'azione delittuosa.

Le difese degli imputati, proponendo ricorsi paralleli per questo non dissimili nei contenuti, hanno dedotto, *in primis*, l'insussistenza dell'elemento oggettivo del reato in oggetto, quindi il carattere dell'abusività dell'accesso effettuato dal pubblico ufficiale.

A parere dei ricorrenti, posto che il carattere di abusività dell'accesso poteva ritenersi integrato solo ove la condotta si fosse concretizzata nello sviamento di un potere, preordinato a raggiungere un fine non istituzionale, la comunicazione delle risultanze estratte dal Pubblico Registro – e derivate dall'accesso al relativo sistema – al proprio informatore non avrebbe potuto qualificarsi come abusiva, inserendosi piuttosto nel loro rapporto di carattere professionale, a conferma di una prassi consolidata ed invalsa negli ambienti di polizia giudiziaria.

Secondo l'assunto della difesa, l'accesso operato dal pubblico ufficiale, che deteneva legittimamente le credenziali d'accesso al sistema, non avrebbe potuto essere qualificato come abusivo, e dunque non avrebbe potuto ritenersi sussistente l'elemento costitutivo del reato. Pertanto, la sentenza resa dalla Corte d'Appello doveva essere annullata.

*In secundis*, con il secondo motivo, le difese dei ricorrenti hanno contestato la sussistenza della circostanza aggravante del comma terzo del predetto articolo, deducendo l'ontologica incompatibilità fra l'applicazione della *ratio* sottesa all'interpretazione della norma – ovvero la tutela degli archivi telematici che contengono informazioni riservate – e la funzione di pubblicità (notizia) propria del Pubblico Registro Automobilistico, al cui interno è possibile consultare tutte le informazioni afferenti le vicende circolatorie dei veicoli registrati.

Allo stesso modo, hanno sostenuto le difese, non avrebbe potuto darsi valore alla controprestazione richiesta dal sistema per accedervi – ovvero al pagamento di una somma di denaro a titolo di contributo per l'accesso al registro stesso – perché afferente unicamente alla sola gestione economica del servizio. Anche il capo d'imputazione, quindi, formulato in termini valutativi, non avrebbe esplicitato gli elementi fattuali in forza dei quali il sistema che si assumeva violato avrebbe dovuto essere qualificato nei termini prospettati, destituendo di fondamento ogni contestazione in fatto.

Espunta la configurazione della circostanza aggravante, infine, ne avrebbe dovuto conseguire la declaratoria di estinzione del reato, per decorso del massimo termine prescrizionale.

Tuttavia, i motivi di doglianza dei ricorrenti non hanno trovato accoglimento per le seguenti ragioni.

## 2. Sul concetto di abusività dell'accesso e del mantenimento in un sistema informatico o telematico

In via preliminare, è opportuno perimetrare la condotta tipica del reato in commento, ovvero quella alternativa di «*accesso o mantenimento*» (2), al fine di meglio comprendere quanto affermato dalla Suprema Corte nella relativa pronuncia.

In maniera sintetica, è integrata la condotta attiva di «*accesso*» dell'agente, quando si instauri un dialogo logico (o automatizzato) con la parte *software* del sistema informatico bersaglio (3), che non può consistere in un mero "entrare in contatto con il sistema", ma che deve tradursi nell'assunzione del controllo dello stesso da parte dell'attaccante, tramite una serie di comandi, sì da avere accesso alle informazioni ivi contenute (4), a nulla rilevando né le finalità soggettivamente perseguite dall'agente, né l'uso successivo dei dati raccolti, condotta che può invece eventualmente integrare una diversa fattispecie di reato (5).

Alternativamente, il reato parimenti si consuma quando l'agente è responsabile della condotta omissiva di «*mantenimento*» (6) in un sistema informatico o telematico; condotta, questa, che si colloca successivamente all'avvenuta introduzione legittima nello spazio informatico protetto e che si sostanzia in una "permanenza" illecita che travalica i limiti per cui l'accesso era stato inizialmente autorizzato (7).

---

(2) Per un ampio approfondimento si rimanda ai contributi di Salvadori, *I reati contro la riservatezza informatica*, in *Cybercrime*, diretto da Cadoppi, Canestrari, Manna, Papa, II, Milano, 2023, 704 ss.; Flor, *La condotta del pubblico ufficiale fra violazione della voluntas domini, "abuso" dei profili autorizzativi e "sviamento di potere"*, in *Dir. pen. e proc.*, 2018, 506 ss.; Salvadori, *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in *Tutela penale della persona e nuove tecnologie*, a cura di Picotti, Padova, 2013, 125 ss.

(3) Perri, *Analisi informatico-giuridica dei reati di frode informatica e accesso abusivo a un sistema informatico o telematico con l'aggravante dell'abuso della qualità di operatore di sistema*, in *Giur. merito*, 2008, 161 ss.

(4) A titolo esemplificativo, basti pensare ad un *hacker* che, tramite un *malware* scaricato nel computer della vittima, infetti il sistema bersaglio e riesca ad introdursi in esso, avendo così accesso a tutti i dati ivi presenti.

(5) Cass. 25 giugno 2009, n. 40078; Cass. 07 novembre 2000, n. 12732.

(6) Picotti - Flor - Salvadori, *Riservatezza e sicurezza informatica, identità digitale*, in *La riforma dei delitti contro la persona*, a cura di Associazione italiana dei professori di diritto penale - DiPLaP, 2023, con relativa *Relazione di accompagnamento*; nonché gli *Atti del Seminario di discussione* (Verona, 10 settembre 2021), ed ivi in specie Lamanuzzi, *Sulla proposta di riforma del delitto di accesso abusivo ad un sistema informatico o telematico*, all'indirizzo <www.aipdp.it/allegato_prodotti/225_AIPDP-DIPLAP_Riforma_reati_contro_la_persona_a_cura_di_AIPDP-DIPLAP.pdf>.

(7) A titolo esemplificativo, basti pensare ad un soggetto che, autorizzato ad intervenire in un sistema per curare dei malfunzionamenti, una

La condotta di accesso, e comunque anche di trattenimento nel sistema – sebbene caratterizzata dalla meno sintetica locuzione: «*contro la volontà espressa o tacita*» di chi detiene lo *ius excludendi* –, per rientrare nell'alveo del penalmente rilevante dev'essere posta in essere «*abusivamente*», poiché, in assenza di questa connotazione, la condotta, di per sé neutra, non presenta alcuna autonoma carica offensiva.

L'abusività va, quindi, ricondotta al momento dell'introduzione o della permanenza, perché nelle condotte commesse dall'agente il disvalore penale va ravvisato nella mancanza di autorizzazione o nella contrarietà rispetto alla volontà del titolare dello *ius excludendi alios*.

Inizialmente, un primo orientamento giurisprudenziale aveva attribuito rilevanza al solo accesso (o al relativo mantenimento) ad un sistema informatico o telematico commesso da un soggetto che, pur se privo di autorizzazioni, divenisse capace di introdursi e carpire successivamente dati ed informazioni, nonostante l'accesso ai dati sensibili nei sistemi non fosse una condizione necessaria per la consumazione del reato stesso.

Successivamente, l'alveo del penalmente rilevante è stato ampliato, tanto da ricondurre all'applicazione del delitto in questione le condotte dei c.d. *insiders*: trattasi di soggetti abilitati all'accesso che, utilizzando un titolo formale (come una chiave di accesso) legittimamente detenuto, si introducono o si mantengono in un sistema informatico o telematico, contravvenendo alle disposizioni del titolare dei poteri di esclusione, allo scopo di realizzare finalità estranee a quelle del proprio ufficio (8).

Secondo questo filone giurisprudenziale, l'agente si serve di un titolo legittimante l'accesso per perseguire finalità estranee a quelle rispetto alle quali l'accesso è consentito: è da questa circostanza che veniva desunto il contrasto con la *voluntas domini* del titolare del sistema stesso (9).

Tale interpretazione giurisprudenziale, tuttavia, sottendeva l'estensione del concetto di abusività. Esso veniva colto sia nel risultato immediato della condotta di introduzione dell'agente, sia in quei fatti commessi *successivamente* all'accesso stesso, che, seppur dal primo già previsti al momento di inserimento delle credenziali per introdursi nel sistema, richiedono ulteriori atti volitivi autonomi per realizzarsi (10).

Il contrasto giurisprudenziale è stato poi risolto dalle Sezioni Unite Casani, con la sentenza in cui si è ritenuto configurato il reato in analisi esclusivamente in presenza di: i) un accesso non autorizzato; ii) un accesso autorizzato, ma posto in essere in violazione dei limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema; iii) un accesso autorizzato, quando l'autore realizzi operazioni di natura ontologicamente diversa da quelle rispetto alle quali egli è incaricato ed in relazione alle quali l'accesso era a lui consentito (11).

La corretta applicazione dei principi fin qui delineati ha incontrato alcuni problemi interpretativi in relazione alla circostanza aggravante del fatto commesso da un funzionario pubblico con «*abuso dei poteri*» o con «*violazione dei doveri*» inerenti alla propria funzione, estromettendo la valutazione sugli scopi effettivamente perseguiti dall'agente.

La condotta delittuosa, infatti, rilevante per la consumazione dell'aggravante del comma secondo n.1 dell'art. 615-*ter* c.p., onde evitare di ritenere delittuoso il mero accesso o mantenimento del pubblico ufficiale, è stata ricondotta ad un parametro oggettivo o normativo – per questo *extra*-penale –, da individuarsi nell'insieme di leggi, disposizioni e regolamenti, anche interni dati dal titolare, che disciplinano i poteri di accesso ai sistemi della pubblica amministrazione. Così facendo, è integrata l'ipotesi delittuosa da parte di un pubblico ufficiale o di un incaricato di pubblico servizio quando l'agente abbia agito travalicando i poteri ed abbia ecceduto i limiti autorizzativi del proprio operato, sanciti dal titolare del sistema, dalla specifica disposizione di legge o dal regolamento funzionale dell'ufficio a cui l'attività è preposta (12).

Dunque, nel caso di soggetto autorizzato, a rilevare è il dato oggettivo dell'accesso e del trattenimento nel sistema informatico, laddove effettuato in violazione dei limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema, ovvero tramite operazioni di natura diversa da quelle di cui egli sia incaricato e per le quali gli sia, pertanto, stato consentito l'accesso. Irrilevanti, e dunque escluse dall'area del divieto penale,

volta terminata questa attività vi si mantenga per visionare i diversi contenuti ivi presenti.

(8) Cass. 07 novembre 2000, n. 1675.

(9) Cass. 08 luglio 2008, n. 37322; Cass. 10 dicembre 2009, n. 2987; Cass. 16 febbraio 2010, n. 19463; Cass. 22 settembre 2010, n. 39620.

(10) Salvadori, *L'accesso abusivo ad un sistema informatico o telematico. una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, opp. cit.

(11) Cass. Sez. Un. 27 ottobre 2011, n. 4694, Casani, che ha affermato il seguente principio di diritto: "integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615-*ter* cod. pen., la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso. Non hanno rilievo, invece, per la configurazione del resto, gli scopi e te finalità che soggettivamente hanno motivato l'ingresso al sistema".

(12) Cass. 31 ottobre 2014, n. 1008; Cass. 26 giugno 2015, n. 44403; Cass. 26 ottobre 2016, n. 14546; Cass. 05 dicembre 2016, n. 11994.

erano invece le finalità che abbiano spinto il pubblico ufficiale all'esecuzione della condotta criminosa.
Ma tale assunto giurisprudenziale non è andato esente da critiche.
L'analisi concreta della formulazione normativa, cui doveva far riscontro la necessità di punire anche ulteriori e diverse condotte esorbitanti da tale alveo criminoso, ha condotto a riflettere sul concetto di sviamento del potere (13).
Questa figura, ripresa dal diritto amministrativo quale conformazione sintomatica del vizio di un provvedimento amministrativo (ovvero l'eccesso di potere), evoca l'operato del soggetto abilitato che, pur eseguendo l'accesso in un sistema informatico utilizzando il proprio titolo autorizzativo, lecitamente detenuto, e ivi mantenendosi senza violare le prescrizioni formali impartite dal suo titolare o da una specifica normativa in materia, agisca al fine di realizzare attività ontologicamente estranee alle finalità istituzionali per cui il rapporto funzionale è instaurato.
In ragione del rapporto funzionale instaurato dal pubblico ufficiale (e dall'incaricato di pubblico servizio) discendono poteri autoritativi, deliberativi o certificativi, i quali devono essere conformati ai principi di buon andamento ed imparzialità della pubblica amministrazione: per cui l'esecuzione di qualsiasi comportamento che si ponga in contrasto con essi, manifesta una «*ontologica incompatibilità*» dell'accesso al sistema, connaturata da un utilizzo dello stesso estraneo alla *ratio* del conferimento del potere (14).
È su questa ultima ipotesi che la sentenza in commento ha condotto la propria analisi e poi fondato la sua decisione.
La questione, di particolare rilievo, è stata trattata dalla pronuncia delle Sezioni Unite della Corte di Cassazione, nella nota sentenza Savarese (15), che ha definitivamente ritenuto abusivo l'accesso al sistema (o il suo mantenimento) dell'*intraneus,* pubblico ufficiale abilitato all'accesso (o al mantenimento) da credenziali formalmente lecite, anche in assenza di divieti espressi e pur senza violazione di specifiche disposizioni normative, quando l'accesso stesso risulti effettuato per finalità estranee, e comunque aliene, rispetto a quelle proprie della funzione esercitata.
In altri termini, la Corte ritiene che, per giudicare la liceità dell'accesso, sia necessario aver riguardo non solo alla titolarità astratta del potere esercitato, ma anche al suo concreto e fattuale esercizio, inscindibile dalle finalità perseguite dall'agente, che devono essere confacenti alla *ratio* sottesa al titolo legittimante il potere di accesso.
Da ciò consegue che può indifferentemente essere definito come abusivo l'accesso anche ove si concretizzi un mero sviamento del potere, realizzabile non solo quando l'attività dell'*intraneus,* pubblico ufficiale, sia svolta in patente violazione di norme (direttive o regolamenti, anche interni) che ne limitino l'esercizio, ma anche quando questa, seppur formalmente lecita, sia esercitata per la realizzazione di un interesse alieno rispetto a quello sotteso alla funzione svolta (16).
Il dato fattuale della vicenda, per quanto non sottoposto (né comunque sottoponibile) allo scrutinio dei giudici di legittimità, era tuttavia eloquente: un pubblico ufficiale, in servizio presso la Sezione di Polizia Giudiziaria della Procura della Repubblica di Avellino, si era ripetutamente introdotto all'interno del Pubblico Registro Automobilistico, sfruttando il suo titolo, formalmente detenuto per le funzioni esercitate, con lo scopo di effettuare delle ricerche, ed estrarre delle informazioni, nell'interesse specifico, ed unico, del suo informatore.
Il Pubblico Registro Automobilistico (17), nel quale il pubblico ufficiale si era introdotto abusivamente, è un registro nazionale gestito dall'Automobile Club Italia, nel quale vanno registrate tutte le operazioni che riguardano le vicende circolatorie o gli elementi identificativi riguardanti un veicolo.
I dati riportati all'interno del Registro sono pubblici, attenendo il pagamento del corrispettivo dovuto alla sola gestione economica del servizio, ma l'accesso e la relativa gestione, proprio in ragione della funzione pubblicistica svolta dal Registro, sono rimessi a soggetti qualificati, titolari del riconosciuto potere, come era l'agente nel caso di specie.

(13) Flor, *La condotta del pubblico ufficiale fra violazione della voluntas domini, "abuso" dei profili autorizzativi e "sviamento di potere*", opp. cit.

(14) *Ibid.*

(15) Cass. Sez. Un. 08 settembre 2017, n. 41210, Savarese, che ha affermato il seguente granitico principio di diritto: "Integra il delitto previsto dall'art. 615-*ter*, comma 2, n. 1, c.p., la condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso (nella specie Registro delle notizie di reato: Re.Ge.), acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, gli è attribuitala facoltà di accesso".

(16) Cass. Sez. Un. 10 gennaio 2012, n. 155, Rossi, in tema di abuso d'ufficio, la quale ha affermato che: "Ai fini della configurabilità del reato di abuso d'ufficio, sussiste il requisito della violazione di legge non solo quando la condotta del pubblico ufficiale sia svolta in contrasto con le norme che regolano l'esercizio del potere, ma anche quando la stessa risulti orientata alla sola realizzazione di un interesse collidente con quello per il quale il potere è attribuito, realizzandosi in tale ipotesi il vizio dello sviamento di potere, che integra la violazione di legge poiché lo stesso non viene esercitato secondo lo schema normativo che ne legittima l'attribuzione".

(17) Istituito con il r.d-l. n. 436 del 15 marzo 1927, denominato "*Disciplina dei contratti di compra vendita degli autoveicoli ed istituzione del pubblico registro automobilistico presso le sedi dell'Automobile Club d'Italia*", con il r.d. del 29 luglio 1927, n. 1814 ne fu approvato il regolamento di attuazione ed attualmente è affidato in gestione all'Automobile Club d'Italia.

Questi, tuttavia, ha specificamente offerto il proprio potere d'accesso al Pubblico Registro quale controprestazione, *rectius* corrispettivo, all'informatore per le precedenti confidenze rese nel corso del loro rapporto professionale, da cui è conseguito per l'istigatore un netto risparmio di spese.
Ebbene, nonostante sia innegabile l'esistenza nel nostro ordinamento della figura dell'informatore (18), quale persona in grado di riferire alla Polizia giudiziaria notizie di interesse strategico per le investigazioni, l'esistenza del rapporto professionale non può giustificare l'esercizio di un potere ed un connesso atto di disposizione delle entrate pubbliche come controprestazione dell'attività da esso svolta, contrarie alle disposizioni pubbliche.
Di conseguenza, integrato l'elemento oggettivo del reato, l'accesso è stato ritenuto abusivo, proprio in quanto preordinato a perseguire finalità estranee a quelle proprie dell'ufficio e delle funzioni esercitate dall'agente, in quanto afferenti unicamente agli interessi privati dell'informatore, *de visu* manifestando la specifica violazione dei principi di imparzialità e buon andamento della Pubblica amministrazione, certificati nell'art. 97 della Costituzione.

## 3. La nozione di sistemi informatici o telematici di interesse pubblico

Resta, dunque, da verificare la sussistenza o meno dell'aggravante prevista dal comma terzo, che è integrata qualora bersaglio delle condotte di accesso o mantenimento dell'agente sia un sistema informatico o telematico di «*interesse pubblico*».
L'art. 615-*ter* c.p., al suo comma terzo, infatti, prevede una specifica circostanza aggravante ad effetto speciale, che punisce in modo sensibilmente severo le condotte previste ai commi primo e secondo (rispettivamente con pene da uno a cinque anni e da tre a otto anni), qualora queste abbiano ad oggetto sistemi di carattere militare, afferenti all'ordine pubblico o comunque alla sicurezza pubblica.
Nella formulazione di tale previsione la dottrina ha ravvisato un evidente difetto di determinatezza (19), non essendo chiari i criteri in base ai quali attribuire la connotazione pubblicistica al sistema. Tuttavia, traspare in modo evidente l'intenzione del legislatore di tutelare infrastrutture informatiche delicate per l'ecosistema statale info-telematico: soprattutto tale disposizione è posta a presidio della riservatezza dei dati contenuti negli archivi digitali, del loro corretto funzionamento e della loro indisturbata fruizione per la collettività.
Come spesso accade, alle lacune del legislatore ha sopperito la giurisprudenza (20), la quale ha adottato un'interpretazione restrittiva – fatta propria dalla Corte anche nella pronuncia in commento –, che ha ravvisato l'integrazione della nozione di «*interesse pubblico*», qualora il sistema sia destinato al servizio di una collettività indifferenziata ed indeterminata di soggetti.
Prescindendo dalla qualifica soggettiva del titolare del sistema stesso, l'obiettivo, e comunque la finalità perseguita dall'effettiva infrastruttura, dev'essere il soddisfacimento di bisogni generali della collettività (21).
All'interno di questa categoria, seppur certamente aperta, rientrano i sistemi afferenti alle "*infrastrutture strategiche dello Stato*", come per la logistica quelle afferenti al traffico aereo, navale o ferroviario, prossimamente anche le *smart roads (22)* per le *self-driving cars (23),* oppure

(18) Per una disamina dell'argomento, confronta in dottrina Pisani, *Informatori, notizie confidenziali e segreto di polizia*, Milano, 2007, 1 ss.; nonché in giurisprudenza: Cass. 12 giugno 2001, n. 36720, la quale ha affermato il seguente principio di diritto: "Gli informatori della polizia o dei servizi segreti sono i confidenti della polizia o dei servizi, che – di regola dietro compensi in denaro o in vista di altri vantaggi – forniscono loro occasionalmente, ma con sistematicità, notizie riservate. Non rientra in questa figura, né può essere ad essa assimilata, la persona informata dei fatti che rifiuti di formalizzare le sue dichiarazioni e di sottoscrivere un verbale, e cui pertanto non sono applicabili le disposizioni contenute nel predetto art. 203 c.p.p.".

(19) Pecorella, *Commento all'art. 615-ter c.p.*, in *Codice penale commentato*, a cura di Dolcini e Gatta, V, Milano, 2021, 2051 ss.

(20) Cass. 16 marzo 2021, n. 24576, la quale ha affermato il seguente principio di diritto: "In tema di accesso abusivo ad un sistema informatico, ai fini della configurabilità dell'aggravante di cui all'art. 615-ter, comma terzo, cod. pen., sono "di interesse pubblico" solo i sistemi informatici o telematici di pubblica utilità, ossia destinati al servizio di una collettività indifferenziata e indeterminata di soggetti, e non anche quelli a vario titolo riconducibili all'esercizio di diritti, pur di rilevanza collettiva, costituzionalmente tutelati".

(21) Cass. 13 dicembre 2010, n. 1934.

(22) Anas, Gruppo FS italiane, all'indirizzo <https://www.stradeanas.it/it/smartroad>: per *smart roads* si intende quelle strade *intelligenti* in grado di comunicare in modo continuo con i sistemi a bordo delle autovetture a guida autonoma, individuando rallentamenti nella mobilità del percorso programmato, pericoli rappresentati da sinistri appena realizzatisi, lavori di potenziamento sulle linee, per cui sussiste la possibilità di essere informati in tempo reale sulle deviazioni consigliate o l'imminenza di condizioni metereologiche avverse. In caso di sinistri stradali, grazie ai servizi di geolocalizzazione delle vetture, nonché di comunicazione continua con le forze pubbliche, sarà possibile ricevere assistenza immediata per qualsivoglia necessità. Individuata l'interconnessione come punto focale tramite le reti ultraveloci e l'I. o. T., la comunicazione sarà bidirezionale: non solo l'utente potrà essere avvisato di eventuali problemi nella viabilità stradale, ma potrà egli stesso comunicare eventuali problematiche intercorrenti all'esterno, ma anche all'interno nell'abitacolo o nella vettura stessa, ampliando così la possibilità di un intervento tempestivo atto a risolvere le criticità che si manifestino.
Nel nostro ordinamento, vedasi il d.m. del 28 febbraio 2018: *modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni di smart road e di guida connessa e automatica*.

(23) Le cui implicazioni, anche penalistiche, vengono ampiamente dissertate in: Cassano - Picotti, *Veicoli a guida autonoma. Veicoli a impatto zero. Regole, intelligenza artificiale, responsabilità,* Pisa, 2023, 1 ss.; Picotti, *Profili di responsabilità penale per la circolazione di veicoli a guida autonoma*, in *Studi in onore di Antonio Fiorella* a cura di Catenacci - D'Ascola - Rampio-

le infrastrutture della rete elettrica, idrica ed energetica; ma anche (grazie al richiamo della clausola di chiusura prevista dal comma terzo) più in generale qualunque sistema con cui si intendano perseguire finalità di rilevanza pubblicistica.
Da ciò consegue l'indubbia qualifica di «*sistema pubblico*» del P.R.A., il quale racchiude in sé una funzione di pubblicità notizia, che consente ad ognuno di aver accesso alle vicende circolatorie (o eventuali garanzie delle obbligazioni) legate alle proprietà dei beni mobili registrati.
Nonostante la formulazione aperta della norma in esame, nel caso di specie la rilevanza pubblicistica del P.R.A. è stata correttamente esplicitata nel capo d'imputazione sia attraverso l'esplicazione degli elementi fattuali rilevanti, sia attraverso la sussunzione di questi nell'art. 615-*ter* comma terzo c.p.
Alla luce di queste considerazioni, pertanto, la Corte ha ritenuto sussistente l'aggravante prevista dal comma terzo dell'art. 615-*ter* c.p. nelle condotte degli imputati, escludendo il decorso del termine prescrizionale del reato, per cui ha rigettato i ricorsi degli stessi, condannandoli al pagamento delle spese processuali.

## 4. Brevi riflessioni conclusive

La sentenza in esame si pone, come detto, nel solco della pronuncia delle Sezioni Unite Savarese in tema di accesso abusivo dell'*intraneus,* pubblico ufficiale, che parametra l'antigiuridicità della condotta allo svolgimento di attività finalizzate al perseguimento di obiettivi diametralmente opposti, e comunque estranei, a quelli preordinati alla funzione e all'ufficio che svolge.
È chiaro l'intento giurisprudenziale, perseguito invero dalle diverse pronunce che si sono inanellate negli ultimi decenni, di meglio tipizzare e formalizzare le condotte penalmente rilevanti del reato in oggetto, che ha imposto sforzi interpretativi nell'individuazione dei limiti del lecito dall'illecito.
Se, inizialmente, ad essere rilevante era solo la condotta dell'*hacker* esterno che accedeva abusivamente al sistema informatico o telematico, successivamente è stato riconosciuto disvalore penale anche alle condotte dell'*insider* che utilizzi in modo abnorme i propri poteri, violando le disposizioni interne (o i regolamenti) del titolare del sistema, per poi pervenire alla criminalizzazione anche delle condotte di coloro che, nonostante non violino specifiche direttive interne, pongano in essere atti incompatibili con le funzioni ed i poteri attribuiti.
È fondamentale tenere a mente, tuttavia, che la condotta materiale di mero "*accesso o mantenimento*", di per sé, è una condotta neutra, mentre è proprio il carattere oggettivo dell'abusività (e del conseguente mantenimento contro la *voluntas domini*) a connotarne la potenzialità lesiva rispetto al bene giuridico tutelato: la riservatezza del c.d. domicilio informatico. Un'analisi sulle finalità in concreto perseguite dall'agente non può che fungere da perno per l'analisi delle condotte commesse dallo stesso.
Inoltre, quando il sistema bersaglio abbia natura afferente all'ordine pubblico, e comunque alla pubblica sicurezza, appare evidente la necessità dell'ordinamento di rendere la risposta punitiva più rigorosa, proprio a tutela dell'ordine costituzionale, dei suoi principi fondamentali e del corretto andamento delle infrastrutture critiche dello Stato; ragion per cui si giustifica non solo un inasprimento sanzionatorio, ma anche l'adozione di accorgimenti tecnici funzionali a salvaguardarne l'utilità e gli obiettivi.
Con il progredire della tecnologia, in un futuro tutt'altro che remoto, i sistemi informatici, normalmente soggetti alle insidie poste dalle condotte umane, dovranno necessariamente rapportarsi anche con le capacità computazionali dei nuovi sistemi di intelligenza artificiale (quali, ad esempio, i *Large Language Models* come ChatGPT) ormai capaci di hackerare autonomamente siti *web* e di carpire i contenuti delle e-mail, i dati sanitari, bancari, accedere ai *cloud online*, sottrarre password e chiavi d'accesso dei sistemi, travalicando le misure di sicurezza apposte, senza più l'intervento materiale dell'uomo-agente.
Gli attacchi cibernetici ai sistemi telematici si sono moltiplicati, ciò grazie all'uso dei nuovi *software* informatici, in misura vistosa nel corso dello scorso anno (24). Oggi più che mai è assolutamente indispensabile investire in strumenti di *cybersecurity* (25) che siano in grado di gestire e limitare il rischio insito nell'uso dei sistemi telematici.
Gli sviluppi e le potenzialità che i nuovi *software* mostrano quotidianamente di possedere porteranno la giurisprudenza a dover analizzare anche il loro utilizzo all'in-

ni, I, Roma, 2021, 813 ss.; Cappellini, *Profili penalistici delle self-driving cars,* in *Dir. pen. cont.*, 2019, 325 ss.. Per uno sguardo all'esperienza francese, vedasi: Marotta, *La Francia avvia ufficialmente la legislazione sulla guida autonoma,* in questa ***Rivista***, 2021, all'indirizzo <https://dirittodiinternet.it/la-francia-avvia-ufficialmente-la-legislazione-sulla-guida-autonoma/>. In ambito civile, vedasi Pellegatta, *Guida autonoma e prime riflessioni in punta di diritto,* in questa ***Rivista***, 2019, 25 ss.

(24) Il Rapporto Clusit 2024 sulla Sicurezza ICT in Italia, del marzo 2024, offre una panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale (Italia inclusa) nel 2023, che, come anticipato, sono in forte crescita rispetto al 2022 (+12%), all'indirizzo <https://clusit.it/rapporto-clusit/>.

(25) In materia penale, vedasi: Flor, *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad protection ai più recenti sviluppi,* in questa ***Rivista***, 2019, 453 ss.; in materia civile, vedasi: Cassano - Iaselli - Spangher, *Cybersecurity: contesto normativo di riferimento a livello nazionale ed europeo*, in questa ***Rivista***, 2022, 637 ss.

terno della condotta tipica dell'agente, quale strumento facilitatore dell'offesa o mezzo tramite il quale essa si esplica, che può usufruire delle capacità computazionali degli stessi per violare le misure di sicurezza ed accedere abusivamente ai sistemi, eventualmente contribuendo alla delimitazione delle condotte lecite, da quelle, invece, illecite.

# Nozione (restrittiva) di "privata dimora" fra captazioni di immagini e gps dotati di microfono

CORTE DI CASSAZIONE; sezione quinta; sentenza 5 dicembre 2023, n. 4840; Pres. Zaza; Rel. Stanislao; P.M. Giordano.

*Non è consentita, neppure al convivente, la captazione di immagini di vita privata altrui (Massima non ufficiale).*

*...Omissis...*

**Ritenuto in fatto**

1. Con ordinanza del 17 luglio 2023, il Tribunale di Roma, sezione per il riesame delle misure cautelari reali, confermava il decreto del Gip del locale Tribunale con il quale si era disposto il sequestro preventivo di un impianto di registrazione di immagini installato nella propria abitazione dall'indagato C.G. (costituito da tre mini telecamere inserite negli alloggi del sistema di allarme e da una centralina di registrazione) mediante il quale erano state tratte immagini della vita privata della convivente e dei figli, in assenza dell'indagato coabitante, così, pertanto, configurandosi, secondo i giudici della cautela reale, il *fumus* del delitto di cui all'art. 615 *bis* cod. pen. in tema di "*interferenze illecite nella vita privata*". La condotta contestata si era inserita in una più ampia contesa fra C.G. e la moglie in allora con lui convivente, Z.E. dalla quale erano scaturite reciproche denunce per maltrattamenti (anche a danno dei figli minori della coppia) e per lesioni personali. 1.1. Il Tribunale, in risposta ai dedotti motivi di gravame, osservava quanto segue. La Z.E. aveva denunciato di essersi accorta delle registrazioni, solo a seguito della loro visione avvenuta a fine settembre 2022, in quanto allegate alla controdenuncia sporta nei suoi confronti dal C.G. così deducendo la presenza del ricordato impianto di ripresa installato (o fatto installare) dal medesimo, a sua insaputa, nella comune abitazione. Aveva così disposto una bonifica dell'abitazione, a seguito della quale, il 1 ottobre 2022, erano state rinvenute le tre videocamere in sequestro e, in un mobile della sala, l'impianto di registrazione delle immagini, anche esso sottoposto al vincolo reale. Le videocamere erano state inserite all'interno dei sensori del sistema di allarme (già da tempo in funzione ed a lei noto). Il consulente tecnico incaricato dal pubblico ministero, a seguito della denuncia della Z.E. aveva confermato la presenza del sistema di registrazione, già rilevato dai tecnici della medesima. Il Tribunale aveva ritenuto, come si è detto, che si fosse concretato il *fumus* del contestato delitto, l'art. 615 *bis* cod. pen., posto che, secondo questa Corte di legittimità, lo stesso si configura anche nel caso in cui sia uno dei conviventi nell'abitazione ad aver installato un sistema di ripresa – di immagini e suoni – destinato però a registrare, in sua assenza, gli atti della vita privata degli altri conviventi (Cass. 36109/2018). Né le diverse conversazioni registrate, dall'indagato, e intercorse fra questi e Z.E. nel maggio del 2022, consentivano di affermare, come assunto dal suo difensore, che la donna fosse al corrente dell'installazione delle videocamere, posto che, dalle frasi proferite, poteva solo dedursi che ella fosse consapevole delle possibili registrazioni dell'ingresso nell'abitazione di estranei, meramente accessorie, pertanto, all'entrata in funzione del sistema di allarme antifurto. Generica era poi la doglianza, della difesa del prevenuto, circa la possibile manomissione del sistema ad opera della Z.E. o di chi, per lei, aveva effettuato la ricordata bonifica, dal momento in cui C.G. si era allontanato dalla comune abitazione. Né poteva configurarsi la scriminante dell'articolo 54 cod. pen., posto che il prevenuto, se avesse temuto per l'incolumità dei figli minori, avrebbe ben potuto, e dovuto, rivolgersi all'autorità inquirente. 2. Propone ricorso l'imputato, a mezzo dei suoi difensori, Avv.ti V.P. e G.M.G. che hanno sottoscritto distinti atti di impugnazione. 2.1. L'Avv. P. articola due motivi di ricorso. 2.1. Con il primo motivo deduce la violazione di legge, ed in particolare degli artt. 360 e 391 *decies* cod. pen., ed il vizio di motivazione. Ricorda, innanzitutto, che: l'accusa si era fondata sugli accertamenti effettuati dal consulente del pubblico ministero nel febbraio 2023 (dopo che la persona offesa era già intervenuta sul sistema di allarme ed era stata fatta una bonifica, rispettivamente il 30 settembre ed il 1 ottobre 2022); la crisi della coppia datava al febbraio 2022; nel marzo 2022, la persona offesa aveva sporto denuncia per un episodio di lesioni patite dal C.G. in epoca recente e per altri episodi, molto risalenti nel tempo; da aprile 2022, C.G. aveva scoperto una serie di

condotte incongrue della Z.E., fra queste, degli episodi di maltrattamento a danno dei figli, e aveva sporto conseguente querela; le ulteriori integrazioni di denuncia da parte del C.G. avrebbero dovuto far comprendere alla Z.E. come egli avesse installato, in casa, delle videocamere; nel giugno 2022, la Z.E. aveva presentato ricorso per la regolamentazione della responsabilità genitoriale e si era riportata alla sua precedente denuncia; C.G. l'aveva denunciata per calunnia; nel settembre 2022, C.G. aveva depositato ulteriore documentazione, ivi comprese le riprese colte con le videocamere installate, e il 29 settembre ed il 1 ottobre, la Z.E. aveva, prima, staccato i fili delle telecamere e, poi, fatto bonificare l'intero appartamento; nel corso delle indagini preliminari per il presente delitto, il pubblico ministero aveva incaricato un consulente per la verifica di quanto dalla Z.E. denunciato; a fine ottobre 2022, la Z.E. con i figli minori della coppia, erano stati collocati presso una casa famiglia e l'indagato C.G. aveva abbandonato l'abitazione. Se ne deduce, allora, come fosse viziato l'accertamento operato dal consulente del pubblico ministero, nel febbraio 2023, visto che era avvenuto quando le videocamere erano già state scollegate e, quindi, manomesse dalla persona offesa e dai tecnici di sua fiducia. Il vizio era anche processuale posto che l'accertamento, effettuato ai sensi dell'art. 360 cod. proc. pen., non era stato operato nel contraddittorio delle parti (nessuno avviso era stato fatto al C.G., che, come si è detto, era mutato lo stato dei luoghi e che lo stesso non era affatto irripetibile). Peraltro, nello stesso atto del pubblico ministero di conferimento dell'incarico, era stato indicato un nome, tale F.F. del tutto estraneo ai fatti. Identiche censure erano state formulate con l'atto di riesame ma non avevano ottenuto congrua confutazione. 2.2. Con il secondo motivo lamenta la violazione di legge, ed in particolare dell'art. 615 *bis* cod. pen., ed il difetto di motivazione. Le videoriprese avevano consentito di acclarare la consumazione del delitto di maltrattamenti e, invece, con il loro sequestro, se n'era determinato l'inutilizzabilità (anche a tal fine, la prova del delitto di cui all'art. 572 cod. pen.). Si sarebbe, invece, dovuto considerare quanto affermato dalla Cassazione nella sentenza 25453 del 2011, ove si era precisato che non poteva ritenersi indebita l'intrusione nella vita personale visto che la stessa era stata determinata da una ragione lecita: l'intento, appunto, di raccogliere elementi di prova in ordine alla condotta abusante (con percosse e mortificazioni) della Z.E. a danno dei figli minori, di 11 e 7 anni, all'epoca dei fatti. Prove che, difatti, erano state immediatamente poste all'attenzione del pubblico ministero. Né poteva condividersi quanto affermato dal Tribunale in ordine al fatto che l'installazione delle videocamere avrebbe potuto essere demandata alle autorità, posto che le condotte illecite erano emerse solo dalla visione dei filmati, così che la loro preventiva denuncia non avrebbe potuto essere sporta. Si doveva poi ricordare che, quanto al delitto di cui all'articolo 615 *bis* cod. pen., lo stesso non si configura quando le immagini siano captate dal *dominus loci* (Cass. 27160/2018, 14253/2017); e quando il soggetto ritratto ne sia consapevole (come emerge, per la Z.E. dalle conversazioni con il prevenuto del 22 e del 30 maggio 2022). 2.2. L'Avv. G. deduce, con l'unico motivo di ricorso, la violazione di legge con riferimento alla ritenuta sussistenza del *fumus commissi delicti* sia sotto il profilo oggettivo, sia sotto l'aspetto soggettivo. Quanto le videocamere erano state installate, C.G. viveva all'interno del medesimo appartamento, così da doversi escludere la configurabilità della condotta vietata dall'articolo 615 *bis* cod. pen., alla luce del la giurisprudenza di legittimità (Cass., n. 27160/2018). Diversamente da quanto affermato dal Tribunale, poi, le conversazioni, registrate nel maggio 2022 e parimenti prodotte dal C.G. dimostravano con certezza che la Z.E. era consapevole della presenza delle telecamere, tanto da averne fatto preciso riferimento. E tanto che i due avevano discusso anche dell'opportunità di installarne di più grandi. La centralina, poi, ove le immagini restavano registrate, era perfettamente visibile. Né si poteva affermare che la Z.E. fosse consapevole del loro utilizzo in relazione al solo sistema d'allarme. Nella sentenza della Cassazione n. 14253/2017 si era precisato che il giudizio sulla illiceità della installazione, perché non a conoscenza dei conviventi, doveva trarsi considerando tutte le deduzioni della difesa a tal proposito, come, invece, il Tribunale non aveva fatto. Nel provvedimento impugnato, poi, nulla si era argomentato in ordine all'elemento soggettivo del reato: le videocamere erano collocate solo negli ambienti comuni (corridoio, sala, cucina), C.G. ne aveva parlato con la Z.E. e C.G. stesso aveva già denunciato alle autorità le ipotizzate condotte abusanti della donna.

*...Omissis...*

**Considerato in diritto**

Il ricorso (complessivamente proposto dai due difensori) promosso nell'interesse dell'indagato non merita accoglimento. 1. Le censure relative alla ritenuta sussistenza del *fumus* del contestato reato sono infondate. L'art. 615 *bis* cod. pen. punisce "*Chiunque mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni*". Dalla stessa lettera della norma si deduce che l'oggetto della protezione sono le immagini della vita privata altrui, riprese all'interno del domicilio. La questione che si è posta – e che si pone nell'odierno giudizio cautelare – è se possa configurarsi il reato nei confronti di chi abbia il libero accesso al domicilio all'interno del quale erano avvenute le riprese,

in quanto convivente, a qualsiasi titolo, con la persona offesa i cui atti di vita privata erano stati registrati. Così delimitata la questione, appare evidente come questa Corte abbia costantemente ritenuto che non sia consentita, neppure al convivente, la registrazione di immagini di vita privata altrui, quando lo stesso non ne sia stato parte, posto che, solo in tale ultima evenienza l'atto di vita privata appartiene anche a chi l'abbia registrato (non diversamente, per altro, dalla registrazione di comunicazioni di cui chi registra sia uno degli interlocutori: vd. Sez. U, n. 36747 del 28/05/2003, Torcasio, Rv. 225466 ove si precisa che la registrazione fonografica di conversazioni o comunicazioni realizzata, anche clandestinamente, da soggetto partecipe di dette comunicazioni, o comunque autorizzato ad assistervi, costituisce prova documentale, e quindi pienamente utilizzabile, del fatto; un orientamento confermato da ultimo Sez. 2, n. 40148 del 06/07/2022, Acanfora, Rv. 283977). È quanto del resto affermano le seguenti pronunce, in cui si è precisato che: integra il reato di interferenze illecite nella vita privata di cui all'art. 615 *bis* cod. pen. la condotta di colui che, mediante l'uso di strumenti di captazione visiva o sonora, all'interno della propria dimora, carpisca immagini o notizie attinenti alla vita privata di altri soggetti che vi si trovino, siano essi stabili conviventi o ospiti occasionali, senza esservi in alcun modo partecipe; ne consegue che detto reato non è configurabile allorché l'autore della condotta condivida con i medesimi soggetti e con il loro consenso l'atto della vita privata oggetto di captazione (Sez. 5, n. 36109 del 14/05/2018, C., Rv. 273598); non integra il delitto di interferenze in illecite nella vita privata la condotta di colui che, ammesso ad accedere nell'abitazione del coniuge separato, provvede a filmare, senza consenso, gli incontri tra quest'ultimo e il figlio minore, in quanto l'art. 615 *bis*, cod. pen., che tutela la riservatezza domiciliare, sanziona la condotta di chi risulti estraneo agli atti – oggetto di captazione – di vita privata, ossia agli atti o vicende della persona in luogo riservato e non quella di chi sia stato ammesso, sia pure estemporaneamente, a farne parte (Sez. 5, n. 24848 del 17/05/2023, N. Rv. 284871). 1. 2. Quanto poi all'eventuale consenso, implicito o esplicito, alle riprese delle scene di vita privata, che parimenti escluderebbe la ricorrenza del reato (come si evince dalle citate sentenze), nel caso di specie risulta essere priva di manifesti vizi logici l'affermazione del Tribunale secondo il quale le frasi altrimenti captate dal prevenuto non costituiscono, affatto, la prova della consapevolezza della persona offesa di essere registrata all'interno dell'abitazione, posto che, dalle medesime, invece, si deduce soltanto che ella riteneva che le stesse costituissero un accessorio dell'impianto di allarme e che, pertanto, entrassero in azione solo a seguito delle eventuali intrusioni dall'esterno. 1.3. Priva di fondamento è anche la censura relativa all'accertamento della presenza delle videocamere all'interno delle placche del sistema di allarme (precedentemente ed autonomamente installato). E ciò per una pluralità di ragioni: neppure il prevenuto, o i suoi difensori, negano che sia stato lo stesso indagato ad aggiungere al sistema di allarme, le videocamere rivenute ed il sistema di registrazione; l'attività del consulente del pubblico ministero si è limitata alla verifica della loro presenza, e, comunque, anche considerando quanto si è rilevato (circa la pacificità della loro installazione ad opera dell'indagato), la difesa, nel sollecitare la declaratoria di inutilizzabilità della verifica del consulente, non ne argomenta la decisività (Sez. 4, n. 18232 del 12/04/2016, Madafferi, Rv. 266644 in cui si ricorda come l'ordinanza applicativa di misure cautelari, pur se formalmente viziata da inosservanza di norme processuali stabilite a pena di inutilizzabilità, in tanto va annullata in quanto si accerti che la fonte di prova illegittimamente indicata e utilizzata ha avuto una efficacia determinante nella formazione del convincimento del giudice del merito cautelare). Né, sempre alla luce di quanto altrimenti provato, sono stati individuati elementi concreti che consentano di ritenere che la persona offesa abbia modificato lo stato dei luoghi così inquinando la prova. Come priva di rilievo appare la citazione, nel contesto della decisione, del nome di una persona estranea ai fatti, circostanza che, al più, costituirebbe un mero errore materiale.

*...Omissis...*

P.Q.M.

Rigetta il ricorso e condanna il ricorrente al pagamento delle spese processuali.

*...Omissis...*

CORTE DI CASSAZIONE; sezione quinta; sentenza 26 ottobre 2023, n. 3446; Pres. Sabeone; Rel. Cirillo; P.M. Passafiume.

*In tema di delitti contro la persona, non integra il reato di interferenze illecite nella vita privata la condotta di chi installi nell'autovettura di altro soggetto un dispositivo GPS dotato di microfono che gli consenta di ascoltare le conversazioni che si svolgono all'interno del veicolo.*

*...Omissis...*

**Ritenuto in fatto**

1. Con sentenza emessa il 18 maggio 2022, il Tribunale di Taranto, all'esito di giudizio abbreviato, aveva condannato S.G. per il reato di cui all'art. 615-*bis* cod. pen., alla pena di sei mesi di reclusione e al risarcimento del danno subito dalla parte civile. Secondo l'impostazione accusatoria, ritenuta fondata dal giudice di primo grado, l'imputato si sarebbe procurato indebitamente le notizie attinenti alla vita privata dell'ex moglie, mediante l'utilizzo di un dispositivo GPS dotato di microfono, che aveva installato all'interno dell'autovettura di quest'ultima e che gli consentiva di ascoltare le conversazioni intervenute all'interno del veicolo. Con sentenza emessa il 24 aprile 2023, la Corte di appello di Lecce – Sezione distaccata di Taranto – ha riformato la sentenza di primo grado, assolvendo l'imputato perché il fatto non sussiste e revocando le statuizioni civili. 2. Avverso la sentenza della Corte di appello, l'imputato ha proposto ricorso per cassazione a mezzo del proprio difensore. 2.1. Con un unico motivo, deduce il vizio di erronea applicazione della legge penale, in relazione all'art. 615-*bis* cod. pen. Il ricorrente rappresenta che la Corte di appello ha assolto l'imputato poiché ha escluso che l'autoveicolo, all'interno del quale era stato occultato il dispositivo GPS, potesse costituire un luogo di privata dimora. Tanto premesso, il ricorrente contesta tale decisione, sostenendo che la giurisprudenza più recente avrebbe recepito una nozione più ampia del concetto di privata dimora e, con specifico riferimento al reato di cui all'art. 615-*bis* cod. pen., avrebbe espressamente ritenuto rilevante, al fine della configurazione del reato, l'installazione di una microspia all'interno di un'automobile. Nel caso in esame, l'autovettura della persona offesa andrebbe sicuramente ritenuta quale luogo di privata dimora, atteso che all'interno di essa la vittima intratteneva colloqui non solo personali, ma anche di carattere professionale, legati all'attività di avvocato, svolta dalla medesima.

*...Omissis...*

**Considerato in diritto**

1. Il ricorso deve essere rigettato. 1.1. L'unico motivo di ricorso è infondato. L'abitacolo di un'autovettura, in quanto spazio destinato naturalmente al trasporto dell'uomo o al trasferimento di oggetti da un posto all'altro e non ad abitazione, non può essere considerato luogo di privata dimora, salvo che, a differenza di quanto dedotto nel caso in esame e desumibile dal contenuto del provvedimento impugnato, esso, sin dall'origine, sia strutturato (e venga di fatto utilizzato) come tale, oppure sia destinato, in difformità dalla sua naturale funzione, ad uso di privata abitazione (cfr. Sez. 1, n. 3363 del 18/10/2000, Galli, Rv. 218042; Sez. 6, n. 5934 del 19/02/1981, Semitaio, Rv. 149373). Con specifico riferimento alla fattispecie di cui all'art. 615-*bis* cod. pen., questa Corte, in relazione a un fatto analogo a quello contestato, ha già affermato un principio pienamente condiviso da questo collegio, secondo il quale «non integra il reato di interferenze illecite nella vita privata (art. 615-*bis* cod. pen.) la condotta di colui che installi nell'auto di un soggetto (nella specie ex fidanzata) un telefono cellulare, con suoneria disattivata e con impostata la funzione di risposta automatica, in modo da consentire la ripresa sonora di quanto accada nella predetta auto, in quanto, oggetto della tutela di cui all'art. 615-*bis* è la riservatezza della persona in rapporto ai luoghi indicati nell'art. 614 cod. pen. – richiamato dall'art. 615-*bis* – tra i quali non rientra l'autovettura che si trovi sulla pubblica via» (Sez. 5, n. 28251 del 06/03/2009, Pagano, Rv. 244196).

*...Omissis...*

P.Q.M.

Rigetta il ricorso e condanna la ricorrente al pagamento delle spese processuali.

*...Omissis...*

# IL COMMENTO

*di Sara Angioni*

**Sommario:** 1. Il "rigoroso ossequio al limite testuale". – 1.1. Le vicende controverse. – 1.1.1. La ripresa (solo privata) di immagini all'interno del domicilio integra il fatto tipico. – 1.1.2. L'autovettura non costituisce un luogo di "privata dimora". – 2. La nozione di "privata dimora" nel diritto penale sostanziale: tra interpretazione restrittiva ed estensiva. – 2.1. Interpretazione restrittiva: i tre "indefettibili elementi". – 2.2. Un recente orientamento interpretativo estensivo. – 3. Un caso difficile: il problema dell'abitacolo dell'autovettura. – 4. La sentenza di legittimità relativa all'abitacolo delle autovetture: un esito non scontato. – 4.1. Due pronunce a confronto: un "contrasto giurisprudenziale sincronico" o un *overruling* definitivo? – 5. Il significato di "privata dimora" nel settore delle intercettazioni *inter preasentes* – 5.1. La posizione restrittiva della giurisprudenza di legittimità: la nozione di "privata dimora" tra diritto sostanziale e diritto processuale.

Le due decisioni in commento sono inerenti al delitto di interferenze illecite nella vita privata, di cui all'articolo 615 *bis* c.p. Il presente lavoro propone una riflessione sulla *quaestio* relativa all'interpretazione del concetto di "privata dimora". Con tali pronunce, la Corte di cassazione sembra aver accolto nuovamente, in materia sostanziale, l'orientamento che predilige l'utilizzo del criterio testuale, conforme ai limiti che l'interpretazione deve rispettare in materia penale. Tuttavia, ciò non esclude che l'interpretazione estensiva possa ripresentarsi, soprattutto per la risoluzione dei casi più "difficili". Un'esegesi restrittiva del concetto è, invece, quasi sempre, accolta dalla Corte nel settore delle intercettazioni e, più in generale, in ambito processuale.

*The two decisions in comment are related to the crime of unlawful interference with private life, referred to in Article 615 bis of the Criminal code. This paper presents a reflection on the quaestio regarding the interpretation of the concept of "private dwelling." With these rulings, the Court of cassation seems to have once again embraced, in substantive matters, the orientation that prefers the use of the textual criterion, which conforms to the limits that interpretation has to respect in the criminal sector. However, this does not preclude the possibility that extensive interpretation may recur, especially for the resolution of more "difficult" cases. A restrictive exegesis of the concept is, instead, almost always accepted by the Court in the field of wiretapping and, more generally, in the procedural sphere.*

## 1. Il "rigoroso ossequio al limite testuale"

Con le due sentenze in commento, la Quinta Sezione Penale della Corte di cassazione si è di nuovo espressa sull'interpretazione dell'articolo 615-*bis* c.p., e, nello specifico, sul c.d. delitto di indiscrezione di cui al primo comma. (1)

Nonostante la diversa composizione del collegio giudicante, in entrambi i casi la Corte ha confermato l'orientamento maggioritario, di carattere restrittivo, relativo all'interpretazione del concetto di "privata dimora" nella fattispecie di interferenze illecite nella vita privata (2). Al fine di risolvere due vicende di diversa complessità, infatti, la Corte ha adottato un'interpretazione letterale della norma (3), escludendo il reato in questione,

(1) Per un'analisi puntuale della norma si veda Palazzo, *Considerazioni in tema di tutela della riservatezza (a proposito del nuovo articolo 615 bis c.p.)*, in *Riv. it. dir. e proc. pen.*, 1975, 126 ss. Analogamente, si rinvia anche a Scalisi, *Diritto alla riservatezza. Il diritto all'immagine, il diritto al segreto, la tutela dei dati personali, il diritto alle vicende della vita privata, gli strumenti di tutela*, Milano, 2002, 335 ss.; Antolisei, *Manuale di diritto penale, Parte Speciale*, Vol. I, Milano, 2008, 242 ss.; Notaro, *I delitti contro l'inviolabilità e la riservatezza del domicilio (Artt. 614 - 615 quinquies)*, in *Trattato di diritto penale - Parte speciale Vol. IX/ I delitti contro la libertà sessuale, la libertà morale, l'inviolabilità del domicilio e l'inviolabilità dei segreti*, a cura di Manna, Papa, Canestrari, Cadoppi, Milano, 2011, 470 ss. L'art. 1, l. n. 98 del 1974 ("Tutela della riservatezza e della libertà e segretezza delle comunicazioni") ha introdotto significativamente la norma citata nel Libro II, Sezione IV, rubricata "Dei delitti contro la inviolabilità del domicilio" del Codice penale. Questa legge fu una delle sei presentate in Parlamento in seguito ai diversi scandali emersi in materia di intercettazioni e in considerazione delle fonti internazionali. Per completezza, si veda la Scheda dei lavori preparatori, disponibile all'indirizzo <https://legislature.camera.it/_dati/leg06/lavori/schedela/trovaschedacamera.asp?pdl=1482||>. Oggetto della tutela penale è la "vita privata", limitatamente all'acquisizione di "notizie o immagini" attinenti alla stessa entro i luoghi di cui all'art 614 c.p., come messo in evidenza da Patrono, voce *Privacy*, in *Enc. dir.*, XXXV, Milano, 1986, 570 ss. A differenza dell'articolo 614 c.p., posto a tutela della violazione fisica del domicilio, l'articolo 615 *bis* c.p. si pone come guarentigia della riservatezza (domiciliare). A questo proposito è bene consultare Bricola, *Prospettive e limiti della tutela penale della riservatezza*, in id., *Diritto alla riservatezza e la sua tutela penale*, Milano, 1970, 82, 88, 122; Mantovani, *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in *Arch. giur.*, 1968, 50 ss.; Zancani, *La nozione di uso di strumenti di ripresa visiva e sonora nel reato di interferenze illecite nella vita privata,* in *Ind. pen.,* 2001, 1405 ss.

(2) Da ultimo, si veda Trib. Reggio Emilia, sez. GIP/GUP, 9 novembre 2021, n. 528, in cui si è escluso, proprio in considerazione del tenore testuale della norma, che si possa configurare il reato in questione nella *toilette* di una discoteca. A proposito, si rinvia a Beccari, *Le prime difficolta applicative nella nuova fattispecie di "revenge porn" in caso di diffusione del materiale da parte di soggetti estranei al rapporto sessuale*, in *Sist. Pen.*, 2022, 5 ss.

(3) Sulla riscoperta della testualità, si deve vedere Corte cost., 14 maggio 2021, n. 98, in *Giur. cost.*, 2021, 1797 ss. e i relativi commenti: Cupelli, *Divieto di analogia in malam partem e limiti dell'interpretazione in materia penale: spunti dalla sentenza 98 del 2021*, in *Giur. cost.*, 2021, 1807 ss.; Palazzo, *Costituzione e divieto di analogia*, in *Dir. pen. proc.*, 2021, 1218 ss.; Manes, *Introduzione ai principi costituzionali in materia penale*, Torino, 2023, 81 ss. Nello stesso senso cfr., più di recente, anche Cupelli, *Tentazioni e contraddizioni del sistema penale contemporaneo: creazionismo giudiziario, panpenalismo legislativo e caccia al colpevole*, in *Cass. pen.*, 2023, 693 ss.

qualora la condotta di indebito procacciamento delle immagini di vita privata non si fosse concretizzata "nei luoghi indicati nell'articolo 614" (4), ossia nei luoghi di "privata dimora".
Dall'analisi della giurisprudenza in materia, su cui più diffusamente nel prosieguo, si può ben osservare quanto sia problematica questa nozione, quanti sforzi siano serviti al giudice di legittimità per adattare, di volta in volta, la fattispecie al caso concreto.

### *1.1. Le vicende controverse*

È opportuno, anzitutto, descrivere le vicende oggetto delle sentenze in commento così da considerare l'applicazione del criterio di interpretazione letterale a due casi di differente complessità. Da subito, si evince che il primo caso sia di "facile" risoluzione: un comportamento realizzato in uno di quei luoghi – il domicilio – che inequivocabilmente si inquadrano nella categoria della "privata dimora". Lo stesso non è possibile affermare in merito al secondo contesto, chiaramente più "difficile", giacché lo spazio fisico – l'automobile – in cui sono state captate le informazioni private risulta essere, in alcune circostanze, di dubbia classificazione.

#### 1.1.1. La ripresa (solo privata) di immagini all'interno del domicilio integra il fatto tipico

La sentenza più recente descrive, invero, un caso piuttosto lineare (5). Rigettando il ricorso proposto, la Corte di cassazione avvalora la precedente ordinanza, in cui il Tribunale di Roma confermava il sequestro preventivo di un supporto di registrazione audiovisiva predisposto nella abitazione dall'indagato (6). Nel caso di specie, in un contesto di intensa lite familiare fra i coniugi, il soggetto sottoposto ad indagine aveva posto in funzione un impianto – costituito da tre mini videocamere inserite nel sistema di allarme e una centralina di registrazione di immagini collocata in un mobile della sala – atto a captare scene della vita privata della moglie e dei figli. Tali momenti di quotidianità erano stati filmati all'insaputa della consorte (7); in alcuni frammenti, i due coniugi erano ripresi insieme mentre in altri neppure era presente l'indagato (8). Per tali ragioni, la Corte ha condiviso il punto di vista adottato dal Giudice per le indagini preliminari, rilevando "il *fumus* del delitto di cui all'art. 615 *bis* cod. pen." e sottolineando che "[d]alla stessa lettera della norma si deduce che l'oggetto della protezione sono le immagini della vita privata altrui, riprese all'interno del domicilio" (9).

#### 1.1.2. L'autovettura non costituisce un luogo di "privata dimora"

Anche con riferimento alla più articolata vicenda affrontata nella decisione più risalente (10), la Corte di legittimità, in linea con quanto affermato dai giudici di merito, "ha escluso che l'autoveicolo, all'interno del quale era stato occultato il dispositivo GPS, potesse costituire un luogo di privata dimora" (11). In particolare, avverso la sentenza di condanna di *prime cure*, la stessa ricorrente lamentava il fatto che l'ex marito fosse, tramite queste modalità, venuto a conoscenza di notizie concernenti non solo la sua vita personale, ma anche quella lavorativa, dal momento che questa era solita intrattenere in auto conversazioni riguardanti la propria professione. Nell'adottare questa soluzione, i giudici di legittimità hanno richiamato la sentenza *Pagano* in base

(4) Il primo comma dell'articolo 615 *bis* c.p., infatti, recita: "[c]hiunque, mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni".

(5) Cass., sez. V, 5 dicembre 2023, n. 4840. Sulla stessa, si veda anche Conti, *Videoriprese di persone conviventi: quando integrano il reato previsto dall'art. 615-bis c.p.?*, in *Il Quot. giur.*, 2024, consultabile all'indirizzo <https://www.altalex.com/documents/2024/02/13/videoriprese-persone-conviventi-integrano-reato-previsto-art-615-bis-c-p>.

(6) Cass., sez. V, 5 dicembre 2023, n. 4840, Ritenuto in fatto, paragrafo 1.

(7) Come emerge proprio dal contenuto delle "frasi proferite", la donna prende consapevolezza di questa macchina di registrazione, solo nel momento in cui le immagini così captate vengono allegate ad una denuncia sporta dall'ex marito nei suoi confronti.

(8) Sebbene il *focus* del presente lavoro non sia il seguente, si nota comunque che, come anche messo in evidenza dalla difesa, a discolpa del soggetto condannato, si sarebbe potuto considerare il fatto che il delitto non venga in essere nel caso in cui le immagini siano riprese dal *dominus loci* (come stabilito in Cass., sez. V, 13 giugno 2018, n. 27160 e Cass., sez. VI, 23 marzo 2017, n. 14253) o nell'ipotesi in cui, come sottolineato dalla stessa Corte, l'autore - convivente delle registrazioni sia anche egli parte delle scene di vita privata captate, che in questo senso gli appartengono (Cass., SU, 28 maggio 2003, n. 36747, *Torcasio*, in *Dir. pen. proc.*, 2004, 67). Infatti, l'elemento della terzietà deve ricorrere perché si possa effettivamente concretizzare la fattispecie (di questo avviso Cass., sez. V, 8 novembre 2006, n. 39827, in *Riv. pen.*, 2007, 264). Tuttavia, la Sezione V rifiuta del tutto questa possibile via interpretativa, richiamando alcuni precedenti in materia (quali, Cass., sez. V, 14 maggio 2018, n. 36109, C. Rv. 273598 e Cass., sez. V, 17 maggio 2023, n. 24848, N. Rv. 284871) e chiarendo che "non sia consentita, neppure al convivente, la registrazione di immagini di vita privata altrui quando lo stesso non ne sia stato parte". Tale conclusione è assolutamente condivisibile poiché il soggetto è comunque condannabile per le scene di vita filmate in cui sia totalmente assente.

(9) Cass., sez. V, 5 dicembre 2023, n. 4840, Considerato in diritto, paragrafo 1.

(10) Cass., sez. V, 26 ottobre 2023, n. 3446. Sulla stessa, si veda anche Ievolella, *"Cimice" nella vettura dell'avvocata ex moglie: impossibile parlare di interferenze illecite nella vita privata della donna*, in *Dir. giust.*, 2024, 6; Cerqua, *GPS nell'autovettura della dell'ex moglie: quale tutela penale della privacy?*, in *Il Quot. giur.*, 2024, disponibile all'indirizzo <https://www.altalex.com/documents/2024/03/19/gps-autovettura-ex-moglie-tutela-penale-privacy>.

(11) Cass., sez. V, 26 ottobre 2023, n. 3446, Ritenuto in fatto, paragrafo 2.1.

alla quale: "non integra il reato di interferenze illecite nella vita privata (art. 615-*bis* cod. pen.) la condotta di colui che installi nell'auto di un soggetto (nella specie ex fidanzata) un telefono cellulare, con suoneria disattivata e con impostata la funzione di risposta automatica, in modo da consentire la ripresa sonora di quanto accada nella predetta auto, in quanto, oggetto della tutela di cui all'art. 615-*bis* è la riservatezza della persona in rapporto ai luoghi indicati nell'art. 614 cod. pen. – richiamato dall'art. 615-*bis* – tra i quali non rientra l'autovettura che si trovi sulla pubblica via" (12). In questo modo è stato ribadito il principio di diritto già enunciato in precedenza secondo cui "[l]'abitacolo di un'autovettura (...) non può essere considerato luogo di privata dimora" (13). Sebbene sia ineccepibile nella sua risoluzione, quest'ultimo caso offre diversi spunti di riflessione, di cui si dirà più diffusamente nel prosieguo.

## 2. La nozione di "privata dimora" nel diritto penale sostanziale: tra interpretazione restrittiva ed estensiva

Per meglio comprendere le vicende giudiziarie in esame, è utile passare in rassegna la ricca giurisprudenza di legittimità in materia. Si evince, invero, un "contrasto giurisprudenziale sincronico" (14) di particolare rilievo. Un primo indirizzo ermeneutico fornisce una nozione restrittiva di "privata dimora", intrinsecamente connessa alla lettera della legge. Il secondo, invece, estende la portata applicativa dell'enunciato giuridico fino a ricomprendere diverse sottofattispecie, a cui nondimeno il dettato normativo non fa espresso riferimento. Questa dicotomia interpretativa è essenziale per comprendere i più recenti approdi della Corte di ultima istanza, come si andrà a considerare nei paragrafi che seguono.

### *2.1. Interpretazione restrittiva: i tre "indefettibili elementi"*

Per inquadrare la questione, è utile spendere qualche ulteriore riflessione in prospettiva sistematica. La locuzione "privata dimora" si ritrova, infatti, in molteplici disposizioni normative, a carattere sia sostanziale che processuale (15). Nello specifico, sulla base della lettera dell'articolo 614 c.p. e dell'articolo 624-*bis* c.p. (16), la suddetta espressione è da intendersi come termine "ombrello" (*open-textured*) (17), volto a ricomprendere, inequivocabilmente, e l'abitazione e le pertinenze (o appartenenze) della stessa. In assenza di ulteriori precisazioni, si deduce che tutte le norme richiamate si pongono, *minimum*, a tutela della riservatezza domiciliare, ovvero della riservatezza non in quanto tale (18) bensì

(12) Si tratta di Cass., sez. V, 6 marzo 2009, n. 28251, *Pagano*, in *Foro it.*, 2009, II, 658. In modo analogo, cfr. anche Cass., sez V, 23 ottobre 2008, n. 4926, in *Cass. pen.*, 2010, 3845 ss. E ancora si veda la più risalente Cass., sez. VI, 17 ottobre 2006, n. 4125, in *Arch. Nuova proc. pen.*, 2007, 669.

(13) Cass., sez. V, 26 ottobre 2023, n. 3446, Considerato in diritto, paragrafo 1.1.

(14) Per approfondire, in argomento, Cadoppi, *Il valore del precedente nel diritto penale. Uno studio sulla dimensione in action della legalità*, Torino, 2014, 73 s.; Amarelli, *Dalla legolatria alla post - legalità: eclissi o rinnovamento di un principio?*, in *Riv. it. dir. e proc. pen.*, 2018, 1406; Manes, *Dalla "fattispecie" al "precedente". Appunti di deontologia ermeneutica*, in *Dir. pen. cont.*, 2018, 10.

(15) Oltre all'articolo 615 *bis*, si vedano anche gli articoli 614, 615, 624 *bis*, 628, comma 3, n. 3 *bis*, 52, comma 2 del Codice penale e l'articolo 266, comma 2 del Codice di procedura penale. In questo secondo paragrafo, l'attenzione va al significato attribuito al concetto in esame nelle norme presenti nel Codice penale. Invece, il quinto paragrafo è dedicato specificamente alla definizione data dalla Corte di cassazione alla locuzione "privata dimora" di cui all'articolo 266 c.p.p. Per una riflessione sull'esegesi in entrambi i piani, si consiglia Quero, *Gli esercizi commerciali quali luoghi di privata dimora ex art. 614 c.p.: interpretazione estensiva o analogia in malam partem?*, in *Giur. merito*, 2010, 484 ss.

(16) Si veda l'art. 614, comma 1, c.p., secondo cui "[c]hiunque s'introduce nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle appartenenze di essi, contro la volontà espressa o tacita di chi ha il diritto di escluderlo, ovvero vi s'introduce clandestinamente o con inganno, è punito con la reclusione da uno a quattro anni". È opportuno consultare Siniscalco, voce *Domicilio (violazione di)*, in *Enc. Dir.*, XIII, Milano, 1964, 873 s., nella parte in cui si sottolinea che "[c]on "luogo di privata dimora" il legislatore ha voluto fare riferimento, senza dubbio, ad ogni luogo adibito ad uso privato. (...) Sul piano letterale "luogo di privata dimora", se pone in evidenza il carattere occasionale e temporaneo del soggiorno, accentua, nel contempo, "l'aderenza alla presenza fisica della persona". L'esame dei lavori preparatori mostra come anche con la nuova formula si è voluto rimanere nell'ambito della nozione di "abitazione" sia pure intesa nel suo più ampio significato". L'art. 624 *bis*, comma 1, recita "[c] hiunque si impossessa della cosa mobile altrui, sottraendola a chi la detiene, al fine di trarne profitto per sé o per altri, mediante introduzione in un edificio o in altro luogo destinato in tutto o in parte ad una privata dimora o nelle pertinenze di essa, è punito con la reclusione da quattro a sette anni e con la multa da euro 927 a euro 1.500". A queste due norme fanno espresso rinvio gli articoli di cui alla nota precedente.

(17) Così Hart, *The Concept of Law*, Oxford, 2012, 226, ove l'A. precisava "[w]hichever device, precedent or legislation, is chosen for the communication of standards of behaviour, these, however smoothly they work over the great mass of ordinary cases, will, at some point where their application is in question, prove indeterminate; they will have what has been termed an open texture" (su cui, *inter alia*, Faralli, *Le grandi correnti della filosofia del diritto – Dai Greci ad Hart*, Torino, 2014, 66 ss.). Sul punto, di recente, in prospettiva penalistica Santangelo, *Precedente e prevedibilità*, Torino, 2022, 264 ss.

(18) Per un approfondimento sul diritto alla riservatezza in generale si consulti De Cupis, *I diritti della personalità*, Milano, 1959, 256 ss. Dal punto di vista normativo, particolare attenzione al bene della riservatezza si riscontra a livello internazionale nell'articolo 12 della Dichiarazione Universale dei Diritti dell'Uomo, nell'articolo 8 della Convenzione Europea dei Diritti dell'Uomo e, da ultimo, nell'articolo 7 della Carta dei Diritti Fondamentali dell'Unione Europea. Con particolare riferimento all'articolo 8 CEDU si veda C. eur. dir. umani, *Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life, home and correspondence*, 2020, 7, disponibile all'indirizzo <https://www.echr.coe.int/documents/guide_art_8_eng.pdf>, ove "[i]n order to invoke Article 8, an applicant must show that his or her complaint falls within at least one of the four interests identified in the Article, namely: private life, family life, home and correspondence".

inerente all'ambiente domestico (19).
Per la prima volta, l'esigenza di identificare una definizione il più possibile univoca a livello giurisprudenziale, è stata (apparentemente) (20) soddisfatta dalla trattazione compiuta nella nota sentenza *D'Amico* (21). Tale decisione era relativa alla configurabilità del delitto di furto in abitazione, di cui all'articolo 624-*bis* c.p., laddove il fatto tipico si svolgesse in luoghi di lavoro (22). In questa sede, adottando una prospettiva costituzionalmente orientata (23), le Sezioni Unite hanno precisato che la definizione di "privata dimora" sia più ampia di quella di abitazione e, nondimeno, hanno ripudiato l'interpretazione estensiva (24), preferendo una nozione di "privata dimora" maggiormente conforme al significato letterale del precetto (25). Nel dettaglio, la Corte ha stabilito che, affinché si possa far riferimento all'enunciato in esame, è necessario che siano presenti i "seguenti indefettibili elementi" (26). In primo luogo, lo spazio fisico deve essere utilizzato per svolgere atti della vita privata, tra cui rientrano le attività di tipo lavorativo e professionale (27). In secondo luogo, deve ricorrere il requisito della stabilità tra l'individuo e il luogo in questione (28). In terzo luogo, il soggetto titolare deve poter sia escludere i terzi da tale ambiente (*ius excludendi alios*) che acconsentire a che essi vi accedano (*ius admittendi*) (29).
Con riferimento alla fattispecie di interferenze illecite nella vita privata, quindi, la Corte di cassazione ha accolto un orientamento esegetico restrittivo, limitando la "privata dimora", di fatto, alla sola abitazione (30). Come enunciato in apertura, si tratta di una dimostrazione di "più rigoroso ossequio al limite testuale" della "recente giurisprudenza di legittimità" (31). Del resto, in concomitanza con l'irrefrenabile passaggio dallo "stato legislativo" alla "giurisprudenza legislativa" (32), il raf-

(19) Scalisi, *Diritto alla riservatezza. Il diritto all'immagine, il diritto al segreto, la tutela dei dati personali, il diritto alle vicende della vita privata, gli strumenti di tutela*, *op. cit.*, 335 ss. Barile - Cheli, voce *Domicilio (libertà di)*, in *Enc. dir.*, XIII, Milano, 1964, 862 ss., nella parte in cui elenca gli "elementi essenziali atti a definire la nozione di domicilio quale luogo di privata dimora".

(20) Si veda, a proposito, il paragrafo che segue (e, nello specifico, anche la nota n. 48).

(21) Cass., SU, 23 marzo 2017, n. 31345, *D'Amico*, in *Foro it.*, 2017, II, 673.

(22) Mezzetti, *Furto in abitazione: nozione di privata dimora e luogo di lavoro*, in *Dir. pen. proc.*, 2017, 1572 ss.

(23) Bernardi, *Le Sezioni Unite ridefiniscono la nozione di privata dimora ai fini dell'art 624-bis* c.p, in *Dir. pen. cont.*, 2017, 227 ss.

(24) Tale tendenza, infatti, comporta un'inammissibile "tutela ad intermittenza" (Cass., SU, 23 marzo 2017, n. 31345, Considerato in diritto, paragrafo 2.2.).

(25) Larizza, *Furto in abitazione: le Sezioni unite chiariscono la nozione di "privata dimora"*, in *Dir. pen. proc.*, 2017, 2478 ss.

(26) Cass., SU, 23 marzo 2017, n. 31345, Considerato in diritto, paragrafo 2.6. Sulla base di quanto stabilito in questa sede dal Supremo collegio, si veda Cass., sez. V, 19 ottobre 2017, n. 51113, C., in Ced. Cass., rv. 271629 (m), che, applicando i suddetti criteri, esclude che un istituto scolastico possa costituire "privata dimora". A proposito, si rimanda a Cavallo, *Estensione e limiti del concetto penale di privata dimora*, in *Il Quot. Giur.*, 2017, disponibile all'indirizzo <https://www.altalex.com/documents/2017/11/20/estensione-e-limiti-del-concetto-penale-di-privata-dimora>.

(27) La questione sottoposta alle Sezioni Unite è infatti "[s]e sia configurabile il reato di cui all'articolo 624 *bis* cod. pen. quando l'azione delittuosa venga posta in essere (...) in luoghi di lavoro". Alla fine della sua ermeneutica, la Cassazione enuncia il principio di diritto in base a cui "[a]i fini della configurabilità del delitto previsto dall'art. 624-*bis* cod. pen., i luoghi di lavoro non rientrano nella nozione di privata dimora, salvo che il fatto sia avvenuto all'interno di un'area riservata alla sfera privata della persona offesa. Rientrano (...) esclusivamente i luoghi, anche destinati ad attività lavorativa o professionale, nei quali si svolgono non occasionalmente atti della vita privata, e che non siano aperti al pubblico né accessibili a terzi senza il consenso del titolare".

(28) Come specificato dalla stessa Cass., SU, 23 marzo 2017, n. 31345, Considerato in diritto, paragrafo 2.5 (che a sua volta riprende la – nota in materia di intercettazioni, come si vedrà in seguito – Cass., SU, 28 marzo 2006, n. 26795, *Prisco*, in *Riv. it. dir. e. proc. pen.*, 2006, 1537 ss., Considerato in diritto, paragrafo 8, settimo capoverso), "il requisito della stabilità, «perché è solo questa, anche se intesa in senso relativo, che può trasformare un luogo in un domicilio, nel senso che può fargli acquistare un'autonomia rispetto alla persona che ne ha la titolarità»".

(29) Per usare le parole della Corte cost., 16 maggio 2008, n. 149, in *Giur. cost.*, 2008, 1825 ss., relativa al tema della tutela del domicilio ex articolo 14 Cost., è possibile identificare il "diritto di ammettere o escludere altre persone da determinati luoghi, in cui si svolge la vita intima di ciascun individuo; e il "diritto alla riservatezza su quanto si compie nei medesimi luoghi". Cfr. anche Pace, *Problematica delle libertà costituzionali. Lezioni. Parte speciale*, II ed., Padova, 1992, 212.

(30) È ricchissima la giurisprudenza di legittimità in materia. Non costituiscono "privata dimora" né gli ambienti carcerari sulla base della Cass., sez. VI, 15 maggio 2018, n. 26028, D.R., in *Ced. Cass.*, rv. 273417 (m) (relativa al reato di oltraggio a pubblico ufficiale *ex* art. 341 *bis*; si veda il Considerato in diritto, paragrafo sesto, nella parte in cui "la cella e gli ambienti penitenziari sono da considerarsi luogo aperto al pubblico, e non certamente luogo di privata dimora [dal momento che ai detenuti] non compete alcuno *ius excludendi alios*"), né la stanza di degenza di un ospedale, secondo Cass., sez. VI, 13 maggio 2009, n. 22836, *Rizzi*, in *Ced. Cass.*, rv. 244148 (m). Allo stesso modo si è detto per una *toilette* pubblica in Cass., sez. V, 16 marzo 2009, n. 11522 e per le docce di una piscina comunale in Cass., sez. V, 14 maggio 2015, n. 28174 (a questo ultimo proposito si vedano: Capitani, *Nascondeva telecamere fra le docce della piscina comunale: violenza privata e non reato di interferenza illecita nella vita privata*, in *Dir. giust.*, 2015, 24 ss.; Torlasco, *Telecamera nascosta nello spogliatoio di una piscina: una discutibile sentenza della S:C: in tema di violenza privata*, in *Dir. pen. cont.*, 2016).

(31) Manes, *Dalla "fattispecie" al "precedente". Appunti di deontologia ermeneutica*, *op. cit.*, 9. Cfr. anche Consulich, *Così è (se vi pare) alla ricerca del volto dell'illecito penale, tra legge indeterminata e giurisprudenza imprevedibile*, in *Dir. pen. cont.*, 2020, 69 ss., nella parte in cui indentifica i tre passaggi da seguire in materia penale nella fase ermeneutica, ossia: "principio di precisione", "dovere di astensione dalle ridefinizioni", "prevalenza dell'interpretazione più favorevole al reo".

(32) Manes, *Dalla "fattispecie" al "precedente". Appunti di deontologia ermeneutica*, *op. cit.*, 2. Inoltre, si consulti anche Fiandaca, *Crisi della riserva di legge e disagio della democrazia rappresentativa nell'età del protagonismo giuri-*

forzamento del criterio letterale in materia penale è da considerarsi assolutamente necessario per assicurare un'interpretazione conforme al principio di legalità proprio di un diritto penale costituzionale (33).
Peraltro, nel caso di cui si discute, anche a voler ricostruire l'*intentio legis*, è possibile confermare questa *narrow interpretation*, dal momento che, anche in fase di elaborazione legislativa, la Commissione parlamentare incaricata si interrogò proprio su questa questione, giungendo all'esclusione di un concetto ampio di "privata dimora" (34).

### *2.2. Un recente orientamento interpretativo estensivo*

Benché l'indirizzo giurisprudenziale di cui sopra sia sicuramente predominante, non mancano alcune recenti pronunce che se ne sono discostate, dando così vita, ad un'antitetica interpretazione estensiva. Ne deriva, allora, il rischio di un preoccupante contrasto interpretativo sincronico (35), in relazione alla possibilità di estendere la fattispecie a spazi ben diversi dal "semplice" domicilio (36).
La questione inerente alla qualificazione di particolari luoghi quale "privata dimora" appare, allora, tutt'altro che risolta. L'argomento di natura sistematica, maggiormente improntato a una generale tutela del diritto alla riservatezza (37), porta a dei risultati ermeneutici distanti rispetto a quelli che si ottengono attraverso la mera lettura del testo normativo o dei lavori preparatori (38). In questo senso, emergono le note fragilità del criterio letterale in presenza di enunciati polisenso (39). Del resto, se è vero che esistono i casi c.d. "facili" in cui è possibile ritrovare immediatamente una corrispondenza tra fattispecie in astratto e in concreto (40), è altrettanto vero che nei casi c.d. "difficili" non sempre l'argomento

*sdizionale*, in *Criminalia*, 2011, 79 ss., disponibile all'indirizzo <https://discrimen.it/wp-content/uploads/Criminalia-2011.pdf>.

(33) Manes, *Dalla "fattispecie" al "precedente". Appunti di deontologia ermeneutica*, *op. cit.*, 6 ss., nonché di recente Id., *Introduzione ai principi costituzionali in materia penale*, cit., 41 s.; Insolera, *Qualche riflessione e una domanda sulla legalità penale nell'"epoca dei giudici"*, in *Criminalia*, 2012, 285 ss.

(34) Risulta estremamente interessante la lettura del verbale della seduta di giovedì 14 febbraio del 1974, 503 ss., tenutasi in seno alla Commissione IV - Giustizia, ove, il Presidente affermò che "[i]l punto più importante è quello relativo all'estensione che vogliamo dare al luogo" (505). In occasione di questa riunione, venne rigettato l'emendamento presentato dall'onorevole Felisetti, il quale avrebbe voluto sostituire il passo "notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614" con "immagini e notizie comunque attinenti all'altrui attività" (505). Così procedendo, si sarebbe esteso l'ambito di applicazione della tutela della norma non tanto più a dei luoghi, più o meno circoscritti, come l'abitazione, bensì sarebbero state garantite "le attività private indipendentemente dal fatto che si siano svolte nell'ambito del ristretto domicilio". Questa modifica è stata aspramente criticata dapprima dall'onorevole Accreman, il quale ha constato "come il Senato abbia scelto di adeguarsi, in questo caso ad una formula già esistente, quella concernente il reato di violazione di domicilio, senza introdurvi elementi nuovi" (505) e poi anche dal Relatore Castelli che ha ragionevolmente sostenuto che "se estendessimo la punibilità a qualsiasi interferenza nell'altrui attività, finiremmo con il limitare in modo pesante l'esercizio di attività legittime", non utilizzando, quindi, più il diritto penale come *extrema ratio* (per esempio, si citano tra le attività legittime, che verrebbero altrimenti sacrificate, quelle relative al "diritto di cronaca"- 507). Inoltre, come evidenziato dall'intervento dell'onorevole Padula, "[p]ure se sarà affidata in larga misura alla elaborazione giurisprudenziale la previsione dei criteri con cui ampliare la formula generica, non possiamo in un testo di legge non fare riferimento al concetto di domicilio, per quanto vago esso sia" (505). È possibile consultare tale documento all'indirizzo <https://legislature.camera.it/_dati/leg06/lavori/stencomm/04/Leg/Serie010/1974/0214/stenografico.pdf>. Ancora, tra tutte e sei le proposte di legge presentate per poter disciplinare le problematiche relative all'uso abusivo delle intercettazioni telefoniche (in palese violazione del diritto alla riservatezza), la l. n. 98 del 1974 è stata la prima e l'unica a contenere l'espressione "privata dimora", distinguendosi così dalle altre, tra cui si ricorda la Proposta di legge 17 gennaio 1973, n. 1482, disponibile all'indirizzo <https://legislature.camera.it/_dati/leg06/lavori/stampati/pdf/14820001.pdf>, nel cui articolo 2 si usa genericamente "luogo privato" e la Proposta di legge 2 agosto 1973, n. 2323, consultabile all'indirizzo <https://legislature.camera.it/_dati/leg06/lavori/stampati/pdf/23230001.pdf>, dove l'articolo 1 si serve dell'ancora più vago "non pubblicamente". Nondimeno, qualora si possa fare riferimento ad una definizione di "privata dimora", questa si potrebbe considerare come "pericolosa", in quanto, per usare le parole di Cadoppi, *Il problema delle definizioni legali nel diritto penale. Presentazione*, in ID. (coord.), *Il problema delle definizioni legali nel diritto penale. Omins definitio in iure periculosa?*, Padova, 1996, 20, "[sembra] destinata comunque ad essere superata nella pratica dell'interpretazione giudiziaria" poiché non pare "in grado di svolgere il suo compito naturale, che è di de-limitare (= de-finire) l'ambito di applicazione della legge".

(35) Per approfondire tale questione critica si rimanda anzitutto a Cadoppi, *Il valore del precedente*, *op.cit.*, 73 ss.; più nel dettaglio, sulla vincolatività del precedente, 303 ss. Si veda poi Fiandaca, *Diritto penale giurisprudenziale e ruolo della Cassazione*, in *Cass. pen.*, 2005, 1722 ss.; Fidelbo, *Il precedente nel rapporto tra sezioni unite e sezioni semplici: l'esperienza della Cassazione penale*, in *Quest. giust.*, 2018, 137 ss.; Fidelbo, *Verso il sistema del precedente? Sezioni Unite e principio di diritto*, in *Dir. pen. cont.*, 2018, 2 ss.

(36) Tale prospettiva è sostenuta anche da parte della dottrina. Si veda Armati - La Cute, *Profili penali delle comunicazioni di massa*, Milano, 1987, 337; Bonzano, *Appunti sulla tutela della riservatezza*, in *Dir. pubbl.*, 1984, V, 116; Manna, *Riservatezza, arte, scienza: quid iuris?*, in *Dir. informaz. e informatica*, 1986, 510 ss.

(37) Pestelli, *Il delitto di "indiscrezione domiciliare" ex art. 615 bis c.p. alla luce della più recente elaborazione giurisprudenziale*, in *Dir. pen. proc.*, 2013, 717 ss.

(38) Morrone, *Fonti normative*, Bologna, 2018, 75 ss. Cfr. anche Pattaro, *Brevi note sull'interpretazione del diritto*, in *Argomenti di teoria del diritto* a cura di Faralli, Torino, 2016, 132 ss. Per meglio comprendere la *voluntas legislatoris* si veda la nota n. 34. Un tipo di interpretazione estensiva, seppur logica per la risoluzione del caso concreto (che, si suppone, abbia come fine la tutela della riservatezza in generale), rischia però di tradire il vero e unico significato letterale della norma.

(39) In questo senso, è interessante vedere Marinucci - Dolcini - Gatta, *Manuale di diritto penale, Parte generale*, X edizione, Milano, 2023, 107, nella parte in cui si afferma che "[r]estare entro la cornice dei 'possibili significati letterali' - il compito primordiale che deve assolvere l'interprete - è impossibile quando le norme siano inguaribilmente imprecise".

(40) Gargani, *Dal corpus delicti al Tatbestand. Le origini della tipicità penale*, Milano, 1997, 18 ss.

testuale non è sufficiente, da solo, per ricostruire in termini ragionevolmente certi il significato degli enunciati giuridici (41). Dunque, non sempre, il criterio testuale è di per sé bastevole. (42) Eppure, il numero di decisioni della giurisprudenza di legittimità, in tale prospettiva, continua a espandersi (43).

In una recente sentenza (44), per esempio, proprio seguendo il *dictum* della sentenza *D'Amico*, la Corte ha stabilito che i servizi igienici di un circolo privato rappresentano un luogo di "privata dimora" (45). Pur applicando, dunque, i tre criteri di cui si è detto, si è specificato che la *toilette* abbia di per se stessa una determinata destinazione d'uso, tale per cui è adibita ad atti della vita privata del fruitore; si è rilevato il requisito di stabilità tra utenti del locale e la stessa *toilette*; si è riconosciuto lo *ius excludendi* dei frequentatori del circolo nei confronti dei non ammessi allo stesso. (46) Sempre sulla stessa scia, da ultimo, la Sezione Quarta della Corte ha considerato "privata dimora" la cantina, benché disabitata e non attigua all'abitazione (47).

Ora, sebbene nella sentenza *D'Amico* la Corte affermi di voler promuovere una nozione più puntuale della locuzione presa in considerazione in questa sede, a dire il vero, non sembra sortire il risultato previsto. Tali indicatori, quindi, rischiano di non essere implementati per il fine che si era originariamente prefissata la Corte, tanto da portare, paradossalmente, ad un significato più vasto di "privata dimora". Gli stessi rischiano, vieppiù, di non essere del tutto applicati – come accaduto nel caso particolare della sentenza n. 3446 in commento (48).

## 3. Un caso difficile: il problema dell'abitacolo dell'autovettura

In virtù delle valutazioni svolte finora, è opportuno tornare al tema dell'abitacolo di un'autovettura, la cui classificazione entro il concetto di "privata dimora" ha animato, e continua ad alimentare, vivacemente, il dibattito dottrinale e giurisprudenziale, spesse volte con riferimento al settore delle intercettazioni (49).

Come è stato messo in luce nei paragrafi precedenti, secondo l'orientamento dominante (50), sia i giudici di legittimità che quelli di merito sostengono che il veicolo non possa rientrare tra i luoghi di "privata dimora" (51), in considerazione della limitata destinazione d'uso, essenzialmente coincidente con la sola circolazione e il solo trasporto dei passeggeri (52), a meno che questo non venga adibito ad abitazione (53), oppure non sia

(41) Donini, *Fattispecie o case law? La "prevedibilità del diritto" e i limiti alla dissoluzione della legge penale nella giurisprudenza*, in *Quest. giust.*, 2018, 84 ss.

(42) Palazzo, *Testo, contesto e sistema nell'interpretazione penalistica*, in *Studi in onore di Giorgio Marinucci* a cura di Dolcini - Paliero, I, Milano, 2006, 515 ss. Da consultarsi anche Santangelo, *Precedente e prevedibilità*, cit., 290 ss.

(43) *Inter alia*, si menzionano i seguenti casi. In Cass., sez. VI, 26 gennaio 2011, n. 7550, in *Cass. pen.*, 521 ss., l'imputato è stato condannato in quanto ha fotografato dei pazienti nudi nelle "docce di un ospedale", le quali sono state riconosciute come luogo di "privata dimora": in merito si veda Mengoni, *Interferenze illecite nella vita privata: il reato sussiste anche se il soggetto ritratto non può essere identificato*, in *Cass. pen.*, 2012, 523 ss. In Cass., sez. III, 17 ottobre 2018, n. 47123, sempre con riferimento all'ambiente ospedaliero, anche l'ambulatorio (nel caso citato, adibito in via provvisoria a spogliatoio, fruibile sia da pazienti che da operatori sanitari) assume questo carattere di privatezza. Allo stesso modo è stata considerata la *toilette* di uno studio professionale in Cass., sez. III, 30 aprile 2015, n. 264196. Più di recente, ancora, in Cass., sez. III, 11 giugno 2020, n. 27990, con nota di Micciché, *Lo studio medico rientra nei luoghi di "privata dimora" ex art. 615-bis c.p.*, in *Cass. pen.*, 2021, 2441 ss., si è considerato uno studio medico come "privata dimora".

(44) Cass., Sez. V, 1 marzo 2021, n. 25263, in *Dir. pen. proc.*, 2021, 1304, Pres. Bruno, Rel. Miccoli.

(45) Corbetta, *Toilette di un circolo privato: è "luogo di privata dimora"?*, in *Dir. pen. proc.*, 2021, 1304 s.

(46) Pittau, *Interferenza illecita nella vita privata e riservatezza domiciliare: la Cassazione estende la nozione di "luogo di privata dimora"*, in *Sist. Pen.*, 2021.

(47) Si rinvia a Panetta - Panetta, *Furto in abitazione: la cantina rientra nella nozione di privata dimora*, in *Dir. giust.*, 2024, 5 ss., nota a sentenza della recentissima Cass., sez. IV, 29 novembre 2023, n. 51596.

(48) A titolo esemplificativo, si ipotizzi di attuare questi *standards* nella sentenza n. 3446 del 2023, da considerarsi, come si metterà in evidenza nei paragrafi successivi, caso "difficile". Per assurdo, si stima che, così facendo, molto probabilmente, l'esito della declaratoria del 2023 sarebbe stato diverso e avrebbe portato ad un'interpretazione estensiva. Visto il primo parametro, considerando che tra le "manifestazioni di vita privata", le Sezioni Unite del 2021 ricomprendono anche "l'attività professionale e di lavoro in genere", le conversazioni captate all'interno dell'autovettura della ricorrente nel caso in commento sarebbero potute rientrare in questa categoria, dal momento che la donna era solita intrattenere nell'auto, *inter alia*, conversazioni di carattere professionale. Inoltre, risulterebbero rispettati anche gli altri due "elementi indefettibili", poiché esiste chiaramente un rapporto di stabilità relativamente a un'auto di proprietà, rispetto cui sussiste il diritto di escludere chi non voglia accedervi, non solo fisicamente, bensì anche di modo che i non autorizzati non siano resi partecipi del contenuto delle conversazioni qui tenute.

(49) Di cui nel dettaglio all'ultimo paragrafo del presente lavoro.

(50) A riguardo, si veda la nota a Cass., sez. V, 30 gennaio 2008, n. 12042, in *Cass. pen.*, 2009, 166 s. di Salamone, *La tutela penale della riservatezza nel caso dell'immagine "rubata" in automobile*, in *Cass. pen.*, 2009, 167 ss.

(51) Come d'altronde accade anche nella sentenza analizzata, che a sua volta richiama la Cass., sez. V, 6 marzo 2009, n. 28251, *cit.*, 658. A tal proposito si vedano le precisazioni di cui alla nota 12. Dello stesso avviso in dottrina Grilli, *La procedura penale. Guida pratica*, vol. I, Padova, 2009, 516.

(52) Scalisi, *Diritto alla riservatezza. Il diritto all'immagine, il diritto al segreto, la tutela dei dati personali, il diritto alle vicende della vita privata, gli strumenti di tutela*, cit., 350 s.

(53) In questo senso, in materia di intercettazioni, Cass., sez. V, 22 aprile 2014, n. 45512, in Ced. Cass., 2014, rv. 260760 secondo cui "[l]e intercettazioni tra presenti captate all'interno di un'autovettura sono validamente utilizzabili, eccetto che il veicolo, sin dall'origine, sia utilizzato oppure destinato ad uso di privata abitazione"; a proposito vi è la nota di Gentile, *L'autovettura è luogo di privata dimora solo se vi è prova della sua destinazione ad uso abitativo*, in *Dir. e giust.*, 2014, 42 ss.

dotato di cella abitativa (come nel caso dei camper) (54). Nel risolvere una questione di natura processuale (55), il Supremo Collegio, d'altra parte, ha dato atto dell'esistenza di questo argomento restrittivo, che risultava essere particolarmente risalente nel tempo (56).
Le stesse Sezioni Unite del 2001, appena citate, mettevano in evidenza, senza proporre alcuna soluzione (57), la sussistenza del contrasto giurisprudenziale considerando l'orientamento di segno opposto (58), il quale rappresenta chiaramente una sottocategoria del più ampio filone che sposa l'interpretazione estensiva del concetto di "privata dimora" (59).
Nel 1987, del resto, persino per la Corte costituzionale "secondo il diritto vivente, l'autovettura [era] considerata come luogo di "privata dimora", coperta dalla tutela apprestata dall'art. 14 Cost." (60). La *ratio* di un simile orientamento si ritrova nella considerazione per cui sia possibile considerare l'automobile come un luogo in cui ci si può aspettare di godere di un livello di riservatezza maggiore rispetto a quello che si può avere in un luogo pubblico (61). D'altronde, come l'esperienza stessa insegna, con riguardo alla struttura e alla conformazione dell'auto, si tratta certamente di uno spazio fisico visibile all'esterno, ma pur sempre di uno spazio chiuso, elemento che lo rende uno di quei luoghi-limite di difficile identificazione, poiché separa solo in apparenza i passeggeri da tutto ciò che si trova all'esterno dell'auto. In un certo qual modo, si potrebbe ritenere più plausibile tutelare le conversazioni che vi avvengono all'interno piuttosto che i comportamenti non comunicativi, che risultano, invece, palesi alla vista (62).
Nientemeno, la sentenza *Prisco* (63) conia la categoria dei "luoghi riservati", che dovrebbe ricomprendere anche le automobili (64); si tratta, tuttavia, di una impostazione estremamente problematica in relazione al *nullum crimen*, e in particolare alla corretta applicazione della deontologia ermeneutica cui è chiamato il giudice penale (65).

(54) Così Cass., sez. V, 6 marzo 2009, n. 28251, *cit.*, 658. Analogamente, anche oltreoceano, in *California v. Carney, 471 U.S. 386* (1985), si stabiliva che "expectations of privacy in a motor home are more like those in a dwelling than in an automobile".

(55) Conti, *Intercettazioni "ambientali" eseguite con impianti esterni alla Procura e obbligo di motivazione*, in *Dir. pen. proc.*, 2003, 194 ss.

(56) Per citare la sentenza in questione, Cass., SU, 31 ottobre 2001, n. 42792, *Policastro*, in *Cass. pen.*, 2002, 2829 (che si esprime in materia di intercettazioni), si devono ricordare in questo senso le seguenti pronunce di legittimità: "Cass., Sez. VI, 19 febbraio 1981, *Semitaio*, rv. 149373; Sez. I, 22 gennaio 1996, *Porcaro*, rv. 203799; Sez. VI, 5 ottobre 2000, *Saggio*; Sez. I, 11 luglio 2000, *Nicchio*, rv. 216749; Sez. I, 18 ottobre 2000, *Galli*, rv. 218042; Sez. VI, 23 gennaio 2001, *De Palma*; Sez. II, 4 maggio 2001, *Berlingeri*; Sez. II, 9 maggio 2001, *D'Agostino*". Come messo in seguito in risalto da Cass., SU, 26 giugno 2014, n. 32697, in *Cass. pen.*, 2014, 4046, si allineano a questo orientamento anche "Sez. 6, n. 2845 del 1° dicembre 2003, dep. 2004, *Cavataio*, Rv. 228420; Sez. 1, n. 2613 del 20 dicembre 2004, dep. 2005, *Bolognino*, Rv. 230533; Sez. 1, n. 47180 del 1° dicembre 2005, *Sarcone*, Rv. 233991; Sez. 1, n. 32581 del 6 maggio 2008, *Sapone*, Rv. 241229; Sez. 1, n. 13979 del 24 febbraio 2009, *Morabito*, Rv. 243556; Sez. 5, n. 8365 del 18 gennaio 2013, *Girasole*, Rv. 254657".

(57) La Corte non ha affrontato in maniera incisiva il problema proponendo una soluzione, poiché tale questione non è risultata rilevante nel caso di specie.

(58) In merito viene citata Cass., sez. II, 12 marzo 1998, n. 1831, *Zagaria*, in Ced. Cass., rv. 211142 (m). Di questo stesso avviso, Barbieri, *In tema di intercettazioni nell'abitacolo*, in *Giur. it.*, 2002, 1 (sebbene si tratti di una nota alla sentenza *Saggio* del 2000, nella quale si sostiene l'orientamento restrittivo). Si veda in seguito anche la pronuncia del 2019, cui si fa riferimento nel paragrafo successivo.

(59) Di cui ampiamente al paragrafo 2.2.

(60) Corte cost., 31 marzo 1987, n. 88, in *Giur. cost.*, 1987, I, 682 ss.

(61) Fumu, *Una dubbia interpretazione restrittiva sui requisiti della privata dimora. L'orientamento contrario erroneamente definito "isolato"*, in *Dir. giust.*, 2001, 21. Ciò deriva anche dal progresso tecnologico che rende l'automobile un ambiente che va al di là della semplice mezzo di trasporto, come specifica Fanuele, *Il concetto di privata dimora ai fini delle intercettazioni ambientali*, in *Cass. pen.*, 2001, 2748 ss. In linea più generale, questo potrebbe rappresentare uno dei casi in cui "i legislatori affidano la scelta al giudice, il quale deciderà in concreto, cioè cercherà di trovare l'equilibrio sciogliendo il conflitto di valori nel contesto della situazione concreta": così Sgubbi, *Il diritto penale incerto ed efficace*, in *Riv. it. dir e proc. pen.*, 2001, 1195.

(62) Il riferimento va ai "comportamenti di tipo comunicativo", di cui, dapprima, alla Corte cost., 11 aprile 2002, n. 135, in *Giur. cost.*, 2002, 1065 ss. e, poi, alla Corte cost., 16 maggio 2008, n. 149, *cit.*, 1825 ss. In ambo le pronunce, la Corte sottolinea che "le riprese visive in luoghi di privata dimora sono soggette alla disciplina delle cosiddette intercettazioni ambientali (...) solo quando mirino alla captazione di comportamenti a carattere comunicativo" (Corte cost., 16 maggio 2008, n. 149, Ritenuto in fatto, sesto capoverso). Pare, dunque, che i comportamenti comunicativi godano di una maggiore tutela. Si veda a proposito della libertà di domicilio, in relazione alle decisioni citate, Paganetto, *Le riprese visive nei luoghi di privata dimora. Spunti per una riflessione sui contenuti e i limiti della libertà di domicilio*, in *Studi in onore di Alessandro Pace*, Napoli, 2012, disponibile anche all'indirizzo <https://www.forumcostituzionale.it/wordpress/images/stories/pdf/documenti_forum/paper/0279_paganetto.pdf>.

(63) Tale pronuncia si esprime in materia di intercettazioni e riprese visive, come più nel dettaglio si dirà nel quinto paragrafo.

(64) Per usare le parole di Cass., SU, 28 marzo 2006, n. 26795, *Prisco*, *cit.*, 1537 ss., dunque,"[i] camerini in cui avvenivano gli incontri all'interno del locale [non possono essere considerati domicilio]" (Considerato in diritto, paragrafo 8, nono capoverso), tuttavia, "[l]a caratteristica e le funzioni di questi luoghi (...) non giustificano un ampliamento del concetto di domicilio fino a comprenderli in esso, dall'altro non consentono che le attività che vi si svolgono possano rimanere esposte a qualunque genere di intrusione" (Considerato in diritto, paragrafo 8, decimo capoverso). In merito Conti, *Le video-riprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati" – Commento*, in *Dir. pen. proc.*, 2006, 1347; Camon, *Le sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*, in *Riv. it. dir. e proc. pen.*, 2006, 1565 ss.

(65) Altamente discutibile in relazione al *nullum crimen*, si ritiene eccessiva questa iniziativa giurisprudenziale, che, creando nuove categorie, tende ad esercitare abusivamente la funzione legislativa. Si veda in questo senso: Manes, *Dalla "fattispecie" al "precedente"*, *op. cit.*, 6, nella parte in cui si propone "una sorta di "licitazione" sulle regole ermeneutiche di

## 4. La sentenza di legittimità relativa all'abitacolo delle autovetture: un esito non scontato

In ragione di tali considerazioni, non si può scongiurare, a monte, che la vicenda controversa relativa all'abitacolo di un'autovettura, avrebbe potuto presentare anche un epilogo opposto. Sebbene, infatti, nella sentenza più datata tra le due in commento, la Corte abbia, correttamente, adottato un'interpretazione più circoscritta di "privata dimora", non si può escludere che il giudice di legittimità si servirà, in futuro, di una definizione più estesa di tale concetto, visto che, come evidenziato in precedenza, la giurisprudenza non appare saldamente consolidata in materia (66).

A dimostrazione di quanto sostenuto, infatti, pochi anni prima, nel 2019, in presenza di un caso quasi del tutto sovrapponibile, la Corte ha elaborato una risoluzione diametralmente opposta a quella fornita nel 2023. Pertanto, pare utile chiedersi se si debba considerare la sentenza antecedente come uno *swing*, un caso isolato, rispetto alla prevalente giurisprudenza restrittiva – prontamente corretto, da ultimo, nel 2024 – oppure come una possibile linea ermeneutica alternativa, che potrebbe acquisire sempre più vigore in seguito – e di cui è bene diffidare in materia sostanziale.

### *4.1. Due pronunce a confronto: un "contrasto giurisprudenziale sincronico" o un overruling definitivo?*

La sentenza più risalente, a cui si fa riferimento nel paragrafo precedente (67), non può passare inosservata, in quanto, come anticipato, presenta numerosi elementi in comune con la pronuncia analizzata avanti, pur raggiungendo un risultato del tutto antitetico. E proprio dal confronto delle due pronunce, è possibile evidenziare come, nonostante i presupposti siano i medesimi (68), non sempre la Corte adotta lo stesso ragionamento nel classificare l'abitacolo dell'auto (69).

La sentenza, con cui si vuole instaurare un confronto, dunque, prende in esame il caso di due investigatori privati, condannati dalla Corte d'appello di Brescia per il reato di cui all'articolo 617-*bis* c.p. (70), avendo questi posizionato, su commissione, un GPS e una "cimice" nell'abitacolo dell'auto della vittima. Nel segnalare un'erronea qualificazione del fatto (71), la Corte di legittimità ha specificato che queste circostanze integravano, a tutti gli effetti, "una tipica ipotesi di interferenza illecita nella vita privata" (72) *ex* articolo 615 *bis* c.p. (73)

base che tengano in conto i tratti di singolarità – o di vera e propria unicità – del diritto penale come "diritto dei limiti" e "scienza delle garanzie""; Id., *Sui vincoli costituzionali dell'interpretazione in materia penale (a margine della recente giurisprudenza della consulta)*, in *Riv. it. dir. e proc. pen.*, 2021, 1233; Id., *Introduzione ai principi costituzionali in materia penale*, cit., 85 ss.; Palazzo, voce *Legge penale*, in *Dig. disc. pen.*, VII, Torino, 1993, 338 ss.; Consulich, *Così è (se vi pare)*, cit., 69, nella parte in cui individua il "dovere di astensione dalle ridefinizioni"; Fiandaca, *Ermeneutica e applicazione giudiziale del diritto penale*, in *Riv. it. dir. e proc. pen.*, 2001, 377 ss., si veda la parte in cui "[l]a giurisprudenza (...) dovrebbe riappropriarsi di quella che definirei "cultura del limite" o dell'autocontenimento: interiorizzando più profondamente il principio della divisione dei poteri e, di conseguenza, sottoponendo a vaglio critico e problematizzando le sue crescenti vocazioni "sostanzialistiche". La presa d'atto che neppure il legislatore penale è "onnipotente" non giustifica palesi o disinvolti aggiramenti dei testi normativi, sia pure a "fin di bene" e cioè per ragioni di giustizia sostanziale considerate vincenti rispetto alle esigenze di certezza e ai vincoli della legalità formale"; ancora Caputo, *In cammino verso un'ermeneutica prescrittiva nell'applicazione della legge penale*, in *Cass. pen.*, 2023, 1064.

(66) Per utilizzare le parole di Viganò, *Il principio di prevedibilità della decisione giudiziale in materia penale*, in *La crisi della legalità. Il sistema vivente delle fonti penali* a cura di Paliero - Moccia - De Francesco - Insolera - Pelissero - Ramponi - Risicato, Napoli, 2016, 249, in via generale, "il giudice dovrà *tendenzialmente* decidere il caso concreto in modo *prevedibile*, e dunque in modo conforme a tale giurisprudenza [che ha già affrontato una determinata questione giuridica]". Sta di fatto che, comunque, come chiaramente mette in risalto Cadoppi, *Il valore del precedente*, cit., 334., l'obiettivo sia "quell[o] di assicurare una maggiore certezza del diritto anche attraverso l'imposizione di una qualche forma (relativa e non assoluta) di *stare decisis*". In senso leggermente contrario, Gorla, voce *Precedente giudiziale*, in *Enc. Giur.*, XXIII, Roma, 1990, 4, secondo cui esisterebbe un dovere giuridico di uniformarsi ai precedenti della Suprema Corte, eccezion fatta per il ricorrere di gravi motivi.

(67) Cass., sez. V, 4 giugno 2019, n. 33499, Pres. Sabeone, Rel. Pistorelli.

(68) In entrambe le circostanze ricorrono gli elementi identificati da Palazzo, *Considerazioni in tema di tutela della riservatezza*, cit., 129 ss., in presenza dei quali si configura la fattispecie di reato in questione.

(69) Questo risultato appare ancora più singolare se si considera che sussista una parziale identità nella composizione del collegio giudicante.

(70) Tale norma è rubricata "Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche". Anche questa è stata inserita dall'articolo 3 della l. n. 98 del 1974.

(71) A proposito si veda Canestrari - Cornacchia - Gamberini - Insolera - Manes - Mantovani - Mazzacuva - Sgubbi - Stortoni - Tagliarini, *Diritto penale - Lineamenti di parte speciale*, Milano, 2016, 683 s., nella parte in cui si afferma che "il posizionamento di una microspia all'interno di un autoveicolo è stato considerato comportamento non rilevante ai sensi dell'articolo 617 *bis* c.p., in quanto idoneo a permettere la registrazione solo delle conversazioni tra i soggetti presenti a bordo del mezzo, e, di conseguenza, non configurabile come intercettazione di comunicazione telefonica o telegrafica (Cass. pen., Sez. V, 16 dicembre 2005, in *Cass. pen.*, 2007, 2062; analogamente in relazione alla collocazione, allo stesso scopo, di un telefono cellulare all'interno dell'autovettura: Cass. pen., Sez. V, 6 marzo 2009, in *Foro it.*, 2009, II, 658; Cass. pen., Sez. V, 23 ottobre 2008, in *Cass. pen.*, 2010, 3845)".

(72) Cass., sez. V, 4 giugno 2019, n. 33499, Considerato in diritto, paragrafo 2.2.

(73) Per un confronto tra le due norme, si vedano Barbieri, *Principio di tassatività e tutela penale della riservatezza delle comunicazioni*, in *Giur. merito*, 2009, 1663 ss.; Manca, *Non v'è tutela penale per la vita privata che si svolge in automobile*, in *Resp. civ. e prev.*, 2008, 2487, nella parte in cui si mette in luce che "il sistema di tutela penale vigente della vita privata non riesca ad inquadrare e reprimere una lesione oggettivamente grave e ragionevolmente allarmante, che scivola indenne tra le sue maglie".

Da ciò discendeva il proscioglimento degli imputati per difetto di querela da parte della persona offesa.
Innanzitutto, in entrambi i casi è stato installato lo stesso "strumento di ripresa (...) sonora", ovvero il dispositivo GPS – nel caso ora citato, in associazione ad una microspia e, nella vicenda più recente (74), invece, integrato da un microfono – al fine di procacciare delle informazioni riservate (75).
Sul punto dei "luoghi indicati nell'art. 614", la Cassazione ha, nondimeno, percorso due strade opposte. Infatti, se, da una parte, nella sentenza più recente, la Corte fa essenzialmente leva sull'interpretazione di "privata dimora" per poter escludere la configurazione del delitto di indiscrezione; al contrario, nella pronuncia precedente, non si è richiamato in alcun modo tale concetto, ma si è dichiarato, in modo implicito, nel ricondurre il fatto alla fattispecie del 615 *bis* c.p., che l'autovettura è uno dei luoghi di "privata dimora".
Dunque, mentre la sentenza depositata da poco prosegue nel solco della giurisprudenza maggioritaria, che non riconosce la vettura come luogo di "privata dimora", invece, la pronuncia anteriore arricchisce ulteriormente il filone ermeneutico che difende un'interpretazione estensiva. La distanza interpretativa, che intercorre tra le due decisioni, nella risoluzione di casi analoghi, se non addirittura coincidenti in punto di fatto, alimenta la spaccatura interna alla giurisprudenza.
Conseguentemente, nonostante l'ultima sentenza segni un ritorno alla giurisprudenza prevalente, è lecito domandarsi se si tratti di un definitivo *overruling*, atto a risolvere, una volta per tutte, il contrasto ermeneutico descritto, oppure rappresenti solo un ritorno temporaneo all'uso del criterio testuale nell'interpretare il concetto di "privata dimora", che potrebbe portare a futuri "colpi di scena".

## 5. Il significato di "privata dimora" nel settore delle intercettazioni *inter praesentes*

Desta interesse, in conclusione, prendere in esame come il concetto di "privata dimora" sia inteso dalla giurisprudenza di legittimità nel particolare ambito delle intercettazioni (76), in quanto il significato attribuito allo stesso circoscrive l'area di efficacia di tale mezzo di ricerca della prova. Anche in questo peculiare settore, infatti, non hanno fatto difetto le interpretazioni contrastanti di cui si è detto nei paragrafi che precedono (77).

### *5.1. La posizione restrittiva della giurisprudenza di legittimità: la nozione di "privata dimora" tra diritto sostanziale e diritto processuale*

Del combinato disposto degli articoli 614 c.p. e 266 (2 e 2 *bis*), il giudice di legittimità ha fornito, nel tempo, alternativamente, una lettura più o meno ampia nell'esegesi della nozione di "privata dimora". Emblematico il contrasto interpretativo emerso dal confronto tra due sentenze piuttosto risalenti (78).
Ultimamente, la Corte sembra aver accolto una definizione più limitata del concetto rilevante in ambito processuale. Questo orientamento si evince da una pronuncia emessa alquanto di recente (79), ove la Sezione Sesta non ha incluso l'Ufficio del Procuratore della Repubblica, entro cui era stata svolta attività di intercettazione, nella categoria dei luoghi di "privata dimora" (80).

(74) Cass., sez. V, 26 ottobre 2023, n. 3446.

(75) In particolare, nel caso esaminato in questo paragrafo si vogliono tracciare le frequentazioni del marito; mentre, nel caso prima analizzato, si viene a conoscenza delle varie conversazioni intrattenute dall'ex moglie nel veicolo.

(76) Il presente paragrafo verterà, in particolare, sulle intercettazioni c.d. ambientali o *inter praesentes*, di cui all'articolo 266, commi 2 e 2 *bis* c.p.p. Più precisamente, l'art. 266, comma 2, recita "[n]egli stessi casi è consentita l'intercettazione di comunicazioni tra presenti, che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Tuttavia, qualora queste avvengano nei luoghi indicati dall'art. 614 del codice penale, l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa". Si veda Bruno, voce *Intercettazioni di comunicazioni o conversazioni*, in *Dig. disc. pen.*, VII, Torino, 1993, 185. Poi, così come introdotto dall'articolo 4, comma 1, lett. a, D. Lgs n. 216 del 2017 e dopo modificato (dapprima dall'art. 1 della l. 9 gennaio 2019, n. 3 e poi dall'art. 2 del D.L. 20 dicembre 2019, n. 161), l'articolo 266, comma 2 *bis* chiarisce che "[l]'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3 *bis* e 3 *quater*, e, previa indicazione delle ragioni che ne giustificano l'utilizzo anche nei luoghi indicati dall'articolo 614 del codice penale, per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'articolo 4".

(77) Come già anticipato alla nota n. 15, l'articolo 266 c.p.p. (che apre il Capo IV, "Intercettazioni di conversazioni o comunicazioni") richiama l'articolo 614 c.p.

(78) Il riferimento va a Cass., sez. I, 20 dicembre 1991, n. 603, in *Cass. pen.*, 1995, 988 ss. e Cass., sez. I, 19 ottobre 1992, n. 604, in *Cass. pen.*, 1995, 990 ss. A proposito si veda il commento congiunto di Scella, *Dubbi di legittimità costituzionale e questioni applicative in tema di intercettazioni ambientali compiute in luogo di privata dimora*, in *Cass. pen.*, 1995, 992 ss. Nella prima pronuncia, un "deposito di carni" non è stato considerato come "privata dimora". Al contrario, nella seconda, un'"agenzia di trasporti" ha ottenuto questa qualifica.

(79) Cass., sez. VI, 25 maggio 2022, n. 32010, in *Giur. it.*, 2022, 2502, Pres. Di Stefano, Rel. D'Arcangelo.

(80) Nello specifico, la Corte di cassazione non ha ammesso "che possa considerarsi luogo di privata ai sensi dell'art. 614 cod. pen. ogni luogo al quale è consentito l'accesso ad un numero indiscriminato o, comunque, elevato di persone" (Cass., sez. VI, 25 maggio 2022, n. 32010, Considerato in diritto, paragrafo 5, nono capoverso). Sulla base di questo presupposto non sono considerati luogo di "privata dimora" anche l'ufficio del sindaco (Cass., sez. II, 21 aprile 1997, n. 2873, *Viveri*) o l'ufficio tecnico di un comune (Cass., sez. I, 13 maggio 2010, n. 24161, *Accomando*). As-

Nell'argomentazione proposta, la Corte ha significativamente seguito le orme del *leading case Prisco* (81). Nel respingere la classificazione del luogo offerta dai difensori dell'imputato (82), infatti, la Corte ha stabilito che sussiste una differenza tra il significato di "privata dimora" desumibile dalle norme di diritto sostanziale e il concetto che si può, invece, trarre a partire dalla lettera del Codice di rito (83), che deve rispettare un diverso bilanciamento degli interessi in gioco (84). D'altro canto, la stessa sentenza *Prisco* affermava che "la giurisprudenza tende ad ampliare il concetto di domicilio in funzione della tutela penale degli artt. 614 e 615-*bis* c.p., mentre tende a circoscriverlo quando l'ambito domiciliare rappresenta un limite allo svolgimento delle indagini" (85). Secondo il ragionamento seguito dalla Corte di Cassazione, dunque, si evince che se una tendenza interpretativa estensiva del concetto di "privata dimora" può essere tollerata – anche se non preferita – a livello sostanziale (86), al contrario, questa si deve ripudiare nel contesto processuale (87).

Tuttavia, visto il suo forte carattere intrusivo, l'attività di intercettazione non solo si pone al servizio della miglior riuscita delle indagini, ma è anche, al tempo stesso, capace di comprime notevolmente i diritti dei soggetti sottoposti a tale misura (88). In considerazione, quindi, del fisiologico conflitto di interessi costituzionali coinvolti, rappresentati, da un lato, dai diritti in capo all'intercettato e, dall'altro, dagli obblighi dell'autorità inquirente, una nozione estensiva in campo processuale sarebbe preferibile in virtù delle maggiori garanzie che sarebbe così possibile assicurare dapprima all'indagato e poi all'imputato (89).

sociando il presente discorso con le considerazioni svolte sull'abitacolo dell'autovettura nel terzo paragrafo del lavoro, la mancata classificazione della stessa entro i luoghi di "privata dimora" è stata elaborata proprio in ambito processuale, e in particolare, in materia di intercettazioni ambientali.

(81) Si tratta della celeberrima Cass., SU, 28 marzo 2006, n. 26795, *Prisco*, *cit.*, 1537 ss. Sul punto la produzione dottrinale è sterminata. Tra gli altri, si vedano Camon, *Le sezioni unite sulla videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi*, *op cit.*; Marinelli, *Le videoriprese al vaglio delle sezioni unite; i limiti di impiego negli spazi riservati di natura extradomiciliare,* in *Riv. it. dir. e proc. pen.*, 2006, 1570 ss. In modo *tranchant*, escludendo che i *privés* di un locale notturno – in cui erano state poste in essere delle videoriprese da parte delle autorità– costituiscano "privata dimora", le Sezioni Unite del 2006 hanno dichiarato che "il concetto di domicilio non può essere esteso fino a farlo coincidere con un qualunque ambiente che tende a garantire intimità e riservatezza. Non c'è dubbio che il concetto di domicilio individui un rapporto tra la persona e un luogo, generalmente chiuso, in cui si svolge la vita privata, in modo anche da sottrarre chi lo occupa alle ingerenze esterne e da garantirgli quindi la riservatezza. Ma il rapporto tra persona e il luogo deve essere tale da giustificare la tutela di questo anche quando la persona è assente" (Considerato in diritto, paragrafo 8, sesto capoverso). Tuttavia, lo stesso caso approfondisce anche la tematica – in questa sede solamente accennata – dell'equiparazione dello strumento investigativo delle riprese visive domiciliari a quello delle intercettazioni ambientali, di modo da applicare la disciplina prevista per queste ultime alle prime. Riprendendo la Corte cost., 11 aprile 2002, n. 135, *cit.*, 1065 ss., la quale, come detto nella nota n. 62, aveva introdotto la distinzione tra "comportamenti a carattere comunicativo" e "comportamenti di tipo non comunicativo", le Sezioni Unite del 2006 ribadiscono che si possa applicare la disciplina legislativa dell'intercettazione tra presenti alla categoria dei "comportamenti comunicativi". Si veda a proposito, Beltrani, *Le videoriprese? Sono una prova atipica. Ma le Sezioni Unite non sciolgono il nodo*, in *Dir. e giust.*, 2006, 40 ss. La distinzione tra "comportamenti comunicativi" e "comportamenti non comunicativi", come già evidenziato, è stata oggetto di un'ulteriore pronuncia del Giudice delle leggi, ossia Corte cost., 16 maggio 2008, n. 149, *cit.*, 1825 ss., per cui si veda Caprioli, *Nuovamente al vaglio della Corte costituzionale l'uso investigativo degli strumenti di ripresa visiva*, in *Giur. cost.*, 2008, 1832B ss. Cfr. anche Rizzo, *Videoregistrazioni domiciliari e l'incerta distinzione tra condotte comunicative e non comunicative*, in *Cass. pen.*, 2017, 722 ss.

(82) Gli stessi lo avevano considerato "privata dimora", servendosi dei tre criteri proposti dalle Sezioni Unite *D'Amico* del 2021. Questi, dunque, se già considerati fallaci in ambito sostanziale, devono escludersi in toto nel contesto procedurale.

(83) Per usare le parole della Corte "[o]ccorre, tuttavia, rilevare come la nozione, delineata dal codice penale, di luogo di privata dimora (...) non possa essere automaticamente trasposta nell'esegesi dell'apparente omologa nozione dettata dall'art. 266, comma 2, cod. proc. pen., in quanto diversi sono i bilanciamenti posti in essere dal legislatore nel delineare il concetto di domicilio, a seconda che il suo intervento operi in funzione della tutela penale di un ambito di riservatezza contro le violazioni e le interferenze illecite altrui o al fine di porre un limite allo svolgimento delle indagini, realizzate nel pubblico interesse al perseguimento dei reati" (Cass., sez. VI, 25 maggio 2022, n. 32010, Considerato in diritto, paragrafo 5, sesto capoverso).

(84) Marandola, *Intercettazioni- L'ufficio del Procuratore della Repubblica non è un luogo di privata dimora*, in *Giur. it.*, 2022, 2502 ss.

(85) Cass., SU, 28 marzo 2006, n. 26795, Considerato in diritto, paragrafo 8, secondo capoverso.

(86) Come messo in evidenza nel paragrafo 2.2.

(87) A questo proposito, si consiglia Solinas, *Lesione della riservatezza, tra garanzia processuale e tutela sostanziale. Brevi osservazioni sulla nozione di "domicilio", tra precedenti processuali e sostanziali di legittimità*, in *Resp. civ. prev.*, 2016, 1609 ss.

(88) Milani, *Processo penale e valori costituzionali nell'insegnamento di Vittorio Grevi*, in *Cass. pen.*, 2012, 388.

(89) Melillo, *Le intercettazioni tra diritto alla riservatezza ed efficienza delle indagini*, in *Cass. pen.*, 2000, 3482 ss. Si veda anche Bargi, voce *Intercettazioni di comunicazioni e conversazioni*, in *Dig. disc. pen.*, Agg. III, Torino, 2005, 795, nella parte in cui riprende la storica Cass., sez. IV, 16 marzo 2000, n. 7063, *Viskovic*, in *Riv. it. dir. e proc. pen.*, 2001, 87. Partendo dall'assunto secondo cui il concetto di "domicilio" di cui all'articolo 14 della Carta costituzionale abbia un significato più vasto di quello ex art. 614 c.p. e ricomprenda, dunque, "tutti i luoghi siano o meno dimora", ne deriva che qualsiasi forma di ingerenza, attuata tramite lo strumento delle intercettazioni, posta in essere nella "privata dimora", deve necessariamente svolgersi in piena ottemperanza dell'articolo 14 Cost.

# Danno erariale indiretto in conseguenza del pagamento della sanzione comminata dal Garante privacy

Corte dei Conti, sezione giurisdizionale di Bolzano; sentenza 9 gennaio 2024, n. 1; Pres. Enrico Marinaro; Consigliere-relatore Francesco Targia; Massimo Giuseppe Urso Referendario.

*È il Privacy manager e non il titolare del trattamento dei dati (legale rappresentante dell'Ente) a rispondere del danno indiretto cagionato a seguito dell'avvenuto pagamento da parte dell'Ente della sanzione irrogata dal Garante per la protezione dei dati personali.*

*Deve ritenersi non sussistente il requisito della colpa grave in capo al titolare per aver confidato nell'operato del responsabile del trattamento e degli incaricati, non potendo essere chiamato ad occuparsi in prima persona degli aspetti tecnici legati alla tutela della privacy, tenuto conto altresì di ulteriori elementi quali le dimensioni dell'Ente, la molteplicità dei compiti assegnati ad un Sindaco di un capoluogo di Provincia, della tecnicità della materia e soprattutto dell'avvenuta o meno predisposizione di un'organizzazione potenzialmente idonea.*

*Al contrario, non va esente da responsabilità, sia pur soltanto per una quota parte del danno (tenuto conto dell'apporto causale fornito da altri soggetti, ossia i dirigenti), il responsabile dei procedimenti amministrativi in materia di protezione dei dati personali che, per un periodo di tempo, ha rivestito anche il ruolo di Privacy Manager, ciò in ragione dei compiti che ineriscono a tali incarichi, i quali presuppongono specifiche competenze con connesse responsabilità.*

*...Omissis...*

**Diritto**

1. Oggetto dell'odierno giudizio è il ristoro dell'indebito pregiudizio patrimoniale subito dal Comune di Bolzano in conseguenza della sanzione irrogata dal Garante per plurime violazioni della disciplina in materia di dati personali. Al riguardo, deve essere preliminarmente precisato che gli atti emanati dal Garante, pur non potendo essere equiparati ad una sentenza passata in giudicato, assumono un valore presuntivo circa l'oggettiva sussistenza della violazione data la particolare competenza specifica del soggetto emanante relativamente alla disciplina di settore. Deve, inoltre, essere evidenziato che tale presunzione trova conferma nell'ampia documentazione prodotta in giudizio dal PM contabile e che gli elementi *ex adverso* dedotti dalla difesa dei convenuti in ordine all'asserita insussistenza di una condotta giuridica appaiono prive di pregio. Infatti, deve osservarsi che l'informazione fornita ai dipendenti sulla raccolta dei *log*, in considerazione della sua genericità, non può considerarsi adeguata, che non rilevano le finalità per le quali la stessa è effettuata, così come l'asserita non attendibilità dei dati raccolti, anche considerato che la conservazione di informazioni, ancorché parziali e imprecise, sui siti internet visitati dai dipendenti appare comunque lesiva del diritto alla loro riservatezza, così come la trasmissione di dati personali sullo stato di salute del lavoratore ai soggetti delegati allo svolgimento delle funzioni datoriali.

2. Ciò premesso, nel merito, il Collegio è chiamato ad accertare, con riferimento ad entrambi i convenuti, la sussistenza dei presupposti, oggettivi e soggettivi, della responsabilità contabile.

Al riguardo, deve osservarsi che sul dott. *...Omissis...*, in quanto legale rappresentante dell'ente (Comune di Bolzano) titolare del trattamento dei dati, ricadeva l'attuazione degli obblighi previsti per tale figura, tra i quali rientra ogni decisione in merito alle modalità del trattamento dei dati personali e agli strumenti da utilizzare. L'ampiezza dei compiti affidati porta a ritenere effettivamente sussistente un obbligo di attivarsi per verificare la conformità della disciplina regolamentare interna a seguito dell'avvenuto mutamento del quadro normativo operato dal d.lgs. 4 settembre 2015, n. 151 e, quindi, astrattamente configurabile una condotta omissiva eziologicamente ricollegabile al danno derivato al Comune dall'avvenuta irrogazione di una sanzione.

Ad un tempo deve evidenziarsi che i compiti e le connesse responsabilità del titolare sono individuate dal legislatore eurounitario e nazionale in modo ampio a tutela del privato leso nei confronti del titolare-persona giuridica. Nel momento, invece, in cui la responsabilità deve riverberarsi sulla persona fisica legale rappresentante dell'ente non si potrà non tenere conto delle dimen-

sioni dell'ente, della molteplicità dei compiti assegnati ad un sindaco di un capoluogo di provincia, della tecnicità della materia e soprattutto dell'avvenuta o meno predisposizione di un'organizzazione potenzialmente idonea. Valutati detti elementi nella concreta fattispecie in esame, il Collegio ritiene non sussistente il requisito della colpa grave, per aver il dott. *...Omissis...* confidato nell'operato del responsabile e degli incaricati e non potendo effettivamente essere chiamato ad occuparsi in prima persona degli aspetti tecnici legati alla tutela della *privacy*. Detta circostanza traspare, peraltro, nello stesso provvedimento di irrogazione della sanzione all'interno del quale il Garante precisa che "*è stato considerato che il titolare del trattamento avesse confidato nella liceità dei trattamenti posti in essere avendo assolto agli obblighi previsti dalla normativa di settore*".

3. A considerazioni diverse deve, invece, addivenirsi in relazione alla posizione dell'altra convenuta, la dott.ssa *...Omissis...*

Infatti, quest'ultima nel periodo *...Omissis...* ha rivestito gli incarichi di responsabile dei procedimenti amministrativi in materia di protezione dei dati personali e, *... Omissis...*, di *Privacy Manager*, compiti questi che presuppongono specifiche competenze con connesse responsabilità. In particolare, la dott.ssa *...Omissis...*, in base alla determina *...Omissis...*, nella qualità di responsabile dei procedimenti amministrativi in materia di protezione dei dati personali, aveva tra gli altri il compito di approvare gli schemi di atti obbligatori e di linee guida e il documento programmatico della sicurezza, nonché predisporre le modifiche al regolamento per il trattamento dei dati sensibili e giudiziari. A seguito del decreto *... Omissis...* ha assunto, poi, il ruolo di *Privacy Manager*, cioè di coordinatore interno delle attività di adeguamento al GDPR.

Ne discende che può ritenersi sussistente a suo carico il contestato obbligo di attivarsi per verificare la conformità della disciplina regolamentare interna al quadro normativo introdotto dal d.lgs. 4 settembre 2015, n. 151, oltre che un generale obbligo di vigilanza sul rispetto della predetta normativa, ed è, quindi, configurabile, anche in questo caso, un comportamento omissivo ricollegabile al danno subito dal Comune a seguito dell'avvenuta irrogazione di una sanzione.

Al riguardo la difesa della convenuta ha segnalato, in primo luogo, la propria totale estraneità rispetto alle condotte omissive contestate rivestendo, all'epoca dei fatti, la qualifica di funzionario dell'Ufficio organizzazione e formazione, come tale privo del potere di adozione di qualsiasi atto di organizzazione e di poteri di verifica relativamente ai trattamenti dei dati posti in essere dai diversi uffici dell'ente. Ha, inoltre, segnalato il ruolo marginale svolto sia come responsabile dei procedimenti amministrativi in materia di dati personali, riguardando l'incarico i soli atti di competenza dell'ufficio di appartenenza, sia di *Privacy Manager*, non avendo autonomi poteri di intervento diretto, ma mere funzioni di coordinamento.

Le argomentazioni non meritano accoglimento.

Dai menzionati determina e decreto emerge, infatti, che la dott.ssa *...Omissis...*, seppur funzionaria e non dirigente, era intestataria di pregnanti compiti in materia di *privacy* inerenti non al solo Ufficio di appartenenza, ma l'intera amministrazione comunale, dato che la struttura in cui la stessa era incardinata, Ufficio organizzazione e formazione, era stata individuata come quella preposta all'attuazione della normativa in materia di *privacy*.

In sede di costituzione in giudizio la difesa della dott. ssa *...Omissis...* ha lamentato l'insussistenza del nesso di causalità tra la condotta contestata e il danno patito dall'ente e l'assenza della colpa grave, dato l'impegno profuso nel settore della *privacy* nonostante le molteplici attività alla stessa affidate.

Anche tali doglianze devono essere disattese.

Deve ritenersi, infatti, che le omissioni contestate siano con evidenza eziologicamente ricollegabili al verificarsi dei comportamenti oggetto di sanzione, che avrebbero potuto essere evitati attraverso un maggiore coordinamento, aggiornate direttive, analisi della normativa e delle novelle intervenute maggiormente attente.

Egualmente può ritenersi sussistente l'elemento psicologico della colpa grave dato che gli episodi presi in considerazione dal garante non sono singoli ma relativi a due tipologie di trattamento massivo dei dati che per l'ampiezza e la generalità dei destinatari (l'intero personale del Comune) non potevano non essere note.

Da ultimo, viene contestata la quantificazione del danno operata dalla Procura erariale, in quanto non si sarebbe tenuto conto dell'ampio arco temporale preso in considerazione dal Garante (2000-2020) a fronte di un periodo di servizio prestato nelle funzioni di responsabile dei procedimenti amministrativi in materia di tutela dei dati personali e *Privacy Manager* limitato, il lungo periodo di assenza *...Omissis...*, delle diverse concause e dei diversi attori incidenti nella determinazione del danno indiretto.

Tali ultime argomentazioni appaiono parzialmente fondate.

*...Omissis...* il Collegio ritiene che effettivamente non risulta si sia tenuto nella dovuta considerazione l'apporto causale fornito dagli altri soggetti coinvolti.

Il riferimento è ai dirigenti dei settori che hanno effettuato i trattamenti massivi dei dati in esame, al dirigente dell'ufficio organizzazione e formazione, struttura preposta all'attuazione della normativa in materia di *privacy*, alle delegazioni di parte pubblica che ha sottoscritto con le organizzazioni sindacali gli appositi accor-

di aventi ad oggetto i trattamenti dei dati risultati non conformi a legge.
Da quanto sopra discende la necessità di rideterminare nella misura complessiva di euro 4.200,00 la quota di danno da porre a carico della dott.ssa *...Omissis...*, determinato tenendo conto dell'arco temporale nel quale era suo dovere adoperarsi, del lungo periodo di assenza *...Omissis...*, della contemporanea attribuzione di altre funzioni e dell'apporto degli altri soggetti coinvolti che hanno causalmente contribuito al trattamento dei dati ritenuto illecito e sanzionato.
4. In conclusione, il Collegio ritiene meritevole di accoglimento la pretesa risarcitoria esercitata nei confronti della dott.ssa *...Omissis...*, mentre reputa di escludere quella promossa nei confronti del convenuto dott. *... Omissis...*
*...Omissis...*

# IL COMMENTO

*di Assunta Palmiero*

**Sommario:** 1. Il caso. – 2. Le sanzioni irrogate dal Garante per la protezione dei dati personali e loro valenza giuridica nel processo contabile. – 3. Il principio di responsabilizzazione del titolare del trattamento (*accountability*) e riflessioni sull'organizzazione dell'Ente (locale). – 4. Conclusioni.

La decisione in commento esamina le componenti strutturali dell'illecito contabile, con particolare riguardo al ristoro dell'indebito pregiudizio patrimoniale subito dal Comune di Bolzano in conseguenza della sanzione irrogata dal Garante per la protezione dei dati personali per plurime violazioni in detta materia.
Il Collegio, valutati gli elementi nella concreta fattispecie in esame, ha ritenuto non sussistente il requisito della colpa grave in capo al legale rappresentante dell'Ente (Comune di Bolzano) che, in quanto tale, rivestiva il ruolo di titolare del trattamento dei dati; al contrario, ha accolto la pretesa risarcitoria nei confronti della funzionaria che aveva ricoperto gli incarichi di responsabile dei procedimenti amministrativi in materia di protezione dei dati personali e di *Privacy Manager*, in ragione degli specifici compiti, con connesse responsabilità, che tali ruoli presuppongono.
In tale contributo si analizza il principio di *accountability* e la necessità da parte della Pubblica Amministrazione di adottare importanti misure organizzative volte alla tutela dei dati personali, sotto il profilo della valutazione dei canonici elementi del danno erariale.

*The commented decision scrutinizes the structural components of the accounting offense, with particular regard to the compensation for the undue financial damage suffered by the Municipality of Bolzano as a consequence of the sanction imposed by the Data protection Authority of personal data for multiple violations in this matter.*
*The Judges, having assessed the elements in the concrete case in question, considered that the requirement of gross negligence on the part of the legal representative of the local Authority (Municipality of Bolzano) who, as such, held the role of data controller was not existent; on the contrary, it accepted the compensation claim against the official who had held the positions of manager of administrative procedures regarding the protection of personal data and of Privacy Manager, due to the specific tasks, with related responsibilities, that these roles presuppose.*
*This contribution analyzes the principle of accountability and the need for the Public Administration to adopt important organizational measures aimed at protecting personal data, with the prospective of evaluating the standard rules related to loss of revenue.*

## 1. Il caso

La pronuncia in esame prende le mosse dall'indebito pregiudizio patrimoniale patito dal Comune di Bolzano a seguito dell'avvenuto pagamento (seppur in misura ridotta) della sanzionata irrogata dal Garante per la protezione dei dati personali, per violazione dell'art. 5, par. 1, lett. a) e c), 8, 9, 35, 13 e 88 del Regolamento europeo n. 2016/679, e degli artt. 113 e 114 del codice della *privacy*, avendo l'Ente posto in essere trattamenti di dati personali dei dipendenti relativi alla navigazione in Internet, in assenza dei presupposti e di idonea informativa, e adottato una modulistica per la fruizione del servizio di assistenza psicologica non conforme al quadro normativo (si prevedeva la conoscenza di dati personali sullo stato di salute dei dipendenti da parte dei soggetti delegati allo svolgimento delle funzioni datoriali).

A fronte di tale ipotesi di danno erariale, la Procura contabile citava in giudizio, dinanzi alla Sezione giurisdizionale della Corte dei conti di Bolzano, il legale rappresentante dell'Ente, in qualità di titolare del trattamento dei dati, e il responsabile dei procedimenti amministrativi in materia di protezione dei dati personali che, per un periodo di tempo, aveva altresì assunto il ruolo di *Privacy Manager*, ossia di coordinatore interno delle attività di adeguamento al GDPR.

La contestazione si appuntava su una condotta omissiva da parte di entrambi i convenuti, i quali, secondo la prospettazione della Procura, non si sarebbero attivati per verificare la conformità della disciplina regolamentare interna rispetto alle intervenute modifiche in materia di trattamento dei dati personali operate dal D.lgs. n. 151 del 2015 (neanche a seguito della pronuncia del Garante del 13.07.2016 "*Trattamento dei dati dei dipendenti mediante posta elettronica e altri strumenti di lavoro*" e neppure in sede di adozione delle "*Linee guida per le procedure di adeguamento del GDPR 2016/679*").

Tale inerzia, inoltre, veniva qualificata come gravemente colposa in quanto non avrebbe riguardato singoli episodi, ma una costante, perdurante violazione della normativa della *privacy* relativamente a due tipologie di trattamenti massivi di dati, noti necessariamente ai convenuti in considerazione della generalità dei destinatari.

I due prevenuti ritualmente costituitisi in giudizio rassegnavano le proprie conclusioni, contestando la prospettazione dell'accusa.

Preliminarmente, la Sezione giurisdizionale adita precisava che gli atti emanati dal Garante assumono un valore presuntivo circa l'oggettiva sussistenza della violazione (data la particolare competenza specifica del soggetto emanante relativamente alla disciplina di settore), evidenziando che tale presunzione trovava conferma nell'ampia documentazione prodotta in giudizio dal PM contabile.

Nello specifico, rispetto alle violazioni contestate, la Sezione osservava che l'informazione fornita ai dipendenti sulla raccolta dei *log*, in quanto generica, non poteva considerarsi adeguata e che non rilevavano, altresì, le finalità per le quali la stessa era stata effettuata, così come l'asserita non attendibilità dei dati raccolti (considerando la conservazione di informazioni sui siti internet visitati dai dipendenti comunque lesiva del diritto alla loro riservatezza), e la trasmissione di dati personali sullo stato di salute del lavoratore ai soggetti delegati allo svolgimento delle funzioni datoriali.

Fatta tale premessa, il Collegio, chiamato ad accertare la sussistenza dei presupposti oggettivi e soggettivi della responsabilità contabile, ha distinto le posizioni dei due soggetti.

Quanto al legale rappresentante del Comune di Bolzano (titolare del trattamento dei dati), i magistrati contabili hanno ritenuto non sussistere nei suoi confronti il requisito della colpa grave e ciò avuto riguardo alla valutazione in concreto della fattispecie posta al loro vaglio. In particolare, la Sezione ha osservato che seppur l'ampiezza dei compiti affidati al Titolare (tra i quali l'obbligo di attivarsi per verificare la conformità della disciplina regolamentare interna) porterebbe a ritenere astrattamente sussistente una condotta omissiva eziologicamente ricollegabile al danno derivato al Comune, tuttavia non si può non tener conto di taluni elementi, quali le dimensioni dell'Ente, la molteplicità dei compiti assegnati ad un Sindaco di un capoluogo di provincia, la tecnicità della materia e soprattutto l'avvenuta o meno predisposizione di un'organizzazione potenzialmente idonea.

Sul punto, il Collegio ha ritenuto che il Sindaco, avendo confidato nell'operato del responsabile e degli incaricati, non poteva essere chiamato ad occuparsi in prima persona degli aspetti tecnici legati alla tutela della *privacy*; circostanza, questa, sottolinea il Collegio, che sarebbe emersa dallo stesso provvedimento sanzionatorio nel quale il Garante precisava che "*è stato considerato che il titolare del trattamento avesse confidato nella liceità dei trattamenti posti in essere avendo assolto agli obblighi previsti dalla normativa di settore*".

La Sezione è pervenuta, invece, a conclusioni diverse in relazione alla posizione dell'altra convenuta, la quale, seppur funzionaria e non dirigente, era, secondo il Collegio, in ogni caso intestataria di pregnanti compiti in materia di protezione dei dati personali inerenti, peraltro, non il solo Ufficio di appartenenza (Ufficio organizzazione e formazione), ma l'intera amministrazione comunale, posto che la struttura in cui la stessa era incardinata era stata individuata come quella preposta all'attuazione della normativa in materia di *privacy*.

Nello specifico, il Collegio ha sottolineato che gli incarichi di responsabile dei procedimenti amministrativi

in materia di protezione dei dati personali e di *Privacy Manager*, che la stessa aveva ricoperto, presuppongono specifici compiti con connesse responsabilità, ritenendo sussistere, quindi, il contestato obbligo in capo alla funzionaria di attivarsi per verificare la conformità della disciplina regolamentare interna al quadro normativo introdotto dal richiamato D.lgs. n. 151 del 2015, oltre che un generale obbligo di vigilanza sul rispetto della predetta normativa.
Il Collegio ha ritenuto, quindi, configurabile, un comportamento omissivo eziologicamente ricollegabile al danno subito dall'Ente, connotato da colpa grave.
Pertanto, ha accolto la domanda proposta nei suoi confronti, operando, tuttavia, una diversa quantificazione della pretesa risarcitoria. Invero, i Giudici di *prime cure* hanno rideterminato la quota di danno, ritenendo che non fosse stato tenuto nella dovuta considerazione l'apporto causale fornito dagli altri soggetti coinvolti, ossia dei dirigenti dei settori che avevano effettuato i trattamenti massivi dei dati in questione.

## 2. Le sanzioni irrogate dal Garante per la protezione dei dati personali e loro valenza giuridica nel processo contabile

Il danno indiretto oggetto della sentenza in esame riguarda l'indebito pregiudizio patrimoniale subito dal Comune di Bolzano, in conseguenza dell'avvenuto pagamento della sanzione irrogata dal Garante per la protezione dei dati personali.
Quale autorità di controllo, al Garante sono attribuiti, come noto, i poteri indicati dall'art. 58 GDPR, tra i quali si annoverano i poteri amministrativi e, in particolare, ai fini che qui rilevano, i poteri sanzionatori di cui lo stesso dispone in base all'art. 166, comma 3, del D.lgs. n. 196 del 2003 (con riferimento all'adozione delle sanzioni amministrative pecuniarie si ha riguardo all'art. 83 dello stesso Regolamento (1)).
In merito a tali sanzioni, e al potere del Garante di irrogarle (2), di recente la giurisprudenza di legittimità si è espressa affermando un importante principio di diritto, ossia che "*In tema di violazioni della disciplina relativa al trattamento dei dati personali, il Garante per la protezione di questi ultimi può infliggere sanzioni amministrative pecuniare anche ad autorità pubbliche e/o organismi pubblici*" (3).
Sul punto, il Supremo consesso ha altresì evidenziato che numerose sono le pronunce di legittimità (4) intervenute in procedimenti aventi ad oggetto contestazioni di sanzioni inflitte dal Garante ad enti e/o organismi pubblici, e la Suprema Corte, accogliendo o respingendo i corrispondenti ricorsi, annullando o confermando le sanzioni pecuniarie irrogate dal Garante, mai ha posto in dubbio (così implicitamente riconoscendola) il relativo potere in capo a quest'ultimo.
Fatta tale premessa di ordine generale, si osserva che il Collegio, nella sentenza in commento, ha affrontato preliminarmente il tema della valenza giuridica degli atti emanati dal Garante dando conto, in particolare, del loro peso probatorio, ritenendo che gli stessi (pur non potendo essere equiparati ad una sentenza passata in giudicato), assumano un valore presuntivo circa l'oggettiva sussistenza della violazione, data la particolare competenza specifica del soggetto emanante relativamente alla disciplina di settore.
A conforto di tale assunto, si osserva altresì che in altra pronuncia i magistrati contabili hanno sostenuto che gli atti sanzionatori del Garante sono ascrivibili, secondo precedenti giurisprudenziali conformi, agli atti fidefacienti ai sensi dell'art. 2700 c.c. (5).
Da tali pronunce appare chiara, quindi, la volontà da parte del Giudice contabile di precisare il valore da attribuire agli atti emanati dal Garante, restando ferma, ovviamente, l'attività del Collegio volta alla valutazione dei canonici elementi del danno erariale.

## 3. Il principio di responsabilizzazione del titolare del trattamento (*accountability*) e riflessioni sull'organizzazione dell'Ente (locale)

Il Regolamento europeo n. 679/2016 ha posto nell'art. 24, come principio cardine di tutta la disciplina sulla protezione dei dati personali, il concetto di *accountability* (o responsabilizzazione, come tradotto dal legislatore italiano) che prevede in capo al "titolare" un obbligo

(1) "*Il Regolamento UE 2016/679 prevede negli artt. 83-84 regole sulle sanzioni amministrative per la violazione di norme contenute nella medesima fonte normativa. L'art. 83 si apre con il rinvio ai principi generali di effettività delle sanzioni pecuniarie, di proporzionalità e di «dissuasività», vale a dire costruite anche nell'ammontare in modo da orientare verso una condotta conforme già prima dell'eventuale violazione. Questi principi si inseriscono nella nozione di sanzione amministrativa di fonte comunitaria (...)*". In tal senso, e con riguardo ai poteri sanzionatori del Garante v. ANTONIAZZI, *Le sanzioni amministrative*, in *I dati personali nel diritto europeo* a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 1093 ss.

(2) Il Garante per la protezione dei dati personali è l'organo competente ad irrogare le sanzioni, lo stesso dovrà avere cura di valutare caso per caso le violazioni, affinché le sanzioni siano sempre effettive, proporzionate e dissuasive (art. 83, comma 1, reg. UE 2016/679, d'ora innanzi GDPR). Andranno tenute in debito conto le circostanze di cui all'art. 83, comma 2, GDPR, ossia la natura, la gravità, la durata della violazione, il carattere doloso o colposo della stessa, le categorie di dati personali interessate dalla violazione, ecc.

(3) Cass. 11 ottobre 2023, n. 28385.

(4) Cass. 11 settembre 2023, n. 26267 e Cass. 21 ottobre 2021, n. 29323, riguardanti entrambe sanzioni del Garante contro la Regione Autonoma Valle D'Aosta; Cass. 29 marzo 2023, n. 8942, concernente una sanzione del Garante contro la Provincia di Benevento; Cass. 1° marzo 2023, n. 6177, avente ad oggetto una sanzione del Garante contro l'Istituto Nazionale per la Previdenza Sociale.

(5) Corte conti, Sez. giur. reg. Calabria 31 ottobre 2019, n. 429.

specifico di responsabilizzazione, risultando quale unico responsabile in ordine alle scelte da effettuare (6).
In particolare, tale concetto non si risolve nella sola responsabilità, ma coinvolge aspetti come la competenza e l'affidabilità nella gestione dei dati, richiedendo al titolare del trattamento il rispetto degli obblighi previsti nel Regolamento, unitamente ad una continua attività di controllo e verifica delle proprie attività. In altre parole, in base al principio di *accountability* il titolare del trattamento deve adottare misure appropriate ed efficaci per attuare i principi posti alla base della protezione dei dati ed ha l'obbligo di dimostrare che tali misure siano state adottate (7).
Con riguardo alle misure da porre in essere, il citato art. 24 GDPR non reca, tuttavia, elenchi o riferimenti specifici a quali esse siano e, quindi, è necessario procedere ad una valutazione da effettuarsi caso per caso, attraverso un'attenta analisi della situazione specifica. In altri termini, l'approccio "*checklist*" risulta superato da un approccio permeato sulla contestualizzazione, in quanto "*le scelte derivanti dalla conoscenza delle dinamiche interne ad un'organizzazione sono più efficaci delle scelte operate al mero fine di adeguarsi ad una norma*" (8).

Sarà necessaria, quindi, l'elaborazione di specifici modelli organizzativi, adeguati al settore di interesse in cui viene svolta l'attività (9).
Tenuto conto, quindi, del principio di *accountability*, definito uno dei pilastri in tema di trattamento dei dati personali (10), in dottrina si è osservato come la sentenza n. 1 del 2024 (qui in commento), nell'aver mandato esente da responsabilità il Sindaco, si sia posta in contrasto con la prevista responsabilità "generale" del Titolare del trattamento, così come espressamente definita nel considerando 74 del GDPR (11). A tal riguardo, si è puntualizzato che: "*Il solo fatto di avere nominato un responsabile protezione dati (ai sensi degli artt. 37-39 GDPR) e una Privacy manager, è stato sufficiente per riconoscere il Sindaco come estraneo ad ogni responsabilità erariale sulla scorta della non condivisibile motivazione secondo cui "non poteva effettivamente essere chiamato ad occuparsi in prima persona degli aspetti tecnici legati alla tutela della privacy*" (12); ed ancora, si è detto che il ricorso all'istituto della delega di funzioni (13) non aveva mai avuto come conseguenza l'esenzione completa di responsabilità da parte del Titolare che ne facesse ricorso (14), e che tale pronuncia potrebbe avere l'effetto di disincentivare i soggetti incardinati all'interno di un'organizzazione a ricoprire i ruoli *privacy*.
Con specifico riguardo a tali ruoli si osserva, in generale, che la gestione dei dati personali non costituisce più solo un adempimento, ma diviene un processo che in-

(6) L'art. 24 sancisce il principio della responsabilità del titolare del trattamento, in quanto, al paragrafo 1 del suddetto articolo, il legislatore indica che è compito del titolare "*mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di mostrare, che il trattamento è effettuato conformemente al regolamento*". Ancora, al paragrafo 2, si enuncia che "*dette misure sono riesaminate e aggiornate qualora necessario*", affermandosi la centralità del ruolo del Titolare e della sua responsabilità nell'adozione di misure sia tecniche che organizzative.

(7) Settimio, *Obblighi e responsabilità dei soggetti del trattamento: titolare e responsabile a confronto*, nota a Cass. 23 luglio 2021, n. 21234, in *www.GiustiziaCivile.com*, 18 marzo 2022, ove si precisa: "*D'altro canto, mentre da un lato il "titolare" deve ponderare bene la scelta dei collaboratori ai quali affidare la qualifica di "responsabili" del trattamento per assicurare una solida tutela degli interessati e per non incorrere in sanzioni, dall'altro, il "responsabile" dev'essere in grado di fornire idonee garanzie che assicurino il pieno rispetto delle disposizioni in materia di protezione dei dati personali; per tale ragione, dev'essere in possesso di competenze qualificate e deve garantire una conoscenza specialistica della materia ed una particolare affidabilità fondata su aspetti etici e deontologici. Di conseguenza, in tutti i casi in cui il "responsabile" del trattamento ecceda i limiti di utilizzo dei dati fissati dal titolare o attui condotte che determinano finalità o mezzi del trattamento, diventa "titolare" ipso iure della gestione illecita dei dati secondo la disposizione dell'art. 28 par. 10 del GDPR e ne risponde come tale insieme all'effettivo titolare secondo quanto previsto dall'art. 82 del Regolamento, sfociando nella disciplina della contitolarità*".

(8) Capparelli, *Regolamento – 27/04/2016 – n. 679 art. 24 – Responsabilità del titolare del trattamento*, in *IUS*, ove si precisa che il Regolamento e l'art. 24 GDPR analizzato non prevedono un adempimento meramente formale degli obblighi in materia di *privacy* ma, al contrario, un'attività concreta e sostanziale da parte degli addetti al trattamento dei dati personali. Si tratta di "*un cambio di rotta che ha una matrice culturale e che detta un approccio rivoluzionario all'osservanza delle disposizioni in campo data protection per le organizzazioni che entrano in contatto con i dati personali*".

(9) Brizzi, *Il GDPR in ambito giudiziario: fino a che punto può spingersi l'accountability?*, in *IUS*, 11 dicembre 2018.

(10) Iaselli, *Il principio di accountability: uno dei pilastri del GDPR*, in *Altalex*, all'indirizzo <https://www.altalex.com/documents/news/2018/02/13/il-principio-di-accountability-uno-dei-pilastri-del-gdpr.>.

(11) La responsabilità generale del Titolare del trattamento è prevista dal considerando (74) del GDPR, ai sensi del quale "*È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche*".

(12) Iadecola, *Danno erariale conseguente al pagamento della sanzione inflitta dal Garante Privacy*, in *Altalex*, all'indirizzo <https://www.altalex.com/documents/news/2024/01/26/danno-erariale-conseguente-pagamento-sanzione-inflitta-garante-privacy>.

(13) La delega di funzioni è prevista dall'art. 2-*quaterdecies* d.lgs. n. 101 del 2018, ai sensi del quale "*il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità*".

(14) In generale, l'atto di delega non comporta un trasferimento definitivo di competenza dal delegante al delegato.

cide profondamento sull'organizzazione di ogni azienda o Ente, attraverso l'individuazione di due figure, vale a dire il Titolare e il Responsabile del trattamento; il Regolamento ha introdotto, inoltre, la figura del "Responsabile per la protezione dei dati" o Data Privacy Officer (DPO).

Occorre dar conto altresì, avuto riguardo alla sentenza in esame, della figura del *Privacy Manager* (15), non prevista dal GDPR, ma dalla norma UNI 11697:2017 "*Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali – Requisiti di conoscenza, abilità e competenza*", la quale definisce diversi profili professionali relativi al trattamento e alla protezione dei dati personali (prevedendone anche i requisiti di accesso), tra cui appunto il *Manager* della *privacy*.

Si tratta di una figura professionale, dotata di un elevato livello di conoscenze e competenze, che garantisce l'adozione di idonee misure organizzative nel trattamento di dati personali e che coordina le attività di trattamento di dati personali in uno specifico contesto organizzativo.

Da tali disamine sembra emergere, quindi, come la Pubblica Amministrazione, nella specifica funzione amministrativa di tutela dei dati personali, sia chiamata ad adottare importanti misure organizzative. Tra queste si considera molto importante la precisa determinazione e la corretta distribuzione dei ruoli che all'interno dell'organizzazione devono essere svolti per dare corretta attuazione al GDPR.

Nello specifico, questo non comporta soltanto l'individuazione delle diverse figure organizzative necessarie, ma in ragione dei compiti che queste sono chiamate a svolgere (sicuramente trasversale rispetto alle altre molteplici funzioni amministrative in cui i dati personali vengono trattati), richiede anche la loro corretta integrazione con il complesso dell'organizzazione amministrativa (16).

Invero, il GDPR, ad esempio, non si occupa della natura e dell'articolazione dei titolari all'interno delle varie realtà organizzative e, al riguardo, c'è chi ha posto in rilievo l'approfondimento della figura del titolare del trattamento nella peculiare prospettiva dell'Ordinamento e dell'organizzazione degli Enti locali (17) (per certi versi in maniera sovrapponibile a quanto valutato dal Collegio); in particolare, si è ritenuto necessario confrontare il complesso sistema di responsabilità e attività poste in capo al titolare con l'ordinamento proprio degli Enti locali, affermando che tale intreccio porta "*inevitabilmente non a individuare il titolare nel sindaco, ma ad un modello di "titolare diffuso", esattamente come avviene più in generale per le altre funzioni degli enti. Occorre, cioè, che il lungo elenco delle "mansioni" del titolare venga allocato all'organo che secondo l'ordinamento ha titolo per svolgerla*".

In altre parole, secondo tale tesi, la natura complessa e composita dei compiti che il GDPR attribuisce al titolare e le articolate competenze degli organi – di governo o gestionali – di comuni e province, comporta che, in ossequio al principio di responsabilizzazione (e in spregio ad una semplicistica identificazione del titolare con il Sindaco (18) negli Enti locali o, in analogia, con il Presidente per la Provincia) questa complessità venga disciplinata attraverso un puntuale atto di organizzazione, adottato dall'organo esecutivo. Tale atto assolverebbe alla funzione di collegare, almeno nei profili essenziali, i compiti del titolare ai soggetti funzionalmente competenti.

Sovrapponibile per certi versi a tale tesi è la stessa valutazione operata dal Collegio nella sentenza qui in commento, che nell'evidenziare i compiti e le connesse responsabilità del titolare-persona giuridica, individuate in modo ampio dal legislatore eurounitario e nazionale, ha valutato gli elementi concreti della fattispecie una volta che le responsabilità devono riverberarsi sulla persona fisica (legale rappresentante dell'ente).

(15) L'approfondimento è disponibile al seguente link <https://asapiens.eu/2022/07/29/chi-e-il-privacy-manager/>. La figura del *Privacy Manager* si distingue da quella del DPO (Responsabile della protezione dei dati), che rinviene la sua disciplina nel GDPR (artt. dal 37 al 39). A differenza del DPO, che gode di una posizione di indipendenza rispetto all'azienda, il *Manager* della *Privacy* è parte dell'organizzazione aziendale, assiste il titolare nelle materie legate alla *privacy* ed è un suo collaboratore. La differenza del *Privacy Manager* con le altre figure apicali aziendali, invece, è nel possedere una specifica formazione e delle specifiche abilità nella materia della *privacy* e, di conseguenza, la possibilità di comprendere e intervenire prontamente sulle eventuali criticità che dovessero essere riscontrate. Come osservato da Capone, *Responsabile Privacy in azienda: nomina, requisiti e differenze con le figure previste dal GDPR*, in *E commerce legale*, all'indirizzo <https://ecommercelegale.it/gdpr/responsabile-privacy-azienda/>, l'introduzione della figura del *Privacy Manager* deriva soprattutto dal principio di *accountability* (art. 24 del GDPR) che richiede al titolare di mettere in atto tutte le misure tecniche e organizzative adeguate per garantire (e dimostrare) che il trattamento sia effettuato secondo il Regolamento.

(16) Bombardelli, *Dati personali (tutela dei)*, voce dell'*Enc. Dir.*, *I Tematici*, III, Milano, 2022, 362 ss.

(17) Tirabassi, *L'attuazione del GDPR. Un modello organizzativo per gli Enti locali*, in *Azienditalia*, 2018, 988 ss.

(18) "*Riproposta recentemente anche nel Quaderno Anci n. 11/2018, laddove a pag. 5, si afferma che responsabilità ultima dell'attuazione del GDPR cade sul titolare del trattamento, figura che negli enti locali è ricoperta dal Sindaco*". Sul punto, cfr. Tirabassi, *L'attuazione del GDPR. Un modello organizzativo per gli Enti locali*, cit., 990.

## 4. Conclusioni

Il tema della personalizzazione dell'illecito e la valorizzazione dell'elemento soggettivo (19) connotano senza dubbio, in maniera significativa, la sentenza n. 1/2024 della Sezione giurisdizionale di Bolzano.

Nel rigettare la domanda proposta nei confronti del titolare del trattamento dei dati – ascrivendo la responsabilità nei soli confronti del responsabile dei procedimenti amministrativi in materia di protezione dei dati personali (che al contempo rivestiva, anche se per un periodo limitato, la qualifica di *Privacy manager*) – il Collegio ha inteso calare la normativa europea nella fattispecie concreta, interpretando le norme chiave in tema di protezione dei dati personali avuto riguardo agli elementi costitutivi della responsabilità erariale, specie dell'elemento soggettivo per l'interpretazione offerta dalla giurisprudenza.

In tal modo, la Sezione ha considerato una pluralità di compiti ed elementi significativi del complesso delle funzioni in capo al Sindaco attribuendo loro valore scriminante. Al contrario, la valutazione dei compiti e delle connesse responsabilità in capo al responsabile hanno portato ad un diverso giudizio nei suoi confronti, nonostante si trattasse di un funzionario e non di un dirigente (tale dato è stato valorizzato solo con riguardo alla rideterminazione della sanzione, ritenendo che una quota parte del danno dovesse esser posta in capo ai dirigenti responsabili).

Emerge, quindi, come la sentenza in esame abbia ricondotto la gestione da parte di una Pubblica amministrazione della disciplina in materia di *privacy*, e del principio di *accountability* ad essa strettamente connesso, nell'ambito dei principi che governano la responsabilità contabile.

Nello specifico, ritenendo sussistente la responsabilità erariale in capo al Funzionario e rigettando, invece, la domanda proposta nei confronti del Sindaco, per carenza dell'elemento soggettivo della colpa grave, tale pronuncia ha chiaramente operato una distinzione dei ruoli nell'ambito dell'Ente di appartenenza dei due convenuti.

In altri termini, dalla decisione del Collegio discende una chiara indicazione nell'operare una netta distinzione tra le due figure in ragione dei compiti ad essi rispettivamente attribuiti, valutate nel complesso della realtà dell'Ente locale.

In tal senso, la sentenza in questione non pare isolata se si tiene conto di altre pronunce del giudice contabile che, in materia di violazione della normativa sulla *privacy*, hanno chiarito la possibile modalità di ripartizione delle sanzioni in ragione della responsabilità personale (20).

In conclusione, può dirsi che la violazione della legislazione in materia di dati personali da parte degli Enti pubblici (tenuto conto che il Regolamento europeo 2016/679 non fa distinzione tra ambito pubblico e privato) costituisce condotta gravemente colposa, fonte di responsabilità personale, che comporta l'obbligo del risarcimento del danno erariale quantificato in misura pari alla sanzione amministrativa pecuniaria irrogata dal Garante, ai sensi degli artt. 161-166 del Codice privacy (21).

(19) La giurisprudenza della Corte dei conti, in più occasioni, ha avuto modo di ribadire che "*del danno indiretto relativo all'irrogazione di sanzioni del Garante della Privacy per la diffusione di dati sensibili possa essere chiamato a rispondere chi, con condotta gravemente sprezzante degli obblighi normativi vigenti in subiecta materia, abbia leso il diritto alla tutela della riservatezza, causando per sua esclusiva colpa l'irrogazione della sanzione, così da creare un danno erariale, in quanto il pagamento di somme con denaro pubblico a causa dell'inosservanza di obblighi imposti normativamente costituisce un aggravio di spesa e sottrae le relative somme all'attuazione degli scopi istituzionali*". In tal senso, Corte conti, Sez. giur. reg. Lazio 14 settembre 2021, n. 672.

(20) Corte conti, Sez. giur. reg. Sardegna 12 aprile 2018, n. 73, la quale, analizzando la possibilità di ascrivere il danno erariale ai sensi dell'art. 1, comma 1-*quater*, l. n. 20 del 1994 – il quale testualmente dispone che "*se il fatto dannoso è causato da più persone, la Corte dei conti, valutate le singole responsabilità, condanna ciascuno per la parte che vi ha preso*" – ha puntualizzato come "*Secondo la prevalente giurisprudenza (cfr. tra l'altro, Sez. III centrale n. 743 del 2012 e Sez. II centrale n. 402 del 2013), la disposizione consente che la ripartizione del danno tra più soggetti responsabili sia effettuata dal giudice anche in proporzioni diverse da quelle prospettate dall'attore pubblico, essendo rimessa alla fase del giudizio la valutazione dell'incidenza causale di ciascuna condotta illecita rispetto al danno prodotto, con le determinazioni che ne conseguono in termini di quantificazione del danno addebitabile a ciascuno dei corresponsabili. La stessa disposizione va intesa nel senso che – in ipotesi di più convenuti – il danno possa essere addebitato all'unico soggetto ritenuto responsabile dell'illecito, ove l'unica condotta illecita sia stata da sola sufficiente a determinare l'evento lesivo, trattandosi comunque, anche in questo caso, della valutazione delle condotte più convenuti e dell'accertamento dell'apporto causale fornito alla produzione del danno (cfr., sul punto, Sez. II centrale n. 741 del 2015)*".

(21) D'AGOSTINO PANEBIANCO, *Lineamenti di responsabilità derivanti dalla violazione al trattamento dati*, in *Eur. dir. priv.*, 2020, 237.

# Accesso ai dati personali detenuti dalla P.A.: GDPR, legge 241, rimedi

T.A.R Veneto; sezione terza; sentenza 18 dicembre 2023, n. 1903; Pres. Farina; Est. Nasini; ...*Omissis*... c. Ministero dell'Interno (Avvocatura Distrettuale dello Stato di Venezia).

*Non sono accessibili le informazioni in possesso di una pubblica amministrazione che non abbiano forma di documento amministrativo, salvo quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, in materia di accesso a dati personali da parte della persona cui i dati si riferiscono.*

*Il diritto di accesso vantato dai consociati nei confronti degli atti detenuti dalla pubblica amministrazione deve necessariamente essere esercitato con riferimento a documenti specifici, già formati ed esistenti, non potendo le loro istanze di accesso afferire a notizie e/o a informazioni che, per poter essere fornite, presuppongono lo svolgimento di attività di ricerca e di elaborazione da parte dell'Amministrazione*

...*Omissis*...

**Svolgimento del processo**

Con ricorso depositato in data 26 settembre 2023, il ricorrente, in giudizio personalmente, ha chiesto, ai sensi dell'art. 116 c.p.a., che l'intestato TAR provveda ad accertare e dichiarare l'illegittimità del diniego parziale frapposto dall'Amministrazione resistente all'istanza di accesso agli atti ex l. n. 241 del 1990 presentata dal ricorrente medesimo in data 30.07.2023, con conseguente accertamento del diritto dello stesso ad accedere a tutti i documenti amministrativi cartacei, digitali e informativi di cui alla predetta istanza, inclusi i file digitali originali della posta elettronica certificata e della -OMISSIS-, i dati, i metadati, le date e gli orari in riferimento ... *Omissis*... e della posta elettronica certificata, la corrispondenza di ogni natura e genere con cui la ...*Omissis*... fu trasmessa al ...*Omissis*..., l'espediente ovvero le circostanze e il modo in cui essa fu acquisita. Con particolare riguardo alla posta elettronica e alla ...*Omissis*..., in particolare, il ricorrente richiederebbe alla P.a. i riscontri di come ne è entrata in possesso, in che data, a che ora, in quale luogo e da quale fonte esatta. Quindi il ricorrente ha chiesto che alla P.a. venga ordinata l'ostensione dei documenti di cui sopra.

Si è costituita in giudizio l'Amministrazione resistente contestando l'ammissibilità e fondatezza del ricorso e chiedendone il rigetto. La parte ricorrente ha depositato memoria difensiva.

All'esito dell'udienza del 13 dicembre 2023 la causa è stata trattenuta in decisione.

Il ricorrente, nel ricorso, lamenta la mancata ostensione dei seguenti documenti:

I. istanza del 13.03.2023, con cui il ricorrente ha formulato istanza di accesso agli atti ex l. n. 241/90;

II. nota del Dirigente del ...*Omissis*..., in data 16.03.2023, con cui è stato eccepito al ricorrente che "la domanda risulta oltremodo generica";

III. istanza integrativa del 20.03.2023, con cui il ricorrente ha integrato la precedente istanza di accesso agli atti ex l. n. 241/90, datata 13.03.2023;

IV. messaggio di posta elettronica del ricorrente del 14.12.2022;

V. messaggio di posta elettronica del ricorrente del 15.12.2022;

VI. ...*Omissis*... rilasciato in data 14.12.2022 dall'...*Omissis*...;

VII. -...*Omissis*... di ...*Omissis*... ...*Omissis*..., documento da egli richiamato nelle sue giustificazioni;

VIII. comunicazione o segnalazione in formato cartaceo, digitale o di posta elettronica istantanea, proveniente da un superiore gerarchico del ricorrente, da un collega del ricorrente, da Autorità o soggetti terzi, che abbiano avanzato al Dirigente del ...*Omissis*..., o a terzi, una ... *Omissis*..., ex art. 12, d.p.r. n. 737/81, da cui lo stesso Dirigente del ...*Omissis*... abbia tratto elementi fondanti per procedere alla contestazione degli addebiti;

IX. i dati, i metadati, la data, gli orari, le fonti e le modalità di ricezione, relativi alla ...*Omissis*... (così descritta nella contestazione degli addebiti);

X. il messaggio/i di posta elettronica integrale (originale) «All. 2: corrispondenza via mail con l'organizzazione del ...*Omissis*... -» del Prof ...*Omissis*... presidente ...*Omissis*... (la xerocopia dell'ultima release ostesa al ricorrente mancando della stringa dati, relativi anche a data e ora di spedizione).

Il ricorrente ha lamentato, altresì, che entrambi i verbali di accesso, sia quello del 02.08.2023 che quello del 03.08.2023, recano in oggetto gli estremi di un'i-

stanza sconosciuta mai avanzata dal ricorrente in data 20/7/2023, l'istanza di accesso rilevane essendo quella datata 30.07.2023.
Inoltre, secondo parte ricorrente la documentazione ostesa sarebbe stata incompleta anche perché non gli sarebbe stato consegnato, non essendo fisicamente presente nel fascicolo esibito nel corso dell'accesso del 2 agosto 2023, il documento rubricato "1, 16/11/2022 Nota riservata al Questore".

**Motivi della decisione**
Occorre premettere che l'istanza di accesso presentata dal ricorrente è espressamente promossa ai sensi dell'art. 22, l. n. 241 del 1990, come precisato anche nel ricorso introduttivo del presente giudizio.
Ai sensi della suddetta disposizione, per quanto in questa sede di interesse, per "documento amministrativo" si intende ogni rappresentazione grafica, ...*Omissis*... cinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale;
Non sono accessibili le informazioni in possesso di una pubblica amministrazione che non abbiano forma di documento amministrativo, salvo quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, in materia di accesso a dati personali da parte della persona cui i dati si riferiscono.
Per quanto in questa sede di interesse, va ricordato che «come più volte chiarito dalla giurisprudenza amministrativa, il diritto di accesso vantato dai consociati nei confronti degli atti detenuti dalla pubblica amministrazione deve necessariamente essere esercitato con riferimento a documenti specifici, già formati ed esistenti, non potendo le loro istanze di accesso afferire a notizie e/o a informazioni che, per poter essere fornite, presuppongono lo svolgimento di attività di ricerca e di elaborazione da parte dell'Amministrazione (cfr. *ex multis*, T.A.R. Lazio, ...*Omissis*..., sent. n. 4182/2022; Cons. Stato, Sez. IV, sent. n. 1751/2022)» (T.A.R. Lazio, sez. III, 26 gennaio 2023, n. 1438).
Premesso quanto precede, va anzitutto rilevato come non siano messi in discussione tanto la legittimazione, quanto l'interesse del ricorrente all'accesso, atteso che, infatti, la P.a. ha accolto, sia pure parzialmente la domanda dell'istante.
Occorre dunque solo verificare se quanto il ricorrente lamenta non essere stato osteso possa e debba esserlo ai sensi delle citate disposizioni degli artt. 22 e ss. l. n. 241 del 1990.
Sotto un primo profilo, la difesa dell'Amministrazione ha dato conto del fatto per cui il riferimento, nei verbali del 2 e 3 agosto 2023, agli estremi di un'istanza sconosciuta è frutto di un errore materiale, l'istanza presa in considerazione dalla P.a. è comunque quella del 30 luglio 2023.
Per quanto concerne, invece, i documenti dal n. I al n. VII che precede, la domanda di accesso di parte ricorrente non può essere accolta, trattandosi di documenti che risultano essere già nella disponibilità del ricorrente medesimo o addirittura da lui formati, o, comunque, il cui contenuto è già di sua conoscenza, di tal che non può ritenersi sussistere un interesse all'ostensione.
Pertanto, in parte qua, il ricorso è infondato.
Con riguardo, invece, al documento n. VIII, si tratta di una indicazione meramente generica ed eventuale, rispetto alla quale, in mancanza di dati certi circa l'esistenza del documento medesimo, non ne può essere disposta l'ostensione, alla luce dell'insegnamento giurisprudenziale sopra ricordato.
Per quanto concerne la nota riservata al Questore con data 16 novembre 2022, l'Amministrazione ha già risposto che il documento in questione non è stato osteso perché "afferisce ad altra e diversa vicenda", di talché in mancanza di elementi che possano far ritenere detto documento effettivamente pertinente al ...*Omissis*... di interesse del ricorrente – in relazione al quale si fonda sostanzialmente il diritto di accesso dallo stesso vantato –, la determinazione della P.a. non è censurabile, la stessa, quindi, essendo incorsa in un errore nell'avere originariamente inserito nell'elenco degli atti del procedimento anche la suddetta nota.
Pertanto, anche in parte qua il ricorso non può essere accolto.
In ordine alla ...*Omissis*... oggetto di contestazione, premesso che, a quanto consta, parte ricorrente ha il documento "cartaceo", ma non gli è stato osteso il file "digitale" o elettronico, recante la ...*Omissis*... medesima, nella memoria difensiva dell'Avvocatura nel presente giudizio è stato dato conto dell'avvenuta acquisizione della ...*Omissis*... da parte del Dirigente del G.I.P.S. – non viene precisato, d'altronde, come e da dove – il quale avrebbe proceduto alla stampa di una copia cartacea.
A tal proposito, ben si comprendono i quesiti che muovono le contestazioni del ricorrente in ordine alla "fonte" e alle modalità in concreto di "acquisizione" della ... *Omissis*..., e che, eventualmente, potrebbero essere oggetto di valutazione, se necessario, in sede di giudizio relativo al ...*Omissis*...: d'altronde, come già sopra ricordato, l'accesso c.d. documentale ex artt. 22 e ss., l. n. 241 del 1990, è finalizzato all'acquisizione di "documenti", cioè di atti preformati e detenuti dalla P.a., e non, invece, alla esposizione di dati o informazioni, né alla imposizione all'Amministrazione dell'obbligo di procedere alla formazione ad hoc di un documento recante i suddetti dati.

Ciò implica che la richiesta relativa alla "ostensione" di tutte le informazioni dedotte dal ricorrente non può essere accolta.
Può invece essere accolta la domanda di ostensione del file "digitale" o informatico o elettronico relativo alla suddetta ...*Omissis*...: l'avere l'Amministrazione, nel presente giudizio, infatti, dato conto dell'intervenuta "acquisizione" della ...*Omissis*..., tantopiù che sulla scorta della stessa è stato iniziato il ...*Omissis*... nei confronti del ricorrente, fa presumere che la P.a. detenga il file elettronico o digitale o informatico, sulla scorta del quale è stata poi effettuata la stampa della ...*Omissis*... già in possesso di parte ricorrente.
Pertanto, la domanda di accesso può essere accolta nei limiti che precedono.
Con riguardo, poi, al messaggio di posta elettronica intervenuto tra il Dirigente del ...*Omissis*... e il Prof. ... *Omissis*... di ...*Omissis*... organizzatore dell'evento scientifico ...*Omissis*... (...*Omissis*...), rispetto al quale non è stato osteso il file elettronico o digitale o informatico, ma solo una copia priva dell'indicazione della data, orario o della stringa di altri dati, va rilevato che la P.a. avrebbe dovuto ostendere al ricorrente il file contenente il messaggio di posta elettronica "integrale", cioè recante tutti i dati sopra ricordati, tenuto conto del fatto, peraltro, che si tratta di messaggio inviato da posta elettronica certificata (...*Omissis*...).
Pertanto, in parte *qua*, il ricorso deve essere accolto.
Non risultano, infine, almeno dagli atti di causa e salvo quanto eventualmente potrà emergere nel giudizio pendente avanti all'intestato TAR relativo al provvedimento disciplinare inflitto al ricorrente, elementi sufficienti per ritenere che vi siano altri specifici documenti, rilevanti nell'ambito del ...*Omissis*... di cui sopra, per i quali debba essere disposta l'ostensione.
In ragione del solo parziale accoglimento del ricorso e tenuto conto della presentazione in proprio del ricorso medesimo, in punto spese di lite deve essere posta a carico dell'Amministrazione resistente la rifusione del contributo unificato corrisposto dal ricorrente.
...*Omissis*...

# IL COMMENTO

*di Elio Guarnaccia e Giulia Campo*

**Sommario:** 1. La vicenda affrontata dal T.a.r. Veneto. – 2. Il perimetro dell'accesso documentale *ex* art. 22 l. 241/1990. – 3. Il diritto di accesso ai dati personali trattati dalla P.A. *ex* art. 15 GDPR. – 4. Accesso documentale e accesso ai dati personali: tutele e rimedi giurisdizionali.

La pronuncia in commento affronta una il sempre attuale tema del diritto di accesso nei confronti della P.A. Nello specifico, il T.a.r. Veneto adito si sofferma sulla distinzione tra accesso documentale *ex* art. 22 l.241/1990 e accesso ai dati personali previsto dall'art. 15 GDPR, chiarendo che il limite oggettivo del "documento amministrativo", valevole per l'accesso documentale *ex* art. 22 cit., non deve considerarsi operativo nel caso di accesso ai dati personali ai sensi dell'art. 15 GDPR. La sentenza, altresì, aggiunge che, nel caso in cui l'amministrazione abbia acquisito un documento (nello specifico, una foto) da un file digitale o elettronico, l'interessato può chiedere direttamente accesso *ex* art. 22 cit. a detto file elettronico.

*The ruling in question addresses an important and current issue, that is the right of access, towards Public Administration. Specifically, the Veneto Regional Administrative Court focuses on the distinction between documentary access under Article 22 of Law 241/1990 and access to personal data under Article 15 of the GDPR, clarifying that the objective limit of the "administrative document," valid for documentary access under Article 22 mentioned above, should not be considered operative in the case of access to personal data under Article 15 of the GDPR. Furthermore, the judgment adds that, if the administration has acquired a document (specifically, a photo) from a digital or electronic file, the individual concerned may directly request access under Article 22 mentioned above to the electronic file.*

## 1. La vicenda affrontata dal T.a.r. Veneto

La vicenda oggetto della sentenza in commento, riguarda un dipendente pubblico che, raggiunto da una sanzione disciplinare, ha chiesto alla P.A. datrice di lavoro di avere accesso alla documentazione amministrativa relativa alla contestazione, ai sensi dell'art. 22 della L. n. 241/1990.

Il Collegio ha riconosciuto che l'istanza di accesso fosse correttamente formulata per singoli documenti amministrativi individuati, tranne che per la richiesta riguardante "ogni comunicazione o segnalazione in formato cartaceo, digitale o di posta elettronica istantanea, proveniente da un superiore gerarchico del ricorrente, da un collega del ricorrente, da Autorità o soggetti terzi, da cui lo stesso dirigente abbia tratto elementi fondanti per procedere alla contestazione degli addebiti".

In sostanza, secondo il Collegio, una simile richiesta si sarebbe sostanziata in una istanza finalizzata ad ottenere l'accesso a tutte le informazioni detenute dalla P.A. sul suo conto.

Secondo il T.a.r. Veneto, tale richiesta non si configura come una richiesta di accesso documentale, non avendo ad oggetto documenti ben determinati e di certa esistenza, ma si configura piuttosto come esercizio del diritto di accesso *ex* art. 15 GDPR.

Orbene, a fronte di tale qualificazione, la domanda in questione è stata rigettata non potendo il giudice amministrativo convertire l'istanza *ex* art. 22 L. 241/1990 in istanza di accesso *ex* art. 15 GDPR, e pronunciarsi su di essa.

## 2. Il perimetro dell'accesso documentale *ex* art 22 L. 241/1990

L'istituto dell'accesso documentale, disciplinato dall'art. 22 della legge 7 agosto 1990 nr. 241, è uno strumento giuridico di grande portata, che contribuisce attivamente a delineare le trame del rapporto tra privato cittadino e Pubblica Amministrazione.

L'art. 22 di tale norma, nel sancire il diritto all'accesso ai documenti amministrativi, lo definisce come "il diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi". Già all'interno di tale definizione è possibile scorgere i requisiti che devono sussistere ai fini dell'esercizio di tale potestà; requisiti, che di fatto perimetrano l'area di applicazione della norma.

In primo luogo, il diritto di accesso è subordinato alla presenza di un interesse in capo all'istante. Analizzando il comma 1 lettera b) dell'art. 22 cit. (1), si apprende precisamente che tale interesse può essere proprio di tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, e deve presentarsi, ai fini dell'accesso, come un interesse "diretto, concreto e attuale e corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso".

La sussistenza un interesse già di per sé circostanzia il perimetro dell'accesso documentale, considerato che, in caso di mancanza dello stesso, non è permessa l'ostensione dei documenti amministrativi richiesti. Di tale aspetto, tra l'altro, vi è traccia anche nella sentenza in commento, là dove parzialmente questa rigetta il ricorso nella parte in cui il ricorrente chiede l'accesso di un documento che, secondo la ricostruzione giudiziale, "afferisce ad altra e diversa vicenda non di interesse del ricorrente".

In secondo luogo, a delimitare l'area dell'accesso documentale *ex* art. 22 è pure la nozione di "documento amministrativo", oggetto dell'accesso agli atti, contenuta nella norma e confermata dalla giurisprudenza.

Interpretando la nozione di documento amministrativo di cui al comma 1 lettera d) dell'art. 22 (2), la giurisprudenza amministrativa ha chiarito che il diritto di accesso va esercitato solo su "documenti amministrativi" e dunque non con riferimento ad una attività di elaborazione", discendendo da ciò che l'accesso ha come oggetto soltanto "documenti specifici, già formati ed esistenti, non potendo le istanze di accesso afferire a notizie e/o a informazioni che, per poter essere fornite, presuppongono lo svolgimento di attività di ricerca e di elaborazione da parte dell'Amministrazione" (3).

Anche la stessa sentenza in commento si pone nel solco di questo orientamento giurisprudenziale, ma, nel farlo, il Giudice adito procede pure con un'interessante riflessione in ordine alla natura dei dati trattati e alla "fonte" degli stessi. A livello generale, il Collegio giudicante enuncia che l'accesso non è consentito se le informazioni non hanno la forma del documento amministrativo, ad eccezione di quanto previsto dal decreto legislativo 30 giugno 2003, n. 196 in materia di accesso a dati personali da parte della persona e cui i dati si riferiscono. Da ciò ineluttabilmente si deduce che, se per la natura dei dati si rientra nella disciplina del d.lgs. 196/2003,

(1) Art. 22, comma 1 lettera b): "per "interessati", tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso".

(2) Art. 22, comma 1 lettera d): "per "documento amministrativo", ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale".

(3) T.A.R. Lazio, sez. III, 26 gennaio 2023, n. 1438, in Giustizia Amministrativa, all'indirizzo <http://www.giustizia amministrativa.it>; Cons. Stato, Sez. IV, 14 marzo 2022, nr. 1751, in Giustizia Amministrativa, all'indirizzo <http://www.giustizia amministrativa.it>.

allora si è di fronte a un diritto di accesso, non sussumibile nell'art. 22 della L. 241/1990, e di diversa portata.
Invero, l'oggetto di tale diritto di accesso non deve necessariamente essere un documento amministrativo, per come inteso dalla L. 241/1990 e dalla giurisprudenza.
Successivamente, la sentenza in commento considera ferma e valida l'interpretazione anzidetta, ossia quella per cui l'accesso *ex* art 22 deve necessariamente riguardare atti preformati e nella disponibilità della Pubblica amministrazione (salvo che, appunto, non si tratti di dati personali), però, puntualizza che è comunque pienamente accoglibile la domanda di ostensione *ex* art 22 l. 241/1990 del file "digitale" o informatico o elettronico, dal quale la Pubblica amministrazione ha acquisito la stampa rilasciata all'istante, specie se si è in grado di ricostruire l'ascendenza della stampa a tale file digitale.
Per l'organo giudicante, dunque, il dipendente può in definitiva sempre chiedere il file digitale o informatico o elettronico relativo ad una fotografia che la Pubblica amministrazione -in funzione di datore di lavoro- ha acquisito e sulla base del quale ha avviato il procedimento disciplinare e, per di più, questa tipologia di accesso è pur sempre pienamente sussumibile nel più rigido sistema di accesso costruito dall'art. 22 della l. 241/1990.
Proseguendo con la perimetrazione dell'area dell'accesso documentale, bisogna, per completezza, sottolineare che essa va fatta considerando anche altri istituti relativi all'accesso ai documenti della P.A., quale l'accesso civico (4), disciplinato dal d.lgs. 14 marzo 2013, nr. 33, che non è tuttavia oggetto di esame della sentenza in commento.

### 3. Il diritto di accesso ai dati personali trattati dalla P.A *ex* art. 15 GDPR

La sentenza, oggetto dell'odierna nota di commento, ha svolto valutazioni importanti circa la distinzione tra accesso documentale *ex* art. 22 l. 241/1990 e diritto di accesso ai dati personali *ex* art. 15 Regolamento UE n. 2016/679 ("GDPR").
L'art. 15 GDPR (5), pietra angolare nella protezione della privacy, prevede che "l'interessato" ha il diritto di ottenere dal titolare del trattamento la conferma che dati personali che lo riguardano vengono o meno trattati e, se trattati, di ottenere l'accesso a tali dati e, contestualmente, a determinate informazioni aggiuntive, come, ad esempio le finalità del trattamento, le categorie di dati personali trattati, i destinatari a cui sono stati o saranno comunicati i dati, il periodo di conservazione dei dati o i diritti dell'interessato relativi al trattamento.
La definizione di "dato personale" è contenuta nell'art. 4 comma 1 lettera b) del d.lgs. 30 giugno 2003, nr. 196 (come modificato dal GDPR), secondo cui per dato personale debba intendersi "qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".
Analizzando, poi, l'art. 15 GDPR, quest'ultimo non solo stabilisce il diritto dell'interessato di ottenere una copia dei dati personali oggetto di trattamento, ma sancisce il principio secondo cui l'accesso è sempre gratuito, fatta salva l'ipotesi in cui vi sia la richiesta da parte dell'interessato di ulteriori copie che, comportando necessariamente dei costi maggiori, implichino la previsione di un ragionevole contributo.
Come puntualizzato poi dall'art. 12, paragrafo 3 del GDPR l'interessato ha il diritto di ricevere dal titolare le informazioni richieste, su esercizio del proprio diritto di accesso, il prima possibile e, comunque, al massimo entro un mese. Soltanto in casi particolari, ad esempio

(4) Sul rapporto tra accesso documentale e accesso civico alcuni autori ritengono che con l'accesso civico il principio di trasparenza venga a profilarsi non semplicemente come "need to know", ma come vero e proprio "right to know". Per una prospettiva in tal senso su accesso documentale, accesso civico e principio di trasparenza: Amodio, Il principio di trasparenza e il procedimento amministrativo: dal diritto di accesso documentale al diritto di accesso civico, in *Amministrativ@mente*, 2018, I-II.

(5) Di seguito, il testo integrale dell'art. 15 GDPR: "L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.
3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

quando le richieste siano molto numerose oppure le informazioni da fornire siano particolarmente complesse, il titolare potrà estendere questo termine ad un periodo massimo di due mesi, informando però, sempre entro un mese dalla sua richiesta, l'interessato della necessità di proroga e dei relativi motivi che l'hanno resa necessaria (ad esempio, i tempi tecnici necessari al titolare per reperire le informazioni e per preparare la documentazione).
Se oggetto dell'accesso documentale sono solo i documenti amministrativi e gli atti già formati e detenuti dalla P.A., tale limite, come sottolineato dalla sentenza in commento, non sussiste nella ipotesi in cui vengano trattati dati personali e, dunque, nell'ipotesi di accesso previsto dall'art. 15 GDPR.
Tuttavia, il diritto di accesso *ex* art. 15 GDPR ha uno specifico perimetro applicativo, a fondo indagato dalla Corte di Giustizia dell'Unione Europea (d'ora in poi, per semplificazione, CGUE), che più volte è intervenuta per chiarire i limiti incerti del diritto di accesso delineato dal Regolamento.
Quanto all'oggetto dell'accesso, la CGUE con la sentenza resa nella causa C-487/21, ha chiarito che il titolare del trattamento non può semplicemente fornire una lista dei dati trattati, ma è tenuto a fornire una copia della documentazione contenente tali dati, purché l'accesso a questa documentazione sia necessario per consentire all'interessato di esercitare efficacemente i suoi diritti garantiti dal GDPR. Tutto ciò sulla base del fondamentale assunto, per cui, secondo la Corte, l'articolo 15 del GDPR conferisce all'interessato il diritto di ottenere una riproduzione accurata, fedele, intelligibile e soprattutto comprensibile dei suoi dati personali e una tale riproduzione spesso, per presentarsi come tale, non può limitarsi alla mera condivisione di estratti di documenti, ma a volte deve anche includere la condivisione di documenti completi o estratti di banche dati, a condizione che ciò non violi i diritti e le libertà di altri (6).
Nella sentenza di definizione della causa C-154/21, la CGUE si è pronunciata su una questione pregiudiziale proposta dalla Suprema Corte austriaca, concernente il quesito se l'articolo 15, paragrafo 1, lettera c), del GDPR debba essere interpretato nel senso che "il diritto di accesso dell'interessato ai dati personali (che lo riguardano) implica, qualora tali dati siano stati o saranno comunicati a destinatari, l'obbligo per il titolare del trattamento di fornire all'interessato l'identità concreta di tali destinatari". La risposta della CGUE ha messo in chiaro che la norma va interpretata nel senso per cui l'interessato ha il diritto di conoscere l'identità stessa dei destinatari dei suoi dati, a meno che non sia impossibile identificare detti destinatari o a meno che il suddetto titolare del trattamento non dimostri che le richieste di accesso dell'interessato sono manifestamente infondate o eccessive, ai sensi dell'articolo 12, paragrafo 5, del GDPR, nel qual caso il titolare del trattamento può indicare a detto interessato unicamente le categorie di destinatari di cui trattasi. L'interpretazione si pone, con il suo fare molto estensivo, a forte garanzia del soggetto interessato ai sensi dell'art. 15 GDPR (7).
L'esercizio di tale diritto di accesso nei confronti della P.A. fa si che essa, in qualità di titolare del trattamento, soggiace alla disciplina prevista sia dal GDPR che dall'interpretazione giurisprudenziale e delle autorità garanti. Tale circostanza ha come conseguenza, che ai diritti di accesso documentale e civico normativamente tipizzati, si aggiunge un ulteriore diritto di accesso ai dati personali detenuti, e dunque trattati dalla P.A., a disposizione degli interessati.

## 4. Accesso documentale e accesso ai dati personali: tutele e rimedi giurisdizionali

Una volta operate le necessarie precisazioni sui diritti di accesso in questione, occorre concentrarsi sulla tutela e i rimedi, anche giurisdizionali, previsti nel caso di accesso documentale e di accesso ai dati personali. Come precedentemente emerso, la sentenza del T.a.r. Veneto distingue l'accesso documentale *ex* art. 22 l.241/1990 dall'accesso ai dati personali regolato dal GDPR, ma tale distinzione non solo ha rilievo con riferimento ai presupposti che devono sussistere per il loro esercizio, ma anche presenta un certo valore con riguardo ai rimedi e alle tutele previste.
Prendendo le mosse dall'accesso documentale *ex* art. 22, la tutela offerta è *in primis* di tipo giurisdizionale; l'art. 25 della l. 241/1990, infatti, sancisce che, se l'amministrazione nega l'accesso a un documento o non risponde a una richiesta di accesso, il cittadino interessato può ricorrere al giudice amministrativo, il quale, nell'ipotesi in cui decida in favore dell'accoglimento del ricorso, "ordina" all'amministrazione l'ostensione del documento. Ciò che, senza dubbio, risulta immediatamente di rilievo è il fatto che trattasi di una disciplina processuale "speciale", sia dal punto di vista della tutela offerta che del rito da seguire, prescritto all'art. 116 c.p.a. (8). Difat-

(6) Della Giustina, *L'interessato ha il diritto di dati personali oggetto di trattamento che sia fedele e intelligibile*, in *Cammino diritto*, 2023, V, all'indirizzo <https://rivista.camminodiritto.it/articolo.asp?id=9608>.

(7) Panzà, *Privacy CGUE: le persone hanno il diritto di sapere a chi sono stati comunicati i loro dati*, in *De Iustitia*, 2023, II.

(8) Di seguito, il testo integrale dell'art. 116 c.p.a.:
*Contro le determinazioni e contro il silenzio sulle istanze di accesso ai documenti amministrativi, nonché per la tutela del diritto di accesso civico connessa all'inadempimento degli obblighi di trasparenza il ricorso è proposto entro trenta giorni dalla conoscenza della determinazione impugnata o dalla formazione del silenzio, mediante notificazione all'amministrazione e ad almeno un controinteressato. Si*

ti, con riguardo alla tutela, questa si connota per il fatto che il giudice amministrativo non fornisce col suo giudizio una tutela di tipo costitutivo (vale a dire finalizzata all'annullamento del provvedimento di diniego o, se si è nel caso del 'silenzio', all'ottenimento di un ordine generico di provvedere), ma fornisce una tutela mirata al rilascio di un ordine specifico con cui si impone all'amministrazione di esibire quel determinato documento controverso (9). Il rito speciale all'art. 116 c.p.a., che culmina sempre con una sentenza in forma abbreviata, è applicabile anche nell'ipotesi di c.d. accesso civico.

Accanto alla tutela di tipo giurisdizionale, esiste una forma di tutela alternativa dal carattere non giurisdizionale. L'istituzione del riesame alla Commissione per l'accesso o al Difensore civico, di cui all'art. 25, comma 4 della l. 241/1990, è una scelta fondata su due ragioni particolari, ossia da una parte evitare un aggravio eccessivo di ricorsi giurisdizionali e dall'altro evitare che, per l'eccessivo costo dei ricorsi, si rinunci al diritto di accesso.

Per quanto concerne l'accesso ai dati personali, in caso di diniego dell'accesso o di violazione della privacy, nessuno degli strumenti previsti dal legislatore per l'accesso documentale è esperibile.

Ed invero, gli strumenti a disposizione sono quelli previsti segnatamente dagli artt. 77-79 GDPR e dagli artt. 140-*bis*-143 del d.lgs. 30 giugno 2003, nr. 196 (c.d. Codice della privacy), i quali non prevedono la possibilità di ricorrere al giudice amministrativo.

Nello specifico, infatti, l'art. 140-*bis* del Codice della privacy prevede che l'interessato, qualora ritenga che i diritti di cui gode sulla base della normativa in materia di protezione dei dati personali siano stati violati (anche in caso di violazione del diritto di accesso ai dati personali), può presentare un reclamo all'autorità di controllo (10) oppure ricorrere dinnanzi all'Autorità giudiziaria ordinaria. Come poi anche lo stesso art. 140-*bis*, comma 3 conferma, il reclamo al Garante è previsto in alternativa rispetto alla tutela giudiziaria, per cui, dopo essersi rivolti al Garante, non è più ammissibile adire il giudice ordinario.

Sotto un profilo marcatamente procedurale, il reclamo può essere sottoscritto direttamente dall'interessato oppure, per suo conto, da un avvocato, un procuratore, un organismo, un'organizzazione o un'associazione senza scopo di lucro e, in tali casi, è necessario conferire una procura da depositarsi presso il Garante assieme a tutta la documentazione utile ai fini della valutazione del reclamo presentato. Sebbene la via del reclamo sia alternativa rispetto alla tutela di fronte all'Autorità giudiziaria, si precisa all'art. 143 Codice della privacy che, in ogni caso, avverso il provvedimento che decide sul reclamo è proponibile ricorso giurisdizionale al tribunale competente nel termine di 30 giorni dalla comunicazione del provvedimento.

Insieme alla possibilità di reclamo, nell'asserita ipotesi di violazione della disciplina in materia di privacy, è previsto pure un altro rimedio in favore dell'interessato, che è quello della segnalazione al Garante *ex* art. 144 Codice della privacy. L'istituto della segnalazione si propone solo e soltanto nei confronti del Garante ed è precipuamente mirato a sollecitare il Garante all'esercizio dei suoi poteri, previsti all'art. 58 GDPR.

Difatti, lo stesso art. 144 cit. sottolinea che la segnalazione è finalizzata proprio a ottenere i provvedimenti previsti dall'art. 58 GDPR, manifestazione di un ampio potere accordato all'Autorità Garante, che può assumere la variante di potere di controllo, di indagine, di correzione o ancora di autorizzazione e consultazione verso i titolari del trattamento.

*applica l'articolo 49. Il termine per la proposizione di ricorsi incidentali o motivi aggiunti è di trenta giorni.*

*2. In pendenza di un giudizio cui la richiesta di accesso è connessa, il ricorso di cui al comma 1 può essere proposto con istanza depositata presso la segreteria della sezione cui è assegnato il ricorso principale, previa notificazione all'amministrazione e agli eventuali controinteressati. L'istanza è decisa con ordinanza separatamente dal giudizio principale, ovvero con la sentenza che definisce il giudizio.*

*3. L'amministrazione può essere rappresentata e difesa da un proprio dipendente a ciò autorizzato.*

*4. Il giudice decide con sentenza in forma semplificata; sussistendone i presupposti, ordina l'esibizione e, ove previsto, la pubblicazione dei documenti richiesti, entro un termine non superiore, di norma, a trenta giorni, dettando, ove occorra, le relative modalità.*

*5. Le disposizioni di cui al presente articolo si applicano anche ai giudizi di impugnazione.*

(9) Parisio, *La tutela dei diritti di accesso ai documenti amministrativi e alle informazioni nella prospettiva giurisdizionale*, in <Federalismi.it>, 2018, XI, all'indirizzo <https://www.federalismi.it/nv14/articolo-documento.cfm?artid=36352>.

(10) Per una disamina completa dei poteri del Garante: Califano, *Il ruolo di vigilanza del Garante per la protezione dei dati personali*, in <Federalismi.it>, 2020, III, all'indirizzo <https://www.federalismi.it/nv14/articolo-documento.cfm?artid=36352>.

# Blockchain e NFT: la funzione notarile al tempo dell'ultima transizione

**di Massimo Palazzo**



La circolazione della ricchezza si avvale oggi di nuove tecnologie come Blockchain ed NFT. Il giurista è chiamato a comprendere se e come le categorie tradizionali in tema di contratto e di proprietà siano in grado di disciplinare la nuova realtà. Confrontarsi con questi nuovi fenomeni è complesso, poiché siamo al cospetto di tre tempi di evoluzione: quella tecnologica, rapidissima; quella legislativa; quella delle prassi applicative.
Parrebbe necessario lavorare affinché i processi in atto, destinati a regolare segmenti crescenti della vita sociale, siano sottoposti a una logica di controllo democratico, che assicuri un adeguato bilanciamento tra la 'funzionalità tecnologica' e la desiderabilità sociale degli scopi perseguiti, e rispetto al quale la mediazione giuridica svolge un ruolo centrale. In tale prospettiva il ruolo del notaio, quale fattore di realizzazione dell'ordine sociale in attuazione dei principi costituzionali, lungi dall'essere superato appare ancora attuale.

*Circulation of wealth today makes use of new technologies such as Blockchain and NFT. Jurist is called to understand if and how the traditional categories in terms of contract and property are able to regulate the new reality. Confronting these new phenomena is complex, since we are faced with three times of evolution: the technological one, which is very rapid; the legislative one; that of application practices. It would seem necessary to work so that the processes in progress, intended to regulate growing segments of social life, are subjected to a logic of democratic control, which ensures an adequate balance between the 'technological functionality' and the social desirability of the objectives pursued, and with respect to which legal mediation plays a central role. From this perspective, the role of the notary, as a factor in the creation of social order in implementation of constitutional principles, far from being overcome, still appears important.*

## 1. *Blockchain Smart contracts ed NFT*: un capitolo del processo di globalizzazione giuridica

La storia del diritto non può separarsi dalla storia delle tecnologie (1). Con specifico riguardo all'interazione tra informatica e diritto, gli sviluppi della tecnologia consentono oggi l'affidamento ad operazioni automatizzate sempre più sofisticate di attività giuridicamente rilevanti, di intere fasi non solo della conclusione di un contratto (es. acquisto un libro su una piattaforma informatica) ma pure della sua esecuzione ed ormai anche della risoluzione delle relative controversie (attraverso piattaforme informatiche *on line*); ed ha generato persino mezzi alternativi al danaro (criptovalute) (2) di grande diffusione e con enormi potenzialità, talora elusive di regole a tutela di interessi pubblicistici, nonché chiavi digitali (NFT) che consentono al detentore di essere identificato univocamente come l'avente diritto all'accesso alla fruizione del contenuto digitale, nei limiti contrattualmente previsti.
Le nuove tecnologie hanno dunque trasformato non soltanto i mezzi di conoscenza del diritto, ma, più in profondità, la sua formazione (3). La circolazione della

(1) Irti, *Norma e luoghi. Problemi di geo-diritto*, Roma-Bari, 2006, 187. Il saggio di Natalino Irti al quale nel titolo di questo contributo si fa riferimento è *L'ultima transizione*, in *Riv. dir. civ.*, 2022, I, 205 ss.

(2) Criptovaluta letteralmente significa "valuta nascosta". Il primo elemento deriva dal greco *Kriptos,* che in questo contesto dovrebbe intendersi non tanto come "nascosto", quanto come "crittografato": si tratta, infatti, di un'entità che può essere individuata e utilizzata solo attraverso un codice informatico, composto dalle chiavi di accesso pubblica e privata.

(3) Come ha recentemente notato il filosofo del diritto, Zaccaria, *Figure del giudicare: calcolabilità, precedenti, decisione robotica*, in *Riv. dir. civ.*, 2020, 289.

ricchezza si avvale oggi delle nuove tecnologie ed il giurista è dunque chiamato a comprendere se e come le regole tradizionali in tema di contratto e di proprietà siano in grado di disciplinare la nuova realtà.
L'evoluzione tecnologica ha generato, grazie alla rete telematica, uno spazio fuori da ogni territorio e da ogni storia: un non luogo astratto ed artificiale, dove si svolgono gli affari dell'economia planetaria. In questo spazio la regola tecnica, imposta da chi dispone della tecnologia e della forza contrattuale, tende a diventare regola giuridica.
Il potere di imporre una regola tecnica si è ben presto tradotto in vero e proprio potere regolatorio, ossia nel potere di imporre una regola con efficacia giuridica tanto sul piano dell'autonomia privata, quanto su quello dell'azione pubblica. Non solo: l'affermarsi della regola tecnica ha reso sempre più labile e sfuggente la distinzione tra dimensione di mercato e dimensione pubblica, a tutto favore della prima (4).
In questo senso la vicenda concettuale degli NFT costituisce uno dei tanti capitoli della storia della globalizzazione giuridica, intesa come processo lungo il quale il diritto assume nuovi tratti e nuove funzioni. Occorre, infatti, sin d'ora sottolineare che attualmente un ruolo centrale nella realizzazione tecnica e nella commercializzazione degli NFT è concentrata nelle mani delle piattaforme che sono in grado di dettare le regole, innanzitutto tecniche, ma anche economiche e contrattuali che governano i rapporti tra il titolare/creatore del contenuto (digitale o digitalizzato) e l'utente/consumatore.
La rivoluzione digitale, inoltre, ha fatto esplodere la scrittura, con una proliferazione di documenti informatici che si moltiplicano non solo perché è facile riprodurli, ma ancor più perché vengono generati automaticamente, al punto che è diventato difficile determinare cosa conta e cosa ha valore giuridico come documento. Dopo la post-verità dobbiamo affrontare come comunità tecnica e sociale la post-documentalità (5).
Siamo quindi, probabilmente, dinanzi a quello che l'epistemologo americano T. S. Khun definiva cambio o più esattamente "slittamento di paradigma": di fronte a problemi nuovi siamo spinti a cambiare il nostro punto di vista sulla realtà, fino all'adozione di un nuovo "paradigma interpretativo".
Lo studio dei profili regolativi delle blockchains e degli NFT impone riflessioni critiche sui processi informatici e sul concreto funzionamento delle infrastrutture tecnologiche utilizzate per la creazione, la conservazione e lo scambio di NFT.
Per un approccio consapevole con il fenomeno degli NFT, in tutte le loro implicazioni socio-economiche e giuridiche, non parrebbe sufficiente avere conoscenze limitate al campo giuridico, o al campo finanziario o al campo informatico, ma è necessaria una visione d'insieme, anche se non specialistica in tutti i campi, per comprendere limiti, rischi e potenzialità offerti dalle nuove tecnologie digitali e per poter bilanciare, in modo ragionevole, i diversi interessi coinvolti imputando, di volta in volta, all'uno o all'altro contraente i relativi rischi e responsabilità.
In breve, l'evoluzione degli scambi commerciali e finanziari preconizza un nuovo processo storico che, da una parte, appare di difficile armonizzazione e compatibilità con le categorie giuridiche tradizionali e, dall'altra, per via della difficoltà di circoscrivere le ricadute del fenomeno entro i confini territoriali di un determinato ordinamento, non consente di individuare univocamente le istituzioni che dovrebbero regolamentare la nuova realtà (6). Il giurista deve accedere ad un nuovo lessico e spesso le nostre competenze non sono sufficienti. Ma occorre fare uno sforzo di dialogo con le nuove dimensioni, pena la marginalizzazione del nostro sapere.

## 2. Assenza di un quadro regolatorio interno e disciplina eurounitaria

Nel contesto di continua evoluzione dei servizi digitali, ha attirato l'attenzione della stampa e degli investitori – anche in relazione alle rilevanti quotazioni raggiunte da alcuni *asset* digitali – e quindi dei giuristi, la creazione e la crescente valorizzazione di un prodotto digitale denominato *non-fungible token* (NFT). Si tratta di uno strumento che può essere utilizzato in una pluralità di settori professionali e dell'intrattenimento per consentire la fruizione di contenuti sportivi, artistici, musicali, di *gaming* ma anche connessi a beni di lusso e immobiliari. Stanno, infatti, proliferando lo studio di progetti e casi d'uso alla ricerca di nuove modalità di soddisfare bisogni attuali e prospettici.
Particolare interesse hanno suscitato alcune proprietà tecnologiche caratteristiche degli NFT che, mediante una funzionalità inserita nel programma del relativo

(4) Per maggiori riferimenti mi permetto di rinviare a Palazzo, *Il contratto nella pluralità degli ordinamenti*, Napoli, 2021, 35 e ss. e 299 e ss.

(5) Dopo che nella fase più recente sembrava che fosse destinata a prevalere la cultura orale (radio, televisione, i primi telefonini, via via sempre più piccoli, poiché destinati solo allo scambio vocale), la tecnologia ci ha sorpreso, rivelando una realtà sociale inattesa. Dopo il massimo declino della cultura scritta, essa ha ripreso vigore e si è vigorosamente affermata con un proliferare di documenti scritti ed anzi registrati sulla memoria dei nostri computer e su quella delle grandi piattaforme tecnologiche sulle quali ci appoggiamo. Il filosofo torinese Maurizio Ferraris parla di *rivoluzione documediale*, sulle orme di Jaques Derrida. Cfr. Ferraris, *Il capitale documediale. Prolegomeni*, in *Scienza nuova. Ontologia della trasformazione digitale*, Torino, 2018.

(6) Condividono tale prospettiva De mari - Gasparri - Poli, *DLT e cripto-attività* in *Tokenizzazione di azioni e azioni tokens, Quaderni giuridici Consob*, a cura di Carriere et al., 25 gennaio 2023, 13.

*smart contract*, consentono di monetizzare il prodotto digitale ad ogni successivo passaggio di proprietà del bene, quindi rispondendo ad esigenze connesse all'esercizio di diritti riconosciuti *ex lege* all'autore e finora di difficile attuazione. Non esiste, tuttavia, nel vigente ordinamento italiano un quadro normativo e regolamentare che identifichi e disciplini compiutamente questo prodotto. Diversamente, in altri ordinamenti come ad esempio la Svizzera (ma analogamente hanno fatto Malta, Panama, Liechtenstain), si è previsto una differenziazione dei *token* in tre macrocategorie (*token* di pagamento/criptovalute, *token* di utilizzo, *token* d'investimento) con l'applicazione di differenti plessi normativi in base alle caratteristiche di ciascuna categoria (7).

Nel contesto europeo l'obiettivo sembrerebbe quello di regolare, in una ottica neutrale rispetto alla tecnologia ed ai prodotti, la correttezza dell'interazione tra i tre principali attori che – ad oggi – caratterizzano la creazione e l'utilizzo degli NFT: i fornitori/titolari dei contenuti, le piattaforme e gli utenti/consumatori. Il 9 giugno 2023 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il Regolamento MiCA disciplinante le cripto-attività, che troverà applicazione dal 30 giugno 2024 per gli emittenti e dal 30 dicembre 2024 per i prestatori di servizi (8).

Un riferimento alla regolamentazione applicabile agli NFT si può reperire nel suddetto Regolamento che modifica la direttiva (UE) 2019/1937 (MiCA) nell'ambito del c.d. *Digital Finance Package*, un pacchetto di misure volte a consentire e sostenere l'ulteriore sfruttamento delle potenzialità della finanza digitale in termini di innovazione e concorrenza, fornendo «*ai consumatori più scelta e opportunità in relazione ai servizi finanziari e di pagamento, garantendo al contempo la protezione degli stessi e la stabilità finanziaria*» (9). Nella strategia della Commissione l'adozione del Regolamento MICA intende stimolare l'innovazione preservando la stabilità finanziaria e, nel contempo, proteggendo gli investitori dai rischi. La definizione della regolamentazione della cripto-attività tramite lo strumento del Regolamento è volta dunque a fornire omogeneità di disciplina e tempestività di adozione delle misure, garantendo perciò maggiore chiarezza sul contesto giuridico di riferimento e più certezze per gli emittenti, gli intermediari di crypto-valute (c.d. *exchange*) e tutti gli attori che operano nella filiera del settore (10).

Approfondendo la possibilità che la disciplina dettata da MiCAR possa introdurre una regolamentazione per l'emissione e la gestione di NFT, la definizione di cripto-attività adottata dall'art. 3, co. 1, n. 2, cioè di «*rappresentazione digitale di valore o diritti che possono essere trasferiti e conservati elettronicamente, utilizzando la tecnologia* distributed ledger *o una tecnologia simile*» parrebbe includere anche gli NFT e quindi la disciplina dettata dal Regolamento, *rebus sic stantibus*, potrebbe essere applicata anche ai prodotti digitali in esame.

Tuttavia, il testo del Regolamento MiCA non fornisce una posizione ben definita in merito ai *Non Fungible Tokens*. *Per avere maggiore chiarezza rispetto alla regolamentazione di questi prodotti digitali sarà necessario attendere successive Direttive Comunitarie, linee guida e Standard Tecnici di Regolamentazione (RTS) prodotti dalla Commissione Europea e dagli altri enti di competenza, come l'EBA e l'ESMA* (11).

Nel percorso legislativo europeo gli obblighi per i soggetti che offrono al pubblico un NFT, che attualmente si possono desumere dal Regolamento, dovrebbero essere

(7) Sul punto v. Varrasi, *Token e Blockchain: spunti ed evoluzioni normative in altri sistemi giuridici*, in *La trasformazione digitale dell'attività notarile*, a cura di Morone, Milano, 2022, 195 ss.; Abriani, *Rappresentazione e circolazione di partecipazioni di società di capitali mediante la tecnologia DLT*, in *ODCC*, 2022, 359 ss.

(8) Con la pubblicazione nella G.U. dell'Unione Europea, il Regolamento MiCA costituisce il primo esempio di quadro regolamentare armonizzato di disciplina del mercato cripto. Frutto di quasi tre anni di negoziati in seno alle istituzioni europee, rappresenta un complesso articolato che disciplina da un lato gli emittenti di cripto-attività e dall'altro i prestatori di servizi, prevedendo numerosi obblighi di comportamento e organizzazione interna per la salvaguardia del mercato europeo. Gli adempimenti richiesti necessiteranno di diversi mesi per essere implementati, e dunque il Regolamento prevede 12 mesi per l'adeguamento degli emittenti e 18 mesi per quello dei prestatori di servizi. In questo periodo, la Commissione Europea e l'ESMA, l'autorità europea di vigilanza sui mercati, saranno chiamate ad emanare normative di livello secondario per disciplinare alcuni aspetti della nuova regolamentazione.

(9) Comunicato stampa della Commissione. Il Parlamento europeo ha approvato la proposta di regolamento il 20 aprile 2023. Sul MiCAR, v. Di Stefano - Guerreschi, *Il nuovo regolamento europeo sui crypto assets*, in questa ***Rivista***, 1 giugno 2023.

(10) Mattasoglio, *Le proposte europee in tema di cryptoassets e DLT. Prime prove di regolazione del mondo crypto o tentativo di tokenizzazione del mercato finanziario (ignorando* bitcoin*)?*, in *Riv. dir. bancario*, 2021, 413.

(11) Al fine di garantire un approccio proporzionato in termini di obblighi regolamentari, all'art. 4, comma 2 MiCAR si prevede che i vincoli di redazione, notifica e pubblicazione di un *White Paper* previsti all'art. 4, comma 1 tra le diverse attività escluse, non dovrebbero essere imposti anche alle emittenti di "*cripto-attività che sono uniche e non fungibili con altre cripto-attività*". La definizione adottata per questo segmento di cripto-attività ragionevolmente include anche gli NFT. La *ratio* di questa esenzione dai complessi obblighi di redazione, notifica, pubblicazione e modifica del *white paper* previsti agli artt. 5, 7, 8 e 11 MiCAR risulta fondata sulla constatazione che un'offerta pubblica di un NFT risulterebbe necessariamente realizzata in una sola transazione, risultando dunque sproporzionato richiedere all'emittente di adottare tutti gli obblighi che il MiCAR impone per la redazione e la pubblicizzazione di un *white paper* (sul punto, cfr. il Considerando 15 del MiCA). Resterebbero comunque fermi, anche per i soggetti che offrono al pubblico un NFT, i restanti obblighi previsti dal MiCA, ossia che l'emissione deve essere comunque effettuata da una persona giuridica che deve rispettare principi di onestà, correttezza e professionalità nelle proprie attività e di correttezza e trasparenza nelle proprie comunicazioni (cfr. artt. 4 e 13 MiCA).

ulteriormente circoscritti con riferimento alla specifica funzione d'uso di questo *token*. Probabilmente il parallelo e tumultuoso percorso di evoluzione dei servizi NFT potrà aiutare a qualificare correttamente i profili regolamentari che si potrebbero introdurre in via legislativa.
Il Consiglio dell'Unione Europea, nella posizione espressa il 24 novembre 2021 relativa al mandato per le negoziazioni con il Parlamento, ha ritenuto che la proposta di Regolamento MiCA non dovrebbe applicarsi alle crypto-attività che siano uniche e non fungibili (come l'arte digitale e gli oggetti da collezione) il cui valore è attribuibile alle caratteristiche di unicità e l'utilità è a beneficio del titolare del *token*, così come alle crypto-attività che rappresentano servizi o beni fisici che siano unici e non fungibili (come le garanzie di prodotto e i beni immobiliari). La ragione della esclusione degli NFT dal perimetro di applicazione del Regolamento MiCA è fondata sul presupposto che la caratteristica di unicità e quindi l'assenza di un mercato di beni fungibili limiti l'utilizzo di questa tipologia di *token* per finalità finanziarie e, conseguentemente, i rischi per gli utenti (12).
Il testo del Regolamento, approvato dal Parlamento europeo nel mese di aprile 2023, vista l'ampiezza della definizione di cripto-attività sembra ricomprendere nel perimetro applicativo della disciplina, sia gli Asset referenced token, sia i token di moneta elettronica, sia gli utility token. L'articolo 3 del regolamento MiCA offre una serie di definizioni importanti, tra cui quella di "cripto-attività", di "tecnologia di registro distribuito (DLT)", di "emittente di cripto-attività", di "token collegati ad attività", "token di moneta elettronica", "fornitore di servizi per le cripto-attività", "*utility token*" e altre.
Il regolamento fornisce poi una – seppur macro – distinzione tra tre sottocategorie di cripto-attività che dovrebbero essere soggette a requisiti più specifici e cioè:

- gli e-money tokens (EMT), un tipo di cripto-asset, simile alla moneta elettronica, che mira a mantenere un valore stabile facendo riferimento al valore di una valuta ufficiale;
- gli asset-referenced Token (ART), un tipo di cripto-asset che non è un token di moneta elettronica e che mira a mantenere un valore stabile facendo riferimento a qualsiasi altro valore o diritto o una combinazione di questi, incluse una o più valute ufficiali;
- gli utility Token, definiti come un tipo di cripto-asset che ha il solo scopo di fornire l'accesso a un bene o un servizio fornito dall'emittente di quel token.

Invece, sono rimasti esclusi, dopo moltissimi ripensamenti, i *non-fungible tokens* (NFT) a condizione però che siano effettivamente e sostanzialmente rappresentativi di *asset* non fungibili. In altri termini, non è sufficiente che un NFT sia nominalmente e tecnicamente disegnato come non fungibile per "sfuggire" alla regolamentazione, ma è necessario che il bene (digitale o fisico) cui fa riferimento sia altrettanto infungibile.
La Francia ha adottato un regime specifico – le ICO (Initial Coin Offering) – a partire dal 2018, mentre la Germania e gli Stati Uniti hanno preferito ricondurre le criptovalute entro la già nota nozione civilistica di bene. Diversamente, il Regno Unito ha preferito identificarle come attività finanziarie. In Italia, invece, la recente Legge di Bilancio 2023 ha introdotto per la prima volta una disciplina in materia di cripto-attività sia per il loro trattamento fiscale sia per la loro regolarizzazione, scegliendo di seguire il legislatore europeo e quindi mutuando l'ampia definizione fornita dal regolamento MiCA. Il quadro è quindi fortemente frammentato e sicuramente di difficile armonizzazione.
Se da un lato quindi la definizione europea così ampia può in un certo senso ricomprendere le varie situazioni normative dei singoli paesi, dall'altro una equiparazione di cripto-asset differenti tra loro potrebbe portare a problematiche sotto il profilo della loro tassazione. Come si intuisce dal quadro normativo europeo, sotto il profilo giuridico – e quindi di conseguenza fiscale – non è stata ancora trovata una classificazione che metta tutti d'accordo a livello globale. D'altro canto, anche in Italia il dibattito è vivace.
Nel tentativo di estendere alle criptovalute qualificazioni giuridiche già esistenti, così come succede in Germania, è stata avanzata la tesi (forse preferibile) secondo cui le criptovalute sono qualificabili dal punto di vista giuridico come "beni", ai sensi dell'art. 810 c.c. secondo cui "Sono beni le cose che possono formare oggetto di diritti". La stessa giurisprudenza (13) ha ipotizzato que-

(12) Come riportato nel testo, il 30 maggio 2022, è entrato in vigore il Regolamento UE 2022/858 in materia di i*nfrastrutture di mercato basate sulla tecnologia a registro distribuito*. Il Regolamento modifica i regolamenti 600/2014 e 909/2014, nonché la direttiva 2014/65/UE (testo rilevante ai fini dello Spazio Economico Europeo). Lo scopo del regolamento quello di disciplinare un campo sempre pi diffuso nei Paesi dell'Unione e soprattutto di garantire le irrinunciabili tutele a investitori e mercati, perseguendo la stabilità finanziaria L'elenco dei titoli che possono essere tokenizzati, non previsto nel regolamento ma demandato alle normative nazionali. Il decreto legge 25/2023, convertito con legge 10 maggio 2023, n. 52, (sul quale v. *infra* par. 12) indica i seguenti asset come tokenizzabili: Azioni, Obbligazioni,Titoli di debito emessi da società con responsabilità limitata, Altri titoli di debito previsti dall'ordinamento italiano, Ricevute di deposito su obbligazioni e altri titoli di debito, Strumenti del mercato monetario regolamentati dalle normative italiane, Azioni o quote di OICR italiani.

(13) Trib. Firenze. 21 gennaio 2019 n. 18 in *Le Corti fiorentine*, 2, 2019, 71 ss., ha affrontato la questione relativa all'individuazione della natura giuridica della criptovaluta, riconducendole nell'ambito del paradigma proprietario quali "beni" fungibili ai sensi dell'art. 810 c.c. Si pensi ad

sto inquadramento giuridico, sostenendo appunto che le criptovalute sono oggetto di diritti e mezzo di scambio in un sistema pattizio e non regolamentato in cui i soggetti che vi partecipano accettano volontariamente tale funzione con tutti i rischi che ne derivano.
A tutt'oggi, nonostante il diffondersi di iniziative imprenditoriali e commerciali (*rectius,* di annunci di iniziative), una individuazione delle caratteristiche giuridicamente rilevanti di un prodotto NFT rimane pressoché sconosciuta per la maggior parte degli operatori del mercato. Tra gli attori economici di questo mercato i dubbi relativi a come applicare i plessi normativi vigenti sono superiori alle certezze o, comunque, i vincoli regolamentari sono spesso sottostimati nel processo di creazione del prodotto digitale.

## 3. La tecnologia utilizzata per gli NFT

Come emerge da queste prime notazioni, **r**iflettere sui non-fungible token è particolarmente stimolante benché, all'evidenza, complesso. Infatti, nonostante si assista ad una certa diffusione del formante dottrinale (14), manca il formante giurisprudenziale (15); nel mentre il formante legale è, da un canto, scarso e, dall'altro, in via di progressivo (lento) assestamento, con rare progressioni e lunghe soste. E la ragione sembra del tutto intuitiva: l'innovazione della tecnica, e segnatamente della tecnologia digitale, produce "opportunità", oggi, ad un ritmo inaccessibile alla produzione di regole giuridiche appropriate – quindi: appositamente dettate allo scopo – a governare le "criticità" che quell'innovazione porta con sé; criticità da ricondurre alla ricerca di soluzioni di conflitti di interessi degli attori in gioco (soluzioni, ovviamente, plausibili ed integrabili nel sistema: non solo giuridico ma, prima ancora, economico, soprattutto in punto di costi per le imprese e, più in generale, per gli operatori).
In tale prospettiva, ci si deve interrogare sul significato giuridico, degli NFT: cosa sono giuridicamente, gli NFT. Il che richiede l'individuazione di una fattispecie che possa fungere da "modello" al quale ragguagliare il "caso concreto" per poi applicare la conseguente disciplina.

Ebbene, nel farlo, parrebbe utile ricordare che l'individuazione della fattispecie (16) è sempre "relativa": dipende, cioè (ed anche), dalla disciplina che si deve applicare e, dunque, in definitiva dipende dagli interessi coinvolti nel caso concreto e che si intende "governare". Ne segue che occorre vigilare nel proporre e selezionare una "sola" e monolitica fattispecie di NFT dovendosi valutare di volta in volta quale disciplina si intende applicare.
Nella ricerca della "fattispecie" degli NFT ci si avvede che manca una definizione "legale", racchiusa in un testo che possa produrre "effetti" verso terzi, che sia, insomma, opponibile a tutti: in altri termini – e sul punto si tornerà – gli NFT sono al momento un "fenomeno tecnico e socio-economico" (17) auto-regolato, frutto di autonomia privata (chi detta la regola ne è il destinatario degli effetti) e non di eteronomia (dove non c'è coincidenza tra chi pone la regola ed i destinatari dei suoi effetti).
Al fine di un'adeguata comprensione dei presupposti della realizzazione di un NFT sembra allora necessario tratteggiare in estrema sintesi quali funzioni svolga una *blockchain* (*rectius,* una *Distributed Ledger Technology* - DLT), cosa sia un *token*, quando abbia una natura *non-fungible*, quali siano le caratteristiche tecnologiche di un NFT e, quindi, quale sia il bene giuridicamente rilevante che le parti si scambiano (18). Sulla base di questi elementi si potranno individuare nei successivi paragrafi i soggetti che svolgono un ruolo nella emissione di un NFT, quali siano i principali casi d'uso correlati all'utilizzo di un NFT e, infine, quale possa essere l'interesse alla base della realizzazione delle più diffuse tipologie di NFT.

## 4. *Blockchain e DLT:* le infrastrutture tecnologiche per la creazione e lo scambio di NFT

Gli NFT vengono realizzati grazie alla registrazione su una piattaforma caratterizzata dalla tecnologia

esempio ai bitcoin, i quali possono essere sostituiti indifferentemente con altri, in quanto irrilevante, generalmente, avere bitcoin di quell'account (utente) o di un altro.

(14) Per tutti si v. Onza, *Non-fungible token e diritto d'autore: (ipotesi di) ricostruzioni e (di) interferenze,* in *Il diritto industriale*, 2023, 103, con ampi e aggiornati riferimenti bibliografici.

(15) Qualche spunto in Trib. Roma sez. specializzata imprese 20 luglio 2022, ord., in *Foro it.* 2022, 3810. Su questa ordinanza cautelare v. Di Stefano - Acquafondata, *NFT: il Tribunale di Roma compie un passo in avanti nella regolamentazione del mondo digitale*, in questa ***Rivista***, 9 gennaio 2023.

(16) Il tema si innesta nel dibattito sulla utilità, per il giurista contemporaneo (ed in particolare per i giudici), della logica della "fattispecie". Per il suo superamento, accedendo ad una logica per "valori", si può limitare il rinvio ai saggi di Grossi e Lipari (v., tra i vari e nell'ordine, *Ritorno al diritto*, Roma-Bari, 2015; *Elogio della giustizia*, Bologna, 2021; cfr. anche Irti, *Un diritto incalcolabile*, Torino, 2016; e Gentili, *Crisi delle categorie e crisi degli interpreti*, in *Riv. dir. civ.*, 2021, I, 633 ss.). Potrebbe forse evidenziarsi che l'uscita dalla logica della "fattispecie" e l'ingresso della logica per "valori" suppone un supplemento di motivazione della decisione giudiziale: ma questo contrasta con il formante legale che tende, piuttosto, a "sintetizzare".

(17) Onza, *op. cit.*, 104.

(18) Può essere interessante evidenziare che questo prodotto digitale ha subìto una ulteriore evoluzione per motivazioni commerciali. Sono stati realizzati dei progetti, soprattutto nel settore dell'arte, che prevedono il frazionamento dei diritti sottesi ad un NFT, che viene quindi denominato *Fractional Non-Fungible Token* o F-NFT.

*blockchain,* che è una sotto-famiglia di piattaforme tecnologiche incluse in un rapporto di genere a specie nella più ampia categoria delle *Distributed Ledger Technology* (DLT).
Una *blockchain* è un elenco crescente di *record*, chiamati per l'appunto blocchi, i quali sono collegati tramite crittografia. Ogni blocco contiene un *hash* crittografico del blocco precedente, un *timestamp* e dati di transazione (generalmente rappresentabili per mezzo di un *Merkle root*).
La *blockchain* consente la creazione di database distribuiti, basati sulla tecnologia dei c.d *Distributed Ledger* (DLT – dove *ledger* sta per libro mastro) strutturati in blocchi di informazioni, ciascuno dei quali contiene un certo numero di transazioni che, a seguito di un articolato procedimento di validazione e controllo (che verifica ad esempio che il soggetto sia effettivamente titolare di un certo diritto, come la valuta o il bene che vuole vendere), vengono validate in tutti i loro elementi attraverso strumenti matematici complessi (funzioni di *hash*) da parte dei nodi della rete ed entrano conseguentemente a far parte della catena di blocchi (*blockchain*) che rende queste transazioni certe, immodificabili. Si viene così a creare uno "storico" nel tempo di tutte le modifiche avvenute (19).
La *blockchain* è quindi esemplificativamente rappresentabile come una lista, in continua crescita, di blocchi collegati tra loro e resi sicuri mediante l'uso della crittografia, a ciascun blocco può essere associata una o più richieste e ogni blocco contiene un puntatore *hash* al blocco precedente e una marca temporale.
La *blockchain* ha rappresentato una risposta alle varie criticità che riguardavano la circolazione delle valute virtuali. Essa può definirsi allo stesso tempo un "*network*", dove operano più utenti tra loro legati in modo orizzontale e senza vincoli gerarchici, uno strumento per la generazione e la circolazione di valute virtuali (ma anche di altri dati) ed un "database", dove vengono raccolti e registrati i dati e le informazioni relative alle transazioni (o ad altre operazioni).
Occorre, tuttavia, evidenziare che la struttura delle architetture *blockchain* può prevedere un diverso grado di decentralizzazione e quindi, di riflesso, un maggiore o minore livello di autogoverno. Accanto ai sistemi completamente aperti (c.d. *permissionless*), come *bitcoin* ed *ethereum*, all'interno dei quali chiunque può prendere parte al *network* e contribuire al processo di validazione delle transazioni da iscrivere nel registro, ne esistono altri definiti *permissioned*, di solito realizzati da operatori economici per scopi commerciali, nei quali la possibilità di accedere al servizio e/o di verificare le operazioni da inserire nella *blockchain* è riservata a utenti selezionati (previamente identificati), sulla base di criteri discrezionali definiti dal loro amministratore o titolare.
In maniera assai condivisibile il documento *Proposte per la Strategia italiana in materia di tecnologie basate su registri condivisi e Blockchain* messo in consultazione pubblica dal 18 giugno al 20 luglio 2020 dal MISE (20) prende atto, forse per la prima volta, che la tecnologia *blockchain* va utilizzata *tenendo conto del contesto in cui opera e dell'ordinamento giuridico di riferimento*, dato che la strategia giuridica è essenziale per tutelare gli interessi delle persone e della stessa pubblica amministrazione.
Non è questa la sede per esaminare gli aspetti tecnici della Blockchain. Giova, tuttavia, rammentare che la Blockchain pura (o aperta) non prevede barriere di accesso e i beneficiari finali delle posizioni giuridiche detengono direttamente le chiavi crittografiche che consentono di disporre di tali posizioni giuridiche, che possono essere auto-rappresentative (come il bitcoin) oppure rappresentare oggetti fisici, che hanno una propria realtà al di fuori della rappresentazione crittografica, che degrada a mero *token* e può circolare sulla Blockchain allo stesso modo dei Bitcoin. Emergono dunque varie criticità.
In primo luogo le posizioni giuridiche, per le quali il *token* rappresenta la chiave di accesso, dovrebbero essere garantite come effettivamente corrispondenti alla loro rappresentazione digitale. *Nulla quaestio* per beni auto-rappresentativi e immodificabili come bitocoin. Non sembra invece possibile utilizzare una Blockchain pura in ambito immobiliare, per la dirimente ragione che terreni e fabbricati cambiano nel tempo. In assenza di un'autorità riconosciuta, chi potrebbe assegnare al

(19) Nell'ordinamento nazionale una definizione legale delle tecnologie basate su registri distribuiti è contenuta nell'art. 8-*ter* della l. 11 febbraio 2019, n. 12. Tale previsione, con una tecnica legislativa molto diffusa ma spesso inefficace, aveva demandato all'Agenzia per l'Italia Digitale (AgID) di individuare – entro novanta giorni dalla data di entrata in vigore della legge (13 febbraio 2019) – gli essenziali «*standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3*». L'art.8-*ter* dispone: «*Si definiscono «tecnologie basate su registri distribuiti» le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili*». Gli standard tecnici non sono stati pubblicati e la previsione normativa non ha dispiegato i propri effetti nell'ordinamento e nel mercato, pur avendo avuto un indubbio effetto positivo da un punto di vista politico e mediatico tra gli attori economici avendo generato una maggiore consapevolezza delle opportunità offerte dalle tecnologie DLT. Per alcune note critiche sulle previsioni del citato articolo si veda, Bomprezzi, *Commento in materia di* blockchain *e* smart contract *alla luce del nuovo Decreto Semplificazioni*, in *Diritto Mercato Tecnologia*, 27 febbraio 2019; Cascinelli - Bernasconi - Monaco, Distributed Ledger Technology *e* Smart Contract*: finalmente è Legge. Prime riflessioni su una rivoluzione tecnologico-giuridica*, in *Rivista di diritto bancario*, 4 marzo 2019.

(20) Consultabile sul sito <Mise.gov.it.>.

proprietario di un terreno tokens aggiuntivi (o variare quello esistente) per rappresentare gli appartamenti che vi sono stati realizzati?
In secondo luogo, la perdita della chiave crittografica di accesso alla posizione giuridica rappresentata dal token implica la perdita della stessa, qualunque sia il suo valore (21).
In terzo luogo è vero che in una Blockchain pura resta traccia delle operazioni compiute e la sicurezza e fiducia all'interno della catena coincidono con la certezza che il sistema informatico riesce ad attribuire al dato temporale in cui avviene la transazione (il c.d. *timestamp* o marca temporale) ed alla validazione della transazione ad opera non di un'autorità terza, ma dalla stessa comunità o, più precisamente dal consenso distribuito della maggior parte dei computer del *network* (50%+1) (22).
Tutto questo non risolve però il problema della identificazione delle persone che vi operano, di regola sotto pseudonimo, con ovvie conseguenze sul piano della normativa antiriciclaggio.
In quarto luogo, è pur vero che anche nella modalità *permissionless* tutti i nodi della rete detengono una copia aggiornata dei dati contenuti nel registro e possono partecipare al processo di validazione delle transazioni da includere nei blocchi che vengono progressivamente inseriti nel registro mediante meccanismi di "*proof of work*" basati sull'utilizzo di risorse computazionali per la risoluzione di problemi matematici estremamente complessi, senza la necessità di un controllo esercitato da alcuna autorità centrale. Tale caratteristica permette una sostanziale disintermediazione grazie alla creazione di un modello di fiducia che non è garantito da un ente centrale o da una entità terza comunque guidati dalle persone (una banca, una Autorità pubblica o un fornitore tecnologico), ma basato sull'esercizio di una attività computazionale da parte delle macchine. La registrazione dei dati presso i nodi della rete assicura una sostanziale inalterabilità e una scansione cronologica (c.d. *time-stamp*) di quanto inserito mediante tecniche crittografiche a chiave asimmetrica nella catena dei blocchi; tutte le transazioni sono trascritte nel registro in modo trasparente e quindi possono essere tracciate e si può risalire con esattezza alla serie di scambi relativi ad un bene digitale che sono consultabili e verificabili. Inoltre, tutte le transazioni, una volta trascritte nel registro, non possono essere modificate senza che sia necessario raccogliere il consenso della maggioranza dei nodi coinvolti per apportare la modifica in discussione, operazione evidentemente molto complessa in termini di capacità di calcolo computazionale, in un rapporto direttamente proporzionale alla numerosità dei nodi della rete (23).
Tuttavia la Blockchain pura vive in uno spazio vuoto di diritto, poiché nessun giudice potrà proteggere consumatori truffati o soggetti deboli, sia per l'anonimato che protegge i nodi, sia per la materiale impossibilità di modificare un'operazione sulla catena di blocchi sia pure eseguita sotto la minaccia di un'arma.
Tra le molteplici criticità evidenziate nell'impiego di tecnologie basate su DLT, preme evidenziare, in quinto luogo, che la tecnologia *blockchain* offre non solo la possibilità di entrare nel registro, ma teoricamente di inserire ciò che ciascuno vuole, senza alcuna forma di controllo non solo sull'accesso, ma anche sul contenuto. Il problema del contenuto non è secondario, perché una cosa è avere un registro tecnicamente sicuro, altra cosa è che quel registro contenga anche informazioni vere e sicure (24).
Dunque, realizzare un registro pubblico sicuro e inattaccabile non significa anche garantire che il contenuto sia attendibile. Si tratta di un tema noto nel settore informatico, conosciuto come "*garbage in, garbage out*" (GIGO) nel mondo delle DLT: le piattaforme informatiche elaborano in modo acritico un insieme di dati in entrata prescindendo completamente dalla veridicità o correttezza del dato immesso (*garbage in*) e producendo, a loro volta, un esito potenzialmente non coerente con quanto auspicato o atteso (*garbage out*). Infatti, una piattaforma DLT/*blockchain* certifica l'inalterabilità di quanto è stato immesso nella catena di blocchi, ma non è in grado di certificare l'unicità e l'autenticità *ab origine* del prodotto digitale, come ad esempio l'autore, il numero delle copie realizzate etc. Questo problema strutturale della tecnologia pone in dubbio che il ruo-

(21) Si vedano gli esempi proposti da Bechini, *Il notaio digitale*, Milano, 2019, 155.

(22) Il blocco genesi della blockchain, creato dal suo fondatore Satoshi Nakamoto, è datato 3 gennaio 2009 (*The Times*, 3 gennaio 2009: "*Chancellor on brink of second bailout for banks*") ed è il primo mattone che ha dato l'avvio alla circolazione dei bitcoin, come moneta virtuale la cui prima versione 0.1.0 risale al dicembre 2010.

(23) La bibliografia in tema di *blockchain* è vasta, per tutti v. Dimitropuolos, *The Law of blockchain*, in *Washington Law Rev.*, 2020, 95 (3), 1117; De Filippi - Wright, *Blockchain and the Law, the Rule of Code*, Harvard University Press, 2018, 25; Jackson, *Is it possible to comply with GDRP using blockchain?*, in *International Financial Law Review*, 2018; Finocchiaro - Bomprezzi, *A legal analysis of the use of blockchain technology for the formation of smart legal contracts*, in *Medialaws*, 2/2020, luglio 2020; Sarzana - Nicotra, *Diritto della blockchain, intelligenza artificiale e Iot*, Milano, 2018.

(24) Ad esempio se visualizziamo la pagina internet del Registro imprese di Londra "*Company's House*", si ottengono, come per il nostro Registro imprese, informazioni di tutte le società registrate, con possibilità di scaricarne lo Statuto, di vedere i nominativi degli amministratori, insomma, di avere un po' tutte le stesse informazioni che abbiamo nel nostro Registro imprese. Però in fondo alla pagina internet c'è un *disclaimer* (esonero di responsabilità), che avverte che le informazioni presenti su quel Registro non sono verificate e quindi possono non essere complete, dati rilevanti possono essere stati omessi, di qui l'esclusione di ogni responsabilità.

lo della piattaforma sia dirimente rispetto alla garanzia che l'utente/consumatore assume di ricevere rispetto a temi essenziali per un NFT quali l'origine (ossia chi è il creatore), la piena titolarità dei diritti anteriormente al tracciamento sulla piattaforma, l'unicità o la scarsità del bene digitale. Nessuno può escludere che a breve ulteriori tecnologie possa offrire in modo stabile e sicuro queste garanzie, ma nell'attuale configurazione dei rapporti giuridici connessi alla realizzazione di un NFT, l'assunzione di responsabilità per questi aspetti viene disciplinata mediante contratti stipulati in linguaggio naturale tra il creatore/titolare e la piattaforma che, a sua volta, assume questi elementi come presupposti per l'offerta agli utenti/consumatori.

Minori rischi presenta la Blockchain chiusa (*permissioned*) che infatti è stata proposta per sostituire registri centralizzati esistenti, come i registri immobiliari. Si pensi al caso che soggetti specializzati detti *Gatekeepers* siano incaricati di verificare i titoli di trasferimento, curandone poi l'inserimento in un registro. A prescindere dai costi energetici di una blockchain composta da molti nodi, il rischio più evidente di una simile prospettiva è quello di trovarsi a "reinventare la ruota": il sistema composto dalle agenzie governative (Catasto e Conservatoria dei registri immobiliari) e notai, cioè un gruppo selezionato di concessionari controllati dal ministero di giustizia e consigli notarili, sembra funzionare egregiamente.

Oggi il sistema che, in Italia e negli altri Paesi di *civil law*, governa il risparmio immobiliare privato è il prodotto di una sinergia virtuosa tra agenzie pubbliche quali Catasto (poi Agenzia del territorio, oggi incorporata nell'Agenzia delle Entrate); Conservatoria dei Registri immobiliari (ora Agenzia delle Entrate); Archivi notarili e un numero relativamente ridotto di concessionari, pubblici ufficiali dotati di solida cultura giuridica, altamente qualificati e controllati (notai). I consigli notarili e l'archivio notarile svolgono infatti una funzione di *gate keeper* e il concessionario che non è all'altezza o che altrimenti tradisce la fiducia in esso riposta viene sanzionato in modo effettivo in quanto organicamente connesso con il sistema di controllo.

Il sistema ha saputo nel tempo mantenersi in equilibrio e la qualità delle relazioni tra agenzie pubbliche e notariato ha consegnato al mondo degli affari e alla società civile una solida spina dorsale istituzionale che spiega il progressivo accrescersi del risparmio immobiliare privato. Il sistema si regge insomma sopra meccanismi istituzionali complessi che vanno salvaguardati da interpretazioni che finirebbero per avvantaggiare non i cittadini ma gli interessi di quanti (sopratutto *corporations* globali) lucrerebbero dalla loro liquidazione.

Pur rifuggendo da ogni determinismo e da ogni spiegazione dogmatica, il dato economico del risparmio immobiliare degli Stati Uniti, basato sull'assicurazione del titolo di proprietà, non rende quel sistema desiderabile, anche, ma non solo, per i maggiori costi dei professionisti e di una assicurazione che, in mancanza di una affidabilità dei registri immobiliari costituisce una sorta di surrogato "per equivalente" della perdita della proprietà del bene immobile.

È la stessa rilevanza del fattore tecnico proprio del registro distribuito e condiviso che impone quindi riflessioni più generali, da tenere sullo sfondo del tema qui trattato. La complessità della tecnologia in esame, attorno alla quale ruotano una molteplicità di attori, in particolare i fornitori di infrastrutture DLT, non può occultare il fatto che questi soggetti si profilano quali possibili nuovi gatekeepers di un mercato immobiliare o finanziario tokenizzato. Un mercato che potrebbe risultare soggetto a un processo non già di disintermediazione attraverso la blockchain, bensì di re-intermediazione attraverso la stessa e i soggetti che la controllano. Mi limito a questo cenno solo per sfatare il mito che pervade gli i *cantores* del progresso tecnologico del nuovo millennio, ed i "panglossiani" declamatori delle nuove tecnologie come migliore dei mondi possibili (25).

## 5. La definizione di *token* e i diversi statuti correlati alle varie funzionalità

Come sopra accennato, non esiste una definizione univoca di *token* né da un punto di vista informatico né giuridico. Si tratta di uno strumento digitale che consente l'incorporazione di diritti e ne permette la circolazione e la conservazione garantita in modalità crittografica. Secondo un interessante indirizzo le caratteristiche del *token* richiamano il modello giuridico sotteso ai titoli di credito e in particolare alle evoluzioni in tema di dematerializzazione di strumenti finanziari (26).

Sebbene il *token* non sia riconducibile necessariamente alla tecnologia *blockchain*, poiché veniva da tempo utilizzato per garantire un maggior livello di sicurezza nelle

(25) Sui limiti all'utilizzo delle tecnologie DLT nel settore immobiliare v. recentemente Bertelli, *Diritti reali e asset digitali: l'utilizzo dei token nel settore immobiliare*, in *Tecnologie e diritto*, 2023, 54 ss. V. anche Alpini, *L'impatto delle nuove tecnologie sul diritto*, in *Comparazione dir. civ.*, 2018, 13 ss.; Manente, Blockchain: *la pretesa di sostituire il notaio*, in *Notariato*, 2016, 211 ss.; Moringello - Odinet *The Property Law of Tokens*, in *Florida L. Rev.*, 2022, 607 ss. Damiani, *Blockchain Application in General Private Law: The Notarchain Case*, in Caliguri (a cura di), *Legal Technology Transformation. A Practical Assessment*, Napoli, 2020, 229 ss. il quale sostiene (p. 236) che «*the intervention of a qualified intermediary is appropriate, and therefore that could also be the Notary, who not only performs the function of a certifying agent but also the one of examining the will of the parties and the one of suggesting in order to adjust it to better realise the ultimate goal the contractors want to pursuit*».

(26) In merito si rinvia a Rulli, *Incorporazione senza* res *e dematerializzazione senza accentratore: appunti sui* token, in *Orizzonti del Diritto Commerciale*, 1, 2019, 121 ss.

transazioni bancarie, ha trovato il suo naturale contesto di sviluppo nell'ambito delle piattaforme basate su *Distributed Ledger Technology* (27).
Poiché gli NFT sono una rappresentazione digitale di sottostanti beni virtuali oppure di beni fisici, e rispetto a tali *asset* possono essere altresì rappresentativi di una pluralità di diritti, occorre illustrare brevemente le diverse tipologie di classificazione che sono state sviluppate a livello nazionale e internazionale, avendo ben presente che la qualificazione giuridica del *token* dipende dal tipo di diritti che sono al medesimo connessi: non tutti gli NFT sono uguali sotto il profilo giuridico. Pertanto, un punto fondamentale al fine di definire il quadro normativo applicabile all'emissione e all'offerta nei confronti del pubblico dei *token* – inclusi quindi gli NFT – è quello di identificare i diritti connessi a ciascun *token*.
Vi è, in primo luogo, una generale tripartizione diffusa a livello internazionale che distingue tra *payment token* (ossia strumenti di pagamento digitali per acquisire beni o servizi), *utility token* (che forniscono accesso digitale ad una applicazione o ad un servizio) e una terza categoria che viene definita come *asset/ security/equity* oppure *investment token*.
Accanto a tale classificazione, a livello nazionale si è anche affermato che un *token* che conferisca al titolare il diritto ai proventi di una attività economica, sia trasferibile e venga offerto come strumento con finalità di investimento – a seconda delle sue specifiche caratteristiche – potrebbe rientrare nelle categorie tradizionali di: «strumento finanziario» (es. strumento di debito o *equity*); oppure «prodotto finanziario» – definiti dalla CONSOB come «proposta di investimento che implichi la compresenza dei tre seguenti elementi: (*i*) impiego di capitale, (*ii*) promessa/ aspettativa di rendimento di natura finanziaria e, (*iii*) assunzione di un rischio direttamente connesso e correlato all'impiego di capitale».
Un *token* che conferisca al titolare il diritto di assumere decisioni in relazione alla gestione di una attività economica potrebbe rientrare nella categoria degli strumenti finanziari, *sub specie* di uno strumento di capitale (ad esempio una azione/ quota di S.r.l. o strumento assimilabile) (28).

Un *token* invece che conferisca al titolare il diritto di godimento di un immobile e che non abbia finalità di investimento, potrebbe non essere attualmente soggetto a specifica regolamentazione (29) (almeno fino all'entrata in vigore della proposta di Regolamento presentata dalla Commissione europea nel settembre 2020, denominata MiCA, di cui sopra).

## 6. Struttura e funzione del *token*. Un gigante dai piedi d'argilla?

A fronte della rapida diffusione di applicazioni legate a *token* infungibili ci dobbiamo porre due quesiti, uno relativo alle modalità tecnologiche che rendono possibile la realizzazione di un *token* infungibile e l'altro teso a comprendere quale finalità possa avere la realizzazione di contenuti "unici" in un ecosistema come quello digitale che è strutturalmente predisposto per replicare gratuitamente in modo illimitato i contenuti senza che le ulteriori copie soffrano alcun degrado in termini qualitativi.
Innanzitutto la qualificazione di infungibilità la possiamo analizzare in termini definitori.
Dal punto di vista civilistico, non può che farsi rientrare l'NFT nella più generale definizione di "bene" contenuta nell'art. 810 c.c., che comprende qualunque cosa materiale ed immateriale, una *res* intesa non in senso naturale ma in senso giuridico, suscettibile di formare oggetto di diritti e idonea a soddisfare un'utilità o una necessità dell'uomo, un interesse giuridicamente apprezzabile, di natura patrimoniale.
Il codice civile non definisce i beni fungibili e infungibili ma la categoria, che ha una tradizione risalente al diritto romano, è spesso richiamata per qualificare e regolamentare in modo speciale determinate figure contrattuali.
Occorre dunque studiare gli NFT non solo in prospettiva strutturale, ma anche tenendo conto della prospettiva economico-funzionale (30), valorizzando il bene NFT

(27) Secondo Glatz, i token sono «central to most social and economic innovations developed with blockchain technology», in *A Blockchain Token Economy*, reperibile in <https://heckerhut. medium.com/a-blockchain-token-taxonomy>.

(28) Sul punto cfr. De Luca, *Documentazione crittografica e circolazione della ricchezza assente*, in *Riv. dir. civ.*, 2020, 100 ss.; Carriere - De luca - De Mari - Gasparri - Poli, *Tokenizzazione di azioni e azioni tokens*, in *Quaderni giuridici Consob*, 25 gennaio 2023, 13. Nella seduta dell'11 Aprile 2023, il Consiglio dei ministri, su proposta del Ministro dell'economia e delle finanze Giorgetti, ha approvato un disegno di legge che introduce interventi a sostegno della competitività dei capitali con l'obiettivo di una riforma organica volta a incentivare la quotazione delle società e diffondere l'azionariato della Borsa italiana, anche al fine di sostenere le imprese che puntano a crescere e ad aumentare la propria competitività mediante il ricorso al mercato dei capitali. Tra le norme, prevista la cosiddetta "dematerializzazione delle quote delle Srl".

(29) Sul punto v. Giordano, *Profili legali degli NFT nel web3: dalla creazione alla vendita degli oggetti nel metaverso*,in *Metaverso*, a cura di Cassano-Scorza, Pisa 2023, 525 ss.

(30) La prima operazione metodologicamente indilazionabile appare quella di liberarsi dalla fallace idea della proprietà di un bene quale "rapporto giuridico puro" e di recuperare il fenomeno alla sua storicità, secondo l'insegnamento di Finzi, *Le moderne trasformazioni del diritto di proprietà*, (1922), in *L'officina delle cose*, Milano, 2013, 17 ss.; e di Pugliatti, *La proprietà nel nuovo diritto*, Milano, 1954. Della tensione tra diritto ed economia per il tramite dell'evoluzione tecnologia si è fatto interprete Grossi, *Globalizzazione, diritto, scienza giuridica*, in *Foro It.*, 2002, 5, 156, il quale ha affermato che «(l)a prassi economica si fa produttrice del diritto: la nuova economia e le nuove mirabolanti tecniche esigono arnesi giuridici nuovi irreperibili nel solco della bimillenaria tradizione romanistica

nelle sue variate strutturazioni immateriali ed economiche, che esigono molteplici statuti disciplinari, nel senso che a diverse funzioni corrispondono statuti diversi.
Si tratta di una impostazione che si colloca dichiaratamente sulla scia dell'insegnamento metodologico ascarelliano, che sottolinea la relatività di ogni schema concettuale; e nel solco di tale impostazione è utile richiamare il monito di Paolo Ferro-Luzzi nell'Introduzione alle sue Lezioni di diritto bancario, che si attaglia perfettamente all'esame dell'evoluzione tecnologica in esame: in quelle pagine, il Maestro ricordava come «possa essere fuorviante il tentativo di inquadrare a forza nuovi fenomeni e nuove realtà entro i modelli tradizionali ricevuti dalla dogmatica»(31).
Gli Nft incorporano al loro interno, a seconda dei casi, diritti amministrativi o patrimoniali o altre utilità legati a progetti imprenditoriali, con l'aggiunta che i diritti che incorporano si attivano, modificano o estinguono in modo automatico, secondo la logica degli *smart-contract* (definibili come un protocollo di transazione computerizzato che esegue i termini di un contratto). Infungibile è un bene considerato nella sua specificità e non sostituibile con un altro della stessa specie. Se esaminiamo il concetto di fungibilità in un ecosistema digitale, sono *fungible token* gli *asset* che possono essere sostituiti con una unità del tutto identica, come ad esempio una criptovaluta, che è del tutto replicabile, sostituibile con altra dello stesso genere e divisibile.
Al contrario, l'NFT è un *token* crittografico che rappresenta un *asset* unico, non reciprocamente intercambiabile con un altro *token* in quanto dotato di una propria peculiarità in termini di funzionalità e caratteristiche e quindi di una propria individualità che lo rende unico o raro (in termini di scarsità). Di conseguenza, una delle principali differenze tra *fungible token* e NFT è che i primi sono divisibili in frazioni, mentre gli NFT sono indivisibili sebbene le esigenze commerciali di soddisfare i bisogni del mercato dell'arte digitale hanno indotto a offrire anche NFT suddivisi in quote.
Da un punto di vista tecnologico la configurazione di un NFT ha come presupposto la realizzazione di *smart contract* da parte di programmatori informatici sulla base di alcuni standard che sono stati sviluppati sulla piattaforma *blockchain* di Ethereum.
Il protocollo più diffuso è lo standard ERC-721, dedicato all'emissione e allo scambio di *token non fungible,* mentre un ulteriore protocollo (ERC1155) è stato successivamente sviluppato per consentire di realizzare degli *smart contract* che abbiano delle funzionalità sia *fungible* che *non-fungible*. Al fine di garantire l'unicità dell'NFT all'interno della piattaforma, ogni NFT possiede perciò un identificativo univoco dato dalla chiave crittografica dello *smart contract* e dall'ID del *token* che è stato creato.
Esaminiamo, infine, quali possano essere le finalità sociali e le motivazioni economiche alla base della realizzazione di un NFT.
In termini funzionali la creazione degli NFT e il loro successo risponde ad una esigenza (quasi) primordiale che induce coloro i quali decidono di acquisire degli *asset* digitali come gli NFT di avere la possibilità di affermare di esserne l'unico proprietario, semplicemente applicando evolutivamente i concetti secolari sviluppati in merito alla proprietà di un bene nell'ecosistema fisico.
Le funzioni essenziali, come abbiamo già evidenziato, che caratterizzano un NFT e inducono a ritenere che un *token non-fungible* possa replicare le caratteristiche di un bene fisico, sono la certificazione dell'unicità/rarità dell'*asset* digitale mediante la *blockchain*, la possibilità di rendere esclusivo l'accesso al contenuto digitale e l'opportunità di commercializzare l'NFT sulla piattaforma *blockchain* di Ethereum o altre piattaforme collegate.
Tuttavia, presumere una analogia tra un NFT e i diritti ad esso connessi e la proprietà di bene fisico risulta inappropriato. Infatti, se appare comprensibile che in un contesto economico e sociale nel quale la gran parte delle relazioni personali e professionali avvengono in un contesto digitale, la realizzazione di un prodotto digitale che possa garantire la scarsità certificata, l'immutabilità e la trasferibilità rappresenti il completamento in ambito digitale degli elementi che hanno sempre caratterizzato un ecosistema fisico, occorre evidenziare che è fuorviante ritenere che un NFT possa avere lo stesso grado di fruibilità e di tutelabilità di un equivalente *asset* fisico.
Infatti, nell'attuale stadio di evoluzione delle tecnologie che consentono la creazione e la gestione di un NFT, tuttora esistono delle incertezze rispetto alla possibilità tecnica di accedere nel lungo periodo al contenuto digitale oggetto delle transazioni a causa delle possibili problematiche tecniche connesse alla funzionalità dell'*hash* e al *link* tra il certificato digitale e l'*asset* digitale, non vi sono garanzie rispetto ai rischi di obsolescenza o di mancata manutenzione delle piattaforme *blockchain* che attualmente costituiscono la tecnologia necessaria della creazione e gestione degli NFT, non vi sono garanzie – se non di natura contrattuale – che il creatore/titolare dell'*asset* digitale non violi gli obblighi negoziali che garantiscono una corretta gestione della unicità/scarsità e il conseguente valore economico dell'NFT.
In altri termini, le caratteristiche tecnologiche degli NFT presentano dei fattori che potrebbero far ritenere

radicata fondamentalmente sulla nozione di cosa corporale, una nozione che a fine novecento appare paleolitica ai contemporanei uomini di affari. Ci sono esperienze giuridiche nuove e si «inventano» strumenti giuridici nuovi atti a ordinare la nuova circolazione globale». Cfr., altresì, IRTI, *Norma e luoghi. Problemi di geo-diritto*, cit., 9.

(31) FERRO-LUZZI, *Lezioni di diritto bancario*, Torino, 1995, VII.

realizzabile la creazione di *token non-fungible* che incorporino immutabilmente degli *asset* digitali di molteplici tipologie, ma l'immaturità delle stesse tecnologie, l'instabilità degli attori del mercato rispetto alle tempistiche di fruizione attese per gli NFT nonché l'inesistenza, allo stato, di strumenti che rendano davvero immutabile e efficacemente tutelabile la relazione tra i beni fisici sottesi e i beni digitali da essi derivati oppure le azioni poste in essere *off-chain* (ad esempio dal creatore/titolare) e quanto certificato all'interno della piattaforma *blockchain,* rendono tuttora gli NFT inadeguati ad essere ritenuti degli *asset* giuridicamente comparabili con gli equivalenti prodotti del mondo fisico. In sintesi, gli NFT parrebbero un "colosso con i piedi di argilla" (32).

## 7. Cenni sugli *smart contracts* utilizzati per gli NFT

Al fine di tratteggiare compiutamente il modello di funzionamento dell'NFT occorre richiamare il ruolo che gli *smart contracts* svolgono nella realizzazione di un NFT.

Infatti gli *smart contracts* presenti in modalità crittografica nei blocchi della piattaforma *blockchain* contengono dei programmi informatici autoeseguibili che tengono traccia di chi ha creato il contenuto digitale, di chi lo acquista e lo scambia, ad esempio attivando ad ogni passaggio di proprietà dell'NFT l'obbligo delle parti di pagare una *royalty* percentuale determinata dal creatore.

Il tracciamento sulla piattaforma *blockchain* mediante *smart contract* (o le successive modalità tecnologiche che verranno sviluppate per garantire la medesima funzione) risulta peraltro un elemento costitutivo nella realizzazione di un NFT poiché garantisce l'immutabilità delle informazioni ricevute sulla unicità (o scarsità) del bene digitale e sulle dichiarazione di originalità e autenticità del prodotto rilasciate dal creatore e/o dalla piattaforma, nonché tiene traccia e aggiorna ogni elemento rilevante circa la creazione, la gestione, la commercializzazione e il valore degli NFT.

La riflessione scientifica ha svolto numerosi interessanti approfondimenti in merito alla natura dello *smart contract* e alle diverse funzioni che possono essere svolte da questi strumenti informatici, sulle opportunità e sui potenziali rischi per l'ordinamento giuridico, nonché sulle sfide che le innovazioni potenzialmente connesse con l'adozione degli *smart contract* potrebbero arrecare alle dinamiche sociali e professionali (33). Nell'ambito del presente contributo non è possibile affrontare la tematica nella sua complessità, ma ci limitiamo a richiamare alcuni elementi che sono funzionali a comprendere il loro utilizzo nella realizzazione di un NFT.

Pur nella consapevolezza che non esiste una qualificazione codificata e generalmente adottata, con il termine *smart contract* si intende un protocollo informatico che, adottando (ad oggi) la tecnologia *Distributed Ledger*, consente di realizzare un processo in grado di dare esecuzione automatica di una o più previsioni contrattuali mediante l'individuazione di condizioni predefinite e intellegibili informaticamente secondo il principio causale dell'*if and then*. In altri termini, al verificarsi dell'evento X (*if*), l'algoritmo è stato impostato per porre in essere l'azione Y (*then*).

Appare largamente condiviso che nell'ordinamento italiano lo *smart contract* non sia un contratto, ossia un accordo con il quale le parti regolano un rapporto giuridico patrimoniale, neppure nella forma di un contratto atipico (art. 1322 c.c.), ma uno strumento per l'esercizio dell'attività negoziale che le parti possono utilizzare in via esclusiva o non esclusiva per negoziare, concludere o eseguire un contratto.

I limiti che possiamo ricondurre all'utilizzo degli *smart contracts* sono ben noti, quali la assoluta (quantomeno allo stato) immodificabilità delle previsioni che possono implicare rilevanti problematiche sia per la soluzione di eventuali vizi genetici del contratto, sia per la gestione degli ulteriori eventi che possono modificare nel tempo i presupposti fattuali che hanno indotto le parti alla conclusione del contratto e che troverebbero soluzione, in un ambiente non algoritmico, ad esempio con la risoluzione per eccessiva onerosità o con la riduzione ad equità.

A questo si aggiungono tre fattori problematici che emergono quando la realtà umana e fattuale si devono necessariamente incrociare con la rigidità degli algoritmi degli *smart contracts*:

*i*) gli errori umani del programmatore nell'impostazione degli condizioni che attivano i programmi autoeseguibili, che obbligano le parti, in una logica di buona fede nell'esecuzione del contratto, ad una successiva pattuizione che, nell'ambito di un ulteriore *smart contract* o in altra sede negoziale, riconduca il sinallagma contrattuale alle originarie pattuizioni (quando è ancora contrattualmente possibile);

*ii*) gli errori (volontari o accidentali) dei c.d. oracoli, cioè di quelle entità qualificate esterne all'infrastruttura nella quale opera lo *smart contract* alle quali le parti delegano la verifica dell'avveramento di una condizione (es. i millimetri di pioggia che sono caduti o il raggiungimento di un prezzo di un titolo azionario o l'unicità di una opera d'arte digitale) che attiva l'esecuzione automatica di uno *smart contract*;

*iii*) in termini più strutturali, ma non meno rilevanti, la presenza di una asimmetria informativa o di un gap

(32) Riprendo la citazione, attribuita a Diderot, da Nava, *I non-fungible token*, in *Il diritto nell'era digitale*, a cura di Giordano - Panzarola - Police - Preziosi - Proto, Milano, 2022, 247.

(33) Per tutti v. Maugeri, *Smart contracts*, in *Enc. dir., I tematici, Contratto*, Milano, 2022, 1132, con ampi riferimenti alla letteratura interna e internazionale.

di conoscenze tecniche che rendono talvolta molto complesso al consumatore medio l'accesso consapevole alla fruizione degli *smart contracts* di cui, soprattutto nei mercati finanziari ed assicurativi, gli utenti finali rischiano di sentirsi "vittime".

Tutti questi elementi di attenzione rispetto ai limiti strutturali dell'utilizzo degli *smart contracts* sono presenti anche nella diffusione dell'utilizzo degli NFT, nella misura in cui l'offerta di contenuti digitali di diversa natura si sta indirizzando verso l'utilizzo di questi strumenti informatici in modo massivo.

Le modalità con le quali sono strutturati gli *smart contracts* nell'ambito della creazione degli NFT sono molteplici e in continua evoluzione, ma in termini generali, in considerazione delle finalità per le quali attualmente vengono utilizzati per rendere possibile un NFT, possiamo qualificarli come degli strumenti per l'adempimento di obbligazioni contrattuali che le parti hanno stipulato in linguaggio naturale in un altro documento (in forma digitale o cartacea) e pertanto in tale contesto negoziale si assume che vengano adottate le previsioni atte a definire gli elementi caratteristici della dinamica contrattuale e a dirimere le relative controversie.

Questa modalità implica che possano emergere alcune problematiche giuridiche rilevanti che occorre evidenziare:

*a*) Poiché le obbligazioni assunte dalle parti con il contratto redatto in linguaggio naturale devono essere convertite in un linguaggio informatico utilizzabile dalla piattaforma *blockchain*, può accadere una errata o incompleta trasposizione delle obbligazioni da parte del programmatore, ad esempio relative alla percentuale di *royalty* attribuita al creatore/titolare del contenuto digitale in occasione di ogni successivo atto di trasferimento dell'NFT.

In tale fattispecie si porrebbero due problematiche:

- *in primo luogo* la natura della responsabilità del programmatore che dovrà rispondere dell'inadempimento contrattuale ai propri obblighi di trasporre fedelmente e diligentemente in linguaggio macchina le previsioni pattizie tra creatore/titolare e piattaforma. Dobbiamo assumere che, nei limiti dei consueti criteri del dolo e della colpa grave e senza presumere comportamenti aventi, ad esempio, rilevanza penale, il programmatore risponderà, anche a fini risarcitori, ai sensi del contratto con il quale è stato incaricato di svolgere tale funzione, ad esempio un contratto di appalto per la fornitura di servizi informatici.
- *in secondo luogo* si pone il tema della inalterabilità delle previsioni dello *smart contract* che è stato reso immutabile grazie alle funzionalità della piattaforma *blockchain*. Nella fattispecie sopra prospettata, ossia di un semplice errore nella definizione della percentuale della *royalty*, le parti, in una logica di esecuzione in buona fede delle previsioni pattizie, potranno introdurre nella piattaforma un ulteriore *smart contract* che preveda in parallelo all'esecuzione del primo *smart contract* un secondo automatico adempimento che neutralizzi parzialmente gli effetti giuridici indesiderati prodotti dal primo, introducendo una previsione in senso opposto che sia pari alla differenza percentuale riscontrabile tra il valore corretto e la *royalty* inizialmente erroneamente trasposta in linguaggio informatico.

*b*) L'utilizzo dello strumento informatico dello *smart contract* ricade nel principio generale della libertà delle forme contrattuali e pertanto la forma scritta *ad substantiam* prevista dall'art. 1351 c.c. e dalle discipline speciali è richiesta nei limiti espressamente previsti e, in relazione alla natura dei contratti, nella misura in cui le caratteristiche tecniche degli *smart contract* lo consentano. Peraltro, come accennato *supra*, non sono ancora state pubblicate dall'Agenzia per l'Italia Digitale le linee guida previste dall'art. 8-*ter*, comma 2 del d.l. n. 135/2018 per definire i requisiti e gli effetti degli *smart contract* e pertanto non è ancora stato possibile un compiuto e strutturato inquadramento delle relative caratteristiche e dei possibili utilizzi.

*c*) Un ulteriore aspetto di analisi si concentra sulla qualificazione dell'utilizzo degli *smart contract* su piattaforma *blockchain* non solo come una modalità necessaria (e non alternativa) di esecuzione del contratto, ma come un elemento necessario del contratto per realizzare un NFT. Probabilmente affermare che l'utilizzo degli *smart contract* su piattaforma *blockchain* possa essere qualificato come un elemento necessario del contratto non tiene in debita considerazione la prospettiva temporale insita nell'utilizzo degli NFT, siano essi certificati digitali relativi ad opere d'arte oppure ad investimenti immobiliari: l'obbligazione che deve essere fornita dalla piattaforma è quella di assicurare un prodotto digitale che sia immutabile, tecnicamente unico/raro, trasferibile (nei limiti già evidenziati) e che, allo stato attuale dell'evoluzione tecnologica, possa essere fornito mediante l'utilizzo di uno *smart contract* su piattaforma *blockchain*. È invece un elemento congenito (e inevitabile) che, nella prospettiva temporale di lungo periodo sottesa alla fruizione degli NFT, lo sviluppo tecnologico si evolva in modo significativo e quindi l'obbligazione contrattuale di garantire le caratteristiche peculiari del *token* digitale debba avere attuazione con strumenti tecnologici differenti e più evoluti. Occorre perciò distinguere in sede di redazione contrattuale tra l'obbligazione di garantire le caratteristiche intrinseche dell'NFT e le modalità tecnologiche che saranno tempo per tempo vigenti, relegandole ragionevolmente in un allegato tecnico al contratto che possa essere separatamente negoziato ed aggiornato.

## 8. Come funziona un NFT e cosa rappresenta

Il prodotto digitale nel contesto delle opere artistiche a cui rimanda l'NFT può essere una foto, una canzone, un video, un *gif,* un *tweet*, una immagine che riteniamo abbia valore artistico (34). In altri termini, tali prodotti digitali non hanno una caratteristica oggettiva intrinseca che risulti necessaria per trasformarli in NFT, ma sono le proprietà che il pubblico dei potenziali acquirenti ritiene di attribuire a questo prodotto digitale a guidare l'identificazione di quali beni possano diventare dei *token* non fungibili (35).

La descrizione della natura tecnologica dell'NFT consente di determinare quale sia la relazione fattuale e quindi giuridica tra il *token* e l'opera digitale e, inoltre, quali ruoli possano svolgere nelle diverse architetture contrattuali possibili i tre principali attori ossia, come detto: il creatore/titolare del prodotto (digitale o digitabile), la piattaforma e l'utente/consumatore.

Alla base del contratto vi è un prodotto nativo digitale oppure che è stato reso digitale (ossia tramutato in alcune linee di codice informatico) tramite un processo di tokenizzazione (un'opera d'arte, un video, una canzone, un data-base immobiliare etc.) che è rappresentato da un file, contenente una serie di *byte*, che può avere diverse dimensioni. Mediante un processo di compressione algoritmica denominato *hashing* viene realizzata una sequenza, chiamata *hash,* che viene memorizzata in modo sostanzialmente inalterabile nei blocchi di una piattaforma *blockchain* e accoppiata con una marca temporale (36).

All'acquirente dell'NFT (*rectius* del prodotto digitale) viene attribuito un certificato digitale che consente di connettersi in modo univoco ad uno *smart contract* realizzato su una piattaforma *blockchain* (di norma Ethereum o una piattaforma ad essa assimilabile o collegata) che, grazie alla natura univoca dell'*hash*, consente di accedere ad un file non presente sulla piattaforma che contiene il prodotto digitale. Grazie a questi *smart contract* viene anche tracciato e memorizzato chi compra o vende l'opera digitale mediante una registrazione sulla piattaforma *blockchain* incaricata delle sequenze di algoritmi che identificano il prodotto digitale.

Occorre però ribadire (v.*supra* par. 4) che la memorizzazione nella *blockchain* non garantisce l'identificazione della persona fisica o giuridica, ma la possibilità di collegare l'entità che ha dato luogo ai presupposti necessari per dare esecuzione allo *smart contract*.

Perciò la realizzazione e la commercializzazione degli NFT si basa interamente su un sistema di diritti e di tutele di matrice contrattuale. Di conseguenza, poiché i mercati che si stanno progressivamente sviluppando e stanno creando le prassi di mercato sono quelli di diritto anglosassone e i maggiori operatori tecnologici sono basati in tali giurisdizioni, il diritto applicabile ad una parte rilevante dei rapporti tra i titolari/creatori e piattaforme dell'NFT e quindi le tutele appellabili in relazione all'acquisto e alla commercializzazione degli NFT e ai diritti che si ritengono ad essi collegati, sono basati su plessi normativi diversi da quelli di matrice europea continentale e, a maggior ragione, italiana.

Un approfondimento sul funzionamento dell'NFT è prodromico ad una più corretta qualificazione della sua natura giuridica: i dati che vengono inseriti nell'NFT in realtà si limitano all'*hash* e ad alcune proprietà algoritmiche del *token*. Perciò il contenuto digitale che è oggetto della transazione non risiede nella piattaforma *blockchain* poiché lo spazio che occuperebbe renderebbe poco efficiente la sua gestione e sarebbe molto dispendioso replicare una tale mole di dati presso tutti i nodi della rete; pertanto il certificato relativo al prodotto digitale che viene scambiato tra le parti include soltanto un codice digitale sottoposta al processo di compressio-

(34) Storicamente i prodotti digitali antesignani degli NFT che abbiano avuto una rilevante diffusione sono stati, innanzitutto, degli avatar denominati *Cryptopunk* lanciati gratuitamente nel mercato nel giugno 2017 e, poi, un gioco creato su piattaforma Ethereum denominato *CryptoKitties* che è stato lanciato a novembre 2017 e consentiva ai giocatori di acquistare, collezionare, allevare e vendere dei gatti digitali.

(35) Non parrebbe che vi sia una correlazione tra il successo degli NFT e la diffusione delle cripto-valute e, a maggior ragione del *bitcoin*. Da un lato, la diffusione di NFT di facile accessibilità economica può rappresentare uno strumento commerciale per attirare un pubblico più ampio ed incentivare l'uso di specifiche criptovalute; dall'altro, gli NFT si possono acquistare utilizzando qualunque valuta con corso legale (dollaro, euro, sterlina, yen, etc.) non essendo in molti casi l'utilizzo di una criptovaluta una condizione necessaria, ma soltanto una opzione ulteriore di pagamento). Inoltre, l'attuale tumultuoso sviluppo degli NFT utilizza delle piattaforme DLT/*blockchain* diverse dalla originaria *Blockchain* di Satoshi Nakamoto costruita intorno alla *proof of work* e alla generazione di bitcoin, ed in particolare è incentrato sulla piattaforma Ethereum che utilizza una diversa valuta (*Ether*), ma soprattutto si contraddistingue per caratteristiche funzionali di flessibilità adatte alla creazione e diffusione *peer to peer* di *smart contract*. Perciò, in concreto, per quanto riguarda la creazione e la gestione degli NFT, la piattaforma *blockchain*/DLT non viene utilizzata per la sua primigenia finalità di strumento di disintermediazione delle transazioni basata sull'utilizzo di criptovalute (*bitcoin*), bensì ai soli fini della certificazione di inalterabilità e quindi di autenticità del *token* iscritto nei blocchi e delle sue caratteristiche.

(36) Nel linguaggio matematico e informatico, l'*hash* è una funzione non invertibile che comprime una stringa di dati di lunghezza arbitraria in una stringa di numeri e di lettere di lunghezza predefinita L'output è denominato *digest*. L'algoritmo di *hash* è una funzione unidirezionale ossia non è invertibile, quindi non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita come *output*. Nella Blockchain l'algoritmo di *hash* viene utilizzato anche per collegare un blocco di transazioni con quello precedente nella "*chain*" inserendo nel nuovo blocco di transazioni anche *hash* del blocco precedente e quindi concatenando in modo indelebile i blocchi.

ne mediante la funzione algoritmica di hash e alcune proprietà del token che rimandano in modo univoco ad un file esterno alla piattaforma che contiene il prodotto digitale.
Dalle superiori notazioni deriva quindi che l'NFT non rappresenta il contenuto digitale acquisito né un titolo rappresentativo di una serie di diritti afferenti all'opera, ma più verosimilmente uno "*strumento per accedere in modo univoco ad un contenuto digitale non-fungibile rispetto al quale i diritti e le tutele correlate risiedono esclusivamente nei contratti sottoscritti in linguaggio naturale dall'utente/consumatore*" (37).
Le caratteristiche strutturali dell'attuale modalità tecnica di realizzazione degli NFT comportano però alcuni rischi connessi alle inevitabili sviluppi delle funzioni di hashing, ai rischi di evoluzione degli standard tecnologici, ai potenziali problemi di obsolescenza o di mancata manutenzione della piattaforma blockchain oppure a semplici errori nella gestione del file che non sono compatibili con le caratteristiche di lunga durata che i prodotti digitali possono richiedere (pensiamo ad un'opera d'arte, alla tokenizzazione di un bene immobiliare etc.) e con i valori economici in questione. Il rischio che la possibilità di accedere al contenuto digitale sia reso impossibile da problematiche tecniche legate alla funzionalità dell'hash oppure al link tra il certificato digitale e il sito dove avviene lo "*storage*" del file, con conseguente perdita dei contenuti digitali, viene superato utilizzando gli indirizzi IPFS (*Inter Planetary File System*) che fanno capo ad una sistema di file distribuito *off-chain* (simile ai sistemi di scambio file *peer to peer*) che offre la ragionevole certezza che vi sia una moltitudine di siti dove questo contenuto sia ospitato e quindi possa continuare ad essere reperibile online. Ovviamente a questa struttura di data storage, ritenuta altamente performante e tecnicamente affidabile, devono essere collegate tecniche crittografiche che connettono i relativi link alla piattaforma *blockchain* e quindi li rendono, nel contempo, sempre accessibili ma soltanto a chi ne abbia le necessarie chiavi crittografiche.
Anche in questa fase di tumultuosa crescita del mercato la garanzia della piena stabilità ed efficienza nel tempo delle piattaforme *blockchain* e dei siti di "*storage*" dei file rappresenta un elemento differenziale che induce ad una progressiva concentrazione del mercato a beneficio di una piattaforma consolidata come Ethereum che potrà essere parzialmente risolto grazie allo sviluppo di sistemi che garantiscano la piena interoperabilità tra le diverse piattaforme.

(37) Nava, *I non-fungible token*, cit., 256.

## 9. I ruoli svolti dai diversi attori nella creazione di un NFT

Attualmente l'offerta sul mercato di NFT si basa sulla seguente struttura contrattuale: il creatore/titolare del contenuto (digitale o digitalizzabile) sottoscrive con la piattaforma una licenza d'uso del contenuto digitale a fronte di una remunerazione che sovente è fondata su un modello di minimo garantito oltre alla *revenue sharing*, ossia in maggior parte basata sull'aspettativa di guadagnare una percentuale rispetto ai ricavi della commercializzazione, con l'obiettivo di una condivisione tra entrambi gli attori del rischio/opportunità di lanciare un servizio in un mercato allo stato embrionale. Il creatore/titolare di norma assume nei confronti della piattaforma le obbligazioni, da un lato, di garantire di essere l'autore e comunque di poter legittimamente consentire la fruizione (usualmente a titolo personale) del contenuto licenziato e, dall'altro, di poter assicurare l'unicità o la predeterminata scarsità del prodotto digitale.
Occorre sottolineare che attualmente un ruolo centrale nella realizzazione tecnica e nella commercializzazione degli NFT è concentrata nelle mani delle piattaforme che sono in grado di dettare le regole innanzitutto tecniche, ma anche economiche e contrattuali che governano i rapporti tra il titolare/creatore del contenuto (digitale o digitalizzato) e l'utente/consumatore. La piattaforma, infatti, si assume l'onere di commercializzare il prodotto digitale, di organizzare le strategie marketing e le politiche di comunicazione (talvolta selezionando anche gli artisti che possono "esporre" sul proprio sito), rappresenta la controparte contrattuale dell'utente/consumatore rispetto al quale, in ciascun ordinamento, è vincolata a rispettare le rilevanti previsioni in termine di tutela del consumatore. Poiché le tecnologie e le competenze non sono una effettiva barriera in questo mercato, chi è in grado di gestire la specifica competenza tecnologica sta diversificando la propria offerta creando piattaforme *white label*, ossia che possono essere offerte "chiavi in mano" ai titolari/creatori dei contenuti (ad esempio alle associazioni sportive oppure ad un artista rinomato) mediante contratti di licenza del *software*, rendendoli perciò operativamente e contrattualmente in grado di interagire direttamente con i consumatori/utenti. In quest'ultimo caso il regolamento contrattuale che definisce le modalità di realizzazione, le regole di circolazione, le licenze di utilizzo concesse potranno essere definite dal soggetto che riunisce in sé le funzioni di creatore/titolare del contenuto e gestore della piattaforma poiché solo in tal caso sarà effettiva la disintermediazione nella relazione creatore/utente.
L'utilizzo degli NFT viene sovente reclamizzata come una modalità che consente di eliminare il ruolo storicamente detenuto dall'intermediario (che in queste fattispecie sono le case d'asta, le agenzie immobiliari, i me-

dia tradizionali etc.), favorendo un rapporto diretto tra creatore/titolare e l'utente consumatore. In concreto, in questi mercati vi sono ancora dei fattori che ostacolano il perseguimento della disintermediazione, tra i quali tuttora appaiono rilevanti sia l'effettiva limitata conoscenza (e fiducia) negli strumenti tecnologici mediamente detenuta dai clienti, sia l'evidenza che l'ampliamento degli utenti del mercato degli NFT (ad esempio di opere artistiche digitali) presuppone che il creatore/titolare abbia la fiducia dell'utente/consumatore quando garantisce la provenienza, l'originalità, l'unicità o la scarsità di un prodotto digitale, operazione possibile soltanto quando il numero degli utenti è molto ristretto e qualificato oppure quando il creatore/titolare ha acquisito una propria rilevante notorietà e fiducia nel pubblico.

Ultimo soggetto significativo nella filiera della diffusione degli NFT è l'utente/consumatore che acquisisce, di norma, il diritto di detenere, fruire e vendere il prodotto digitale irreversibilmente connesso all'NFT, ma la cui ampiezza del diritto è vincolato alle previsioni contrattuali stipulate tra il creatore/titolare e la piattaforma, ad esempio per quanto riguarda il diritto di fruirne in pubblico, di metterlo a disposizione (a titolo gratuito o oneroso) presso un museo o una galleria d'arte, di trarne copia etc.

Tra le obbligazioni che vengono indirettamente assunte dagli utenti/ consumatori vi è l'onere di corrispondere all'autore di opera artistica una *royalty*, di norma pari al 10% del valore del prezzo di acquisto, per ogni ulteriore cessione del prodotto digitale a cui l'NFT si riferisce, in virtù del fatto che nel codice informatico dello *smart contract* collegato alla piattaforma *blockchain* di norma viene previsto che ogni successivo trasferimento del prodotto digitale registrato dalla piattaforma dia luogo ad una erogazione economica a beneficio dell'originario autore.

È evidente che, in un mercato come quello degli NFT in inarrestabile ascesa e che presenta valori economici rilevanti, oltre ai presidi regolamentari che tutelano in caso di proposizione di token digitali come prodotti finanziari, occorre che sia rapidamente diffusa tra gli utenti/consumatori la consapevolezza che l'ampiezza dei diritti collegati ai prodotti digitali come gli NFT è disciplinata soltanto mediante pattuizioni contrattuali e perciò che la trasparenza, la piena comprensione e la garanzia rispetto alle condizioni negoziate tra creatore/titolare e piattaforma costituiscono il presupposto necessario per lo sviluppo del mercato in una prospettiva di lungo periodo.

Nel mercato si possono rilevare una pluralità di progetti che interessano mercati molto diversificati e prodotti con funzionalità molto variegate tanto da far sorgere il dubbio che talvolta l'utilizzo di un *non-fungible token* e della tecnologia *blockchain* non siano i più adeguati ed efficienti per l'obiettivo, ma siano funzionali ad attirare l'attenzione dei media e degli investitori.

Uno dei presupposti del successo degli NFT è la capacità di creare unicità o quantomeno scarsità dei beni digitali e di poterlo garantire in modo duraturo grazie all'utilizzo della tecnologia *blockchain*. Ma occorre essere consapevoli che, fintanto che la diffusione degli NFT viene veicolata dalle importanti piattaforme che stanno imponendo degli standard contrattuali e delle prassi commerciali fondate sui principi e sulle regole di altri ordinamenti, i rapporti contrattuali e le capacità di tutela degli interessi saranno in larga parte disciplinati sulla base di altri sistemi giuridici, ad eccezione della applicazione necessaria di alcuni plessi normativi, quali le eventuali regolamentazioni settoriali vigenti *ratione materiae* nonché il Codice del consumo nella misura in cui tali prodotti siano destinati ai consumatori italiani.

## 10. Natura giuridica degli NFT: diritto di proprietà, licenza d'uso o ricevuta dell'acquisto?

Numerose teorie si stanno affacciando in dottrina al fine di qualificare la natura e gli effetti giuridici riconosciuti agli NFT (38).

Una parte della dottrina, di matrice nordamericana, qualifica l'NFT come una "*digital personal property*" sostenendo che, sulla base di considerazioni giuridiche e sociologiche legate all'inarrestabile dilagare dell'ecosistema digitale e al crescente rapporto tra l'identità della persona e i beni anche nell'universo virtuale, a fronte dell'espansione delle licenze d'uso per la fruizione dei beni digitali, sarebbe necessario che gli atti dispositivi relativi agli NFT ricadessero invece nella disciplina applicabile ai trasferimenti di proprietà dei beni fisici poiché "*the economic reality of an NFT sale is that is the sale of personal property, not a lease, or other transaction designed to extend the control of the vendor over the buyer through the asset*" (39).

Al contrario un importante filone di matrice europea (40) si interroga sulla natura e sull'ampiezza dei diritti di proprietà intellettuale che possono essere ricollegati ad un NFT, sia con riferimento ai possibili limiti

(38) Per tutti v. Granieri, *Alcune considerazioni preliminari circa le forme di appartenenza dei non fungible tokens* in *Foro.it.* 2022, 3813 ss.; Hales, *Non-Fungible Tokens and Art that Lives on the Blockchain*, in <www.internetandtechnologylaw. com> del 22 febbraio 2021; Koonce-Sullivan, *What You Don't Know about NFT's Could hurt you: non-Fungible Tokens and the Truth About Digital Asset Ownership*, in <www.dwr.com/insights/2021/03>, marzo 2021.

(39) Fairfield, *Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property*, in *Indiana Law Journal*, SSRN, 7 aprile 2021.

(40) Caglayan Aksoy-Ozkan Uner, *NFT's and copyright: challenges and opportunities*, in *Journal of Intellectual Property Law and Practice*, 2021.

all'utilizzo del prodotto digitale sia in relazione al bene fisico che spesso, soprattutto nel mondo dell'arte, ha una forte connessione oggettiva con il bene digitale, ma al titolare del quale vengono riconosciuti numerosi e in parte diversi diritti.
Volendo invece seguire un ragionamento basato su un approccio fattuale possiamo provare a qualificare la natura giuridica dell'NFT sulla base delle seguenti considerazioni.
Innanzitutto, per motivazioni tecniche, l'NFT non incorpora il contenuto digitale che viene trasferito tra le parti, ma rappresenta soltanto una sequenza informatica sottoposta a un processo di *hashing* ed alcune proprietà algoritmiche del *token*. Questo certificato poi è connesso in modo univoco mediante un link ad un sito *off-chain* ove viene conservato il prodotto digitale oggetto della transazione; In secondo luogo, lo *smart contract* che opera sulla piattaforma *blockchain* si limita a dare esecuzione alle previsioni contrattuali disciplinate dalle parti con separati contratti stipulati in linguaggio naturale.
Sembra corretto concludere che l'NFT non incorpora alcun diritto connesso all'oggetto della transazione, ma risulta un titolo abilitativo che consente l'accesso al contenuto digitale.
Taluno (41) ha qualificato l'NFT come una "ricevuta digitale", ma questa definizione probabilmente non coglie compiutamente gli aspetti di innovazione e la garanzia di sicurezza che questo strumento tecnologico è attualmente in grado di offrire.
Forse, l'NFT può essere più adeguatamente qualificarsi come una "chiave digitale" che, grazie all'intelligenza informatica e ai protocolli di sicurezza applicati mediante la crittografia, può assicurare un accesso univoco e sicuro al contenuto digitale. Infatti, come una "chiave digitale" consente di accedere alla camera di albergo prenotata sulla base di un contratto stipulato in linguaggio naturale con il gestore della struttura ricettiva, così l'NFT consente a chi la detiene di essere identificato univocamente come l'avente diritto alla prestazione, ossia all'accesso e alla fruizione del contenuto digitale nei limiti previsti contrattualmente.
Conclusivamente, in assenza di una esplicita qualificazione giuridica, nel nostro ordinamento l'NFT si potrebbe qualificare come un titolo di credito atipico riconducibile alla categoria dei documenti di legittimazione disciplinati dall'art. 2002 c.c. che servono soltanto ad identificare l'avente diritto alla prestazione, mentre il vincolo contrattuale si è formato e resta disciplinato sulla base delle pattuizioni stipulate tra le parti in separati documenti (42). Parafrasando una celebre frase di L. Lessing, si potrebbe affermare che *NFT is not Law, it is just an electronic key*.

## 11. Funzione notarile e nuove tecnologie

Nel panorama normativo vigente, l'esigenza di garantire da un lato la legalità del procedimento di formazione del vincolo, e, dall'altro la posizione del terzo che verosimilmente agisce riponendo affidamento su quanto gli appare dall'analisi dell'economia reale (e non in considerazione di ciò che emerge dalla realtà digitale) non consente di sacrificare gli interessi di carattere pubblicistico ai quali rispondono sia l'intervento di un'autorità espressione del potere statuale, sia la gestione centralizzata dei registri immobiliari. Un de-potenziamento del ruolo del notaio non sembra quindi un obiettivo desiderabile (43).
In un recente convegno tenuto a Roma il 2 dicembre 2022, il notariato italiano ha formulato una interessante proposta in materia di opere d'arte (44).
Come è noto, in caso di vendita al pubblico, esposizione ai fini di commercio o intermediazione relative ad opere fisiche di pittura, di scultura, di grafica o oggetti di interesse storico o archeologico, l'art. 64 del Codice dei

(41) Guadamuz, *Can Copyright Teach Us Anything about NFTs?*, in <www.technollama.co.uk del 7 marzo 2021>.

(42) Pur potendo presentare – per il tramite della tecnologia *DLT* – elementi distintivi comuni, l'NFT non sembrerebbe riconducibile *tout court* né nell'ambito della categoria dei titoli di credito né in quella dei titoli di legittimazione o dei titoli impropri: ciò non tanto o non solo per la mancanza del documento, il quale in teoria potrebbe essere sostituito mediante l'utilizzazione di un altro veicolo, anche non cartolare, in grado di produrre la duplicità dei rapporti (cartolare e fondamentale), ma in ragione del rapporto obbligatorio che le medesime cripto-attività intendono veicolare e rappresentare. Volendo esemplificare, si potrebbe sostenere che l'emissione di un'azione sotto forma di cripto-attività non è riconducibile ad altro rapporto ad eccezione di quello mutuato nel titolo azionario digitale dal momento che la creazione delle azioni non avrebbe quale effetto quello di produrre un nuovo rapporto diverso ma riconducibile, in tutto o in parte, a quello costituito nel contratto di società; la rappresentazione in termini cartolari, contabili e, infine, digitali delle azioni non assumerebbe efficacia costitutiva ma eminentemente dichiarativa del rapporto fondamentale, per la circostanza che non sarebbe idonea a costituire una situazione giuridica distinta, analogamente a quanto accade mediante l'emissione della *chartula* per i titoli di credito. A supporto di questa argomentazione vi è la constatazione che i regimi cartolare, contabile e digitale intendono offrire soltanto differenti modalità di circolazione delle azioni e non legittimare l'esistenza stessa di un determinato rapporto sociale, originato dalla sottoscrizione del capitale sociale che conferisce lo status di socio, nonché i diritti, i poteri e le facoltà ad esso inerenti, indipendentemente dal sistema di gestione.

(43) Cfr. Alpini, *L'impatto delle nuove tecnologie sul diritto*, cit., 9, la quale rileva «la necessità di recuperare il senso della funzione notarile che risiede innanzitutto nella fiducia quale valore irrinunciabile in qualunque tipo di scambio. L'assenza di un soggetto responsabile, che oltre a verificare l'identità delle parti del contratto ne controlli anche la capacità e l'effettiva volontà, rappresenta un limite del sistema informatico».

(44) Gli Atti del convegno sono pubblicati in Gunnella (a cura di), *Notariato e nuove tecnologie a servizio del patrimonio artistico e museale. Realtà virtuale e garanzie*, *Biblioteca della Fondazione italiana del notariato*, Milano, 2024.

beni culturali e del paesaggio impone l'obbligo di consegnare all'acquirente la documentazione che ne attesti l'autenticità e la provenienza, o comunque, in assenza, impone una dichiarazione ove siano indicate le informazioni disponibili sull'autenticità e la provenienza (45).
Sul fronte pubblico l'Italia soffre di risorse talvolta insufficienti per la tutela e lo sviluppo del patrimonio artistico e culturale a fronte del valore strategico che questa risorsa rappresenta, e non ha ancora colto appieno il potenziale dato dalle nuove tecnologie digitali. Manca ad oggi in Italia un "Catasto" delle opere d'arte e non esiste alcuna modalità di certificazione "ufficiale" dell'autenticità di un'opera. Il notariato ha proposto la creazione di un registro (su base, inizialmente, volontaria) delle opere d'arte (nuovo Registro digitale dell'arte) che vede il punto nodale nella raccolta di dati "anagrafici" ed evidenze biometriche dell'opera (attributi e informazioni) stessa e, come suo risultato, una certificazione delle caratteristiche dell'opera – sulla base delle evidenze raccolte – e della relazione biunivoca con il suo autore (46).
Il problema dell'autenticità di un'opera d'arte (e della relativa certificazione) è infatti una questione fondamentale nell'ambito del mercato dell'arte, in quanto incide in maniera significativa sulla valutazione della stessa sia dal punto di vista artistico sia da un punto di vista economico.
La raccolta, archiviazione e, quindi, la conservazione delle evidenze documentali (pubbliche, private, umanistiche e tecnico-scientifiche ecc.) – una delle attività in cui si esplica la normale attività del notaio – permetterebbe la creazione di un inventario certificato delle opere stesse, generato ed alimentato da una parte terza fidata in collaborazione con i *players* del settore (archivi, fondazioni, gallerie ecc.), istituzionalmente deputata a farlo.
La registrazione può avvenire sia in registri centralizzati, la cui titolarità è definita da norme o accordi, che in sistemi gestiti da più utenti in modalità distribuita (quale una blockchain *permissioned* e federata). L'architettura decentralizzata è, probabilmente, non l'unica ma, forse, quella più idonea ad evitare DDOS (*distributed denial of service*), manomissioni o altre forme di "attacco informatico" in una materia così delicata e, allo stesso tempo, strategica.
Un simile registro potrebbe anche contribuire a risolvere il problema della contraffazione che coinvolge sia il segmento dell'arte contemporanea sia quello dei reperti archeologici.
Invece con riferimento agli NFT non vi è, allo stato dell'evoluzione tecnologica, una modalità per connettere in modo indissolubile l'identità del soggetto che afferma di essere il creatore dell'opera d'arte digitale alla quale si connette il *token*. Infatti la piattaforma *blockchain* può certificare tutti i passaggi di un NFT da quando è stato connesso al relativo *smart contract*, ma non può garantire tutto ciò che accade anteriormente al collegamento dei metadati con la piattaforma, ossia che il creatore dell'NFT sia anche l'autore dell'opera d'arte, così come che l'opera sia originale. Infatti, chiunque può creare con facilità su una qualsiasi piattaforma un NFT che sia connesso ad un contenuto di terzi ed affermare di esserne l'autore e quindi non vi può essere alcuna prova, certificato, parere o documentazione fotografica inserita nella piattaforma *blockchain* che possa indissolubilmente collegare il creatore dell'NFT all'autore dell'opera o certificare l'autenticità di un'opera.
Uno strumento per superare l'incertezza sull'identità dell'autore/titolare del contenuto e i connessi rischi contrattuali e di diritto d'autore, potrebbe essere rappresentato dall'affiancamento, esternamente all'ecosistema degli NFT, delle applicazioni di *Self Sovereign Identity* che utilizzano le chiavi di crittografia asimmetrica congiuntamente con le funzionalità della piattaforma *blockchain* al fine di creare delle identità digitali decentralizzate, certificate e sicure che possono essere controllate in modo unitario dal legittimo titolare rispetto alle diverse piattaforme e alle differenti richieste di informazioni personali (47).
Le problematiche appena esaminate relative alla fonte, all'ampiezza dei diritti connessi ad un NFT e alla loro tutelabilità non possono non incidere sulla completa affidabilità di uno degli elementi essenziali del successo mediatico ed economico degli NFT, ossia la garanzia della loro unicità, in merito alla quale attualmente la tecnologia che crea e abilita gli NFT non può offrire all'interno del suo ecosistema ulteriori certezze di "autenticità" rispetto a quanto è stato dichiarato e reso immutabile e

(45) La prassi ha poi introdotto forme più sofisticate che includono documentazioni fotografiche sottoscritte dall'autore, perizie sulla firma autografa dell'autore, pareri sull'autenticità rilasciati da esperti, descrizioni tecniche dell'opera sottoscritte dall'autore, da esperti o dal venditore, mappatura delle apparizioni in mostre e in cataloghi, che poi, in tempi più recenti, sono diventati parte di un pacchetto informativo sull'opera fisica certificato da una piattaforma *blockchain*.

(46) Apostolo, *La fiducia nel mondo dell'arte*, in *Infonews*, *Newsletter trimestrale di informazione di Notartel*, 1 marzo 2023. Id., *La dematerializzazione e la tokenizzazione di documentazione relativa ad opere d'arte e beni culturali*, in Gunnella (a cura di), *Notariato e nuove tecnologie a servizio del patrimonio artistico e museale*, cit., 47 ss.

(47) In generale sul tema della identità digitale v. Nastri, *Identità digitale e identità personale: un percorso di sintesi*, in *Il diritto nell'era digitale*, a cura di Giordano - Panzarola - Police - Preziosi - Proto, cit., 3 ss. In merito ai diversi profili della *Self Sovereign Identity* la letteratura è vasta: si rinvia, *ex multis*, Tobin - Reed, *The Inevitable Rise of Self-Sovereign Identity*, Sovrin Foundation, 2017; *Eidas Supported Self- Sovereign Identity* in <ec.europa.eu>; Muhle - Grune - Gayvoronskaya - Meinel, *A Survey on Essential Components of Self-sovereign Identity*, 17 luglio 2018, in <Argiv.org.>.

certificato mediante i programmi autoeseguibili stabiliti negli *smart contract* e nella piattaforma *blockchain*.
Perciò applicare i medesimi principi e cercare tutela con gli strumenti riconosciuti dal diritto d'autore nei confronti delle opere d'arte fisiche rispetto a quelle connesse ad un NFT senza discernere le sostanziali differenze tecnologiche e di tutelabilità dei diritti può condurre non soltanto ad investimenti ed aspettative di valore da parte del singolo utente/consumatore basate su una scarsa consapevolezza del rischio sotteso, ma anche ad un inevitabile effetto negativo sulla percezione di affidabilità dell'intero mercato degli NFT.
Una seconda proposta avanzata dal Notariato consiste nella creazione di un registro digitale degli investimenti a favore del patrimonio culturale ed artistico Italiano (musei, biblioteche, archivi, aree e parchi archeologici, complessi monumentali) attraverso la tokenizzazione del credito fiscale conseguente alle erogazioni liberali (48).
L'intervento del notaio nella tokenizzazione del credito:
- identifica il mecenate, verifica la correttezza della richiesta di sovvenzione di un'opera/attività;
- effettua le verifiche previste dalle normative e assicura il rispetto dei controlli antiriciclaggio;
- assicura la regolarità formale dell'erogazione per evitare futuri contenziosi;
- facilita le erogazioni da parte di soggetti stranieri.

Una volta tokenizzato il credito, in maniera certa e garantita dal notaio, questo potrebbe essere ceduto sia a banche sia ad altri soggetti privati avendo la possibilità di mantenere un tracciamento dell'effettivo titolare del credito. La cessione del credito potrebbe essere un utile volano per l'iniziativa dell'Art Bonus, in quanto esso diventerebbe maggiormente appetibile per i soggetti stranieri i quali – in mancanza di redditi in Italia – non avrebbero alcuna possibilità di beneficiare del credito d'imposta.

### 12. Tokenizzazione degli strumenti finanziari: tra semplificazione e sicurezza delle transazioni

Da qualche mese è in vigore in Italia il d.l. n. 25 del 17 marzo 2023 convertito con la legge 10 maggio 2023, n. 52 recante: «Disposizioni urgenti in materia di emissioni e circolazione di determinati strumenti finanziari in forma digitale e di semplificazione della sperimentazione FinTech» che introduce nel nostro ordinamento un innovativo sistema di digitalizzazione degli strumenti finanziari.
La previsione della emissione e circolazione di azioni ed altri strumenti finanziari attraverso la tecnologia basata su un registro distribuito e condiviso (DLT) è stata motivata dall'esigenza di evitare che gli operatori italiani si trovino in svantaggio competitivo rispetto ad altri operatori stabiliti in Stati membri. In realtà, il legislatore nazionale è andato oltre la prospettiva delineata nel Regolamento 2022/858. Quest'ultimo prefigurava un "regime pilota" da sperimentare nei vari ordinamenti nazionali entro predefiniti limiti quantitativi e un arco temporale triennale, all'esito del quale si sarebbe operata un'analisi dell'impatto in termini di costi e benefici per poi procedere ad eventuali correzioni di tiro. La disciplina interna ha una portata più ampia sia sul piano cronologico, non contemplando alcun limite temporale, sia nell'ambito applicativo: il nuovo sistema di tokenizzazione potrà essere adottato, in alternativa ai regimi tradizionali, per l'emissione e la circolazione di tutti i titoli azionari e obbligazionari di s.p.a., per i titoli di debito delle s.r.l. e per altri strumenti finanziari indicati nel decreto, tra i quali le azioni e quote degli organismi d'investimento collettivo.
Il Regolamento europeo, tra le altre cose, ha previsto la modifica della definizione di "strumento finanziario" di cui alla Direttiva MiFID II (Direttiva 2014/65/UE), per includere nella categoria degli strumenti finanziari anche "gli strumenti emessi mediante tecnologia a registro distribuito" (DLT) cioè la tecnologia che consente il funzionamento e l'uso dei registri distribuiti.
Pertanto, il decreto-legge come convertito ha introdotto innanzitutto nell'ordinamento nazionale la definizione di "strumenti finanziari digitali" intendendosi determinate categorie di strumenti finanziari che siano emessi su un registro per la circolazione digitale cioè un "*archivio di informazioni in cui sono registrate le operazioni e che è condiviso da una serie di nodi di rete DLT ed è sincronizzato tra di essi, mediante l'utilizzo di un meccanismo di consenso*" (definizione di "registro distribuito" di cui all'art. 2, punto 2 del Regolamento DLT) utilizzato per l'emissione di strumenti finanziari digitali.
Nel dettaglio, le categorie di strumenti finanziari che possono essere considerati digitali sono le azioni di società, le obbligazioni di società per azioni, i titoli di debito emessi dalle società a responsabilità limitata, gli ulteriori titoli di debito la cui emissione è consentita ai sensi dell'ordinamento italiano, nonché – elemento di novità apportata in sede di conversione – i titoli di debito regolati dal diritto italiano emessi da emittenti diversi dagli emittenti italiani, le ricevute di deposito relative ad obbligazioni e ad altri titoli di debito di emittenti non domiciliati emesse da emittenti italiani, gli strumenti del mercato monetario regolati dal diritto italiano e le azioni o quote di organismi di investimento collettivo del risparmio italiani.
Le disposizioni del decreto-legge come convertito riguardano quindi gli aspetti relativi alle emissioni e alla

(48) Art. 1 d.l. 31 maggio 2014, n. 83 convertito con l. 29 luglio 2014, n. 106 (c.d. Art bonus).

circolazione dei sopra richiamati strumenti finanziari digitali, tra cui, ad esempio:

- l'emissione e il trasferimento degli strumenti finanziari digitali, che deve avvenire mediante scritturazioni su un registro per la circolazione digitale;
- i requisiti dei registri per la circolazione digitale nonché gli effetti della scritturazione sui registri;
- l'individuazione dei responsabili dei registri e gli obblighi in capo a tali soggetti.

Inoltre, in sede di conversione, è stato introdotto un nuovo articolo relativo alla disciplina antiriciclaggio che prevede che i responsabili dei registri per la circolazione digitale siano soggetti obbligati alle disposizioni antiriciclaggio, rientrando nella categoria di "altri operatori non finanziari" ai sensi dell'articolo 3, comma 5, del d. l.vo n. 231/2007.

Il sistema di tecnologia a registro distribuito è destinato ad affiancarsi al regime tradizionale di emissione e circolazione non soltanto nell'ambito dei valori mobiliari, ai quali soltanto fa riferimento il pilot regime europeo, ma di ogni titolo emesso da s.p.a., quand'anche non qualificabile come strumento finanziario, oltre ai titoli di debito delle s.r.l.

Questa opzione estensiva – ed ancor più un sua eventuale dilatazione alle quote di s.r.l. – merita un supplemento di riflessione in considerazione di alcuni delicati problemi fattuali che la struttura DLT può determinare, primo tra tutti la stessa identificazione dell'azionista, in quanto la chiave di accesso al sistema blockchain non corrisponde necessariamente all'identità del soggetto che ne è titolare. Ma vi è di più: nel nuovo scenario potrebbero essere tokenizzati anche titoli non negoziabili per la presenza di limiti alla loro circolazione, con l'ulteriore delicato problema di verifica digitale del rispetto delle regole statutarie al trasferimento delle partecipazioni. Si tratta di problemi in larga misura inediti che spiegano l'indicazione del legislatore europeo di riferire il regime sperimentale ai soli valori mobiliari e che legittimano alcuni dubbi sulla scelta di chi quella indicazione ha disatteso.

Al di là di queste difficoltà tecniche, che rivestirebbero ben altro rilievo applicativo in ipotesi di ulteriore estensione del sistema DLT alle quote di s.r.l., soggette nella prassi statutaria a limiti o finanche divieti al trasferimento, istanze sovraordinate di ordine pubblico imporrebbero comunque di appurare che i soggetti chiamati a gestire i registri elettronici siano effettivamente in grado di mettere in atto processi di *whitelisting* degli investitori ed altri processi di validazione per identificare con precisione i titolari di token azionari, anche ai fini dell'antiriciclaggio e del *know your customer*.

Come ha ricordato Piergaetano Marchetti (49), il regolamento comunitario ha avuto cura di sottolineare l'esigenza di mitigare i rischi giuridici, sistemici e operativi insiti nella sperimentazione della tecnologia a registro distribuito nel settore in esame. Se per i valori mobiliari si impone in generale la predisposizione di presidi adeguati in punto di vigilanza sui soggetti chiamati a gestire i registri DLT, la questione risulta più delicata per azioni e quote che si collocano al di fuori della portata del regolamento europeo. In questo ambito si potrebbe riallineare il nostro ordinamento alle più caute indicazioni eurounitarie o, in alternativa, valorizzare il ruolo rivestito nel nostro ordinamento dal notariato.

L'inclusione del notaio nella catena di nodi *permissioned* è una soluzione realizzabile con una modifica alla legge notarile: un intervento di estrema semplicità, per il quale si potrebbe proporre una estensione ai trasferimenti di titoli tokenizzati delle regole alla base della piattaforma notarile per la costituzione della società *online* (50). In tal modo si coprirebbero i vuoti di tutela che potrebbero derivare anche dalla scarsa appetibilità del mercato delle partecipazioni di PMI da parte di altri gestori, legata a costi organizzativi, masse intermediate e rischi giuridici. Il notariato invece integrerebbe verticalmente le proprie funzioni con un nuovo servizio digitale a servizio delle attività che già è chiamato istituzionalmente a svolgere (51).

## 13. Il potere della tecnica e la funzione del diritto. Verso una regolazione partecipata

L'analisi che precede ha omesso, per ragioni di spazio, una disamina relativa agli ulteriori temi della disciplina fiscale applicabile al trasferimento degli NFT e dei diritti sui contenuti connessi così come un approfondimento relativo alle tematiche dell'applicazione della disciplina antiriciclaggio che, nella prassi, nell'ecosistema delle criptoattività viene interpretata in senso estensivo (52).

---

(49) Marchetti, *Fintech, il possibile ruolo dei notai nelle certificazioni*, *Sole 24 ore* del 3 aprile 2023, il quale ribadisce la perdurante necessità della figura del notaio al fine di garantire semplificazione, celerità e certezza rispetto ai dati riportati sui registri distribuiti, con particolare riferimento ai controlli antiriciclaggio e sui vincoli statutari.

(50) Mucciarelli, *La costituzione digitale di società nell'evoluzione del diritto societario europeo*, in *Intelligenza artificiale e diritto: una rivoluzione?*, a cura di Pajno - Donati - Perrucci, Bologna, 2022, vol. 3 371 ss.; Carioti, *La costituzione di srl on line :l'atto pubblico telematico (d.lgs.n.183/2021)*, in <Giustiziacivile.com> del 29 dicembre 2022.

(51) Abriani, *Un ruolo al notariato nei processi di digitalizzazione*, *Sole 24 ore* del 25 aprile 2023, 10.

(52) Si rinvia, in termini generali, alla definizione di valuta virtuale prevista nella V Direttiva Antiriciclaggio 2018/843 recepita nell'ordinamento italiano con il d.lgs. 4 ottobre 2019 n. 215 che ha modificato il d.lgs. 231/2007 introducendo all'art. 1, co. 2, lett. *qq*) la seguente definizione: «*La rappresentazione digitale di valore, non emessa né garantita da una banca*

In considerazione della tumultuosa crescita dell'utilizzo di NFT in diversi mercati, affidata finora interamente alla disciplina privatistica e ai rapporti negoziali tra i diversi attori del mercato, nonché della possibile parziale efficacia di un intervento del legislatore europeo o nazionale vista la molteplicità di funzioni per le quali può essere utilizzato lo strumento dell'NFT, occorre auspicare che la dinamica competitiva consenta di arrivare ad uno standard di settore che renda più chiaro e trasparente a tutti coloro che si affacciano all'utilizzo di NFT nei diversi mercati (e non solo ai *crypto addicted*), non soltanto quali siano i potenziali rischi connessi a un investimento in *Non-Fungible Token*, ma anche incrementi la consapevolezza di quali siano effettivamente le funzionalità, i limiti e i diritti connessi all'utilizzo di un NFT allo stato attuale dell'evoluzione della tecnologia.

Il tempo contemporaneo e la connessa rivoluzione tecnologica prodotta dalla digitalizzazione sembrano foriere di promesse ambigue per la nostra civiltà. La comunità scientifica appare profondamente divisa sull'impatto giuridico della nuova era digitale ed è obiettivamente difficile orientarsi rispetto ai benefici annunciati da questi nuovi scenari, anche se inquietanti ombre già si allungano sulle luci che ne hanno esaltato l'avvento.

Nella latitanza della politica spetta al diritto ricostituire un *nomos,* a partire dai grandi campi di frizione tra vecchio e nuovo, come la regolazione di *blockchain e* delle piattaforme digitali, ma si potrebbero aggiungere anche altri fronti, come l'antitrust o la proprietà intellettuale dei prodotti informatici.

Confrontarsi con questi nuovi fenomeni è complesso, poiché siamo al cospetto di tre tempi di evoluzione: quella tecnologica, rapidissima; quella legislativa; quella delle prassi applicative. Tre tempi di evoluzione non riducibili ad unità. A dispetto dell'asperità della sfida le considerazioni esposte in questo modesto contributo suggeriscono quale dovrebbe essere, ad avviso di chi scrive, l'approccio tecnicamente più adeguato al tema delle nuove tecnologie e dei *big data,* intorno a cui stiamo costruendo le basi della nostra convivenza futura.

Non ci si dovrebbe ispirare a un *laissez-faire* tecnologico, né a un luddismo di retroguardia.

Sembra invece necessario operare, in tutte le sedi, perché i processi in atto, i quali sono destinati a regolare segmenti crescenti della vita sociale dell'uomo, siano sottoposti a una logica di controllo democratico, che assicuri un adeguato bilanciamento tra la 'funzionalità tecnologica' e la desiderabilità sociale degli scopi perseguiti, e rispetto alla quale la mediazione giuridica svolge un ruolo centrale. Si dovrebbe cioè lavorare all'adozione di strumenti regolatori e di governo, preordinati ad evitare che la saldatura tra potere economico e potere tecnologico produca una società della sorveglianza (53) e della discriminazione, in cui tutti siano profilati, segmentati in gruppi e resi destinatari di effetti giuridici o sociali in funzione dell'assetto di potere esistente.

Se ciò implica rigettare tanto un modello sregolato di "capitalismo della sorveglianza", il quale finirebbe per inchiodare la società alle sue iniquità e ai suoi pregiudizi, codificandoli nel linguaggio informatico, è necessario stabilire quale tecnica di intervento sia più adeguata al controllo dei trattamenti algoritmici.

La logica del divieto *tout court* non sembra percorribile, per il semplice fatto che l'innovazione tecnologica, se attentamente monitorata, può apportare notevoli benefici sociali, creando le premesse per una società più aperta ed inclusiva. Del pari, sembra utopistico pensare a un meccanismo di co-decisione pubblico-privato o a un'approvazione preventiva da parte di appositi enti pubblici degli algoritmi utilizzabili anche da soggetti privati. La strada più proficua appare quella dell'intervento a geometria variabile, composto cioè da forme più *soft* di incentivazione all'adozione di tecnologie e prassi organizzative *rights compliant* e strumenti più incisivi con funzione prettamente regolamentare (come nel caso dei limiti sostanziali posti dalla normativa anti-riciclaggio), i quali dovrebbero poi ricadere a cascata sulla fase della programmazione delle piattaforme, incentivando in ultimo una sorta di *legality by design*. Appare chiara, infatti, l'esigenza di fondo di garantire "certezze" relazionali per la collettività (informatica e non) che assumono un rilievo decisivo nella regolazione delle attività economiche. Questa operazione non è riducibile "all'attività ordinativa" dei pubblici poteri così come formulata da Giannini (54) alla metà degli anni Novanta del secolo scorso. Nella DLT e nella blockchain le regole sono incorporate nella tecnologia. Lo smart contract può orientare flussi economici, comprimere diritti fondamentali, ecc. È quindi impossibile per l'autorità di vigilanza o di regolazione intervenire ex post, imponendo non solo obblighi

*centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente».* Nell'implementazione della citata Direttiva nell'ordinamento italiano è stata adottata una definizione estensiva di moneta virtuale nonché di prestatori di servizi di valuta virtuale perciò i servizi funzionali all'emissione, offerta, trasferimento e negoziazione degli NFT potrebbero ricadere nel perimetro di applicazione della disciplina antiriciclaggio, sebbene si ritenga ragionevole una preventiva analisi caso per caso delle caratteristiche degli NFT in esame. Per chi voglia approfondire mi permetto di rinviare a Palazzo, *Blockchain e cripto-attività*, in *Il diritto nell'era digitale*, a cura di Giordano et al., cit., 211 ss.

(53) Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era di nuovi poteri*, Roma, 2020; Mannoni, *Millenarismo 2.0. Il diritto al cospetto della nuova era digitale,* Napoli, 2016.

(54) Giannini, *Diritto pubblico dell'economia*, Bologna, 1995, 47 ss.

di trasparenza e non discriminazione, ma anche requisiti tecnici che garantiscano un livello minimo di diritti e tutele previsti dall'ordinamento. Occorre pertanto che le autorità intervengano sin dall'inizio, cooperando con gli operatori, consentendo lo sviluppo della tecnologia secondo condizioni e requisiti minimi condivisi, conformi e coerenti con il welfare che corrisponde alla tradizione giuridica che s'intende difendere.
Questa procedura regolatoria viene definita in dottrina 'regolazione partecipata' (55) per differenziarla dalle altre forme di collaborazione tra autorità e mercato, che si estrinsecano ad esempio nelle procedure di consultazione sui provvedimenti delle autorità, o nella definizione degli impegni comportamentali o strutturali delle imprese in posizione dominante (diritto della concorrenza) o detentrici di una posizione di mercato significativa (regolazione delle comunicazioni elettroniche).
In tale prospettiva il ruolo del notaio, quale fattore di realizzazione dell'ordine sociale in attuazione dei principi costituzionali, lungi dall'essere superato appare ancora attuale: la dematerializzazione dei documenti non può che aumentare il primato dell'atto pubblico notarile, sia pure digitale, rispetto ai documenti prodotti dai privati, poiché essa richiede certezze documentali ancora maggiori di quelle richieste nella passate stagioni della società industriale (56). Nella prospettiva, appunto, di una regolazione partecipata.

(55) Goes, *The Interblockchain Communication Protocol: An Overview* (2020), eprint arXiv:2006.15918

(56) Ho sviluppato questo aspetto in Palazzo, *Il ruolo del notaio nel tempo della postverità*, in <https//biblioteca fondazionenotariato.it/art/ruolo-del-notaio-tempo-postverità.html> e in Id., *Il notaio nella stagione dei documenti digitali*, in *Vita not.*, 2017, 1285 ss.

# Le Smart City. Sostenibilità sociale ed ESG

**di Fortunato Costantino**

**Sommario:** 1. Premessa metodologica e inquadramento sistematico. – 2. La questione definitoria. Ricognizione in negativo degli ambiti di rilevanza della *smartness* della città. – 3. Smart City ed approccio multidisciplinare. Il focus sulla sostenibilità sociale quale ambito di possibile rilevanza specifica del paradigma della Smart City in relazione agli SDGs e alla luce dei nuovi indici di rilevazione del benessere collettivo. – 4. Il rapporto tra smartness (ITC driven) e sostenibilità sociale. La aporia definitoria del concetto di sostenibilità sociale e il riflesso sulla difficoltà di una elencazione esaustiva delle dimensioni della sostenibilità sociale e dei suoi indicatori. – 5. Conclusioni. Dalla "Smart City" alla "Social Sustainable Smart City". Una prospettiva costituzionalmente orientata.

L'autore si propone di svolgere una ricognizione sistematica degli ambiti di rilevanza della smartness della città, cercando di privilegiare un approccio multidisciplinare il cui traino è rappresentato da un ripensamento complessivo delle scelte strategiche della politica nel settore dei servizi essenziali alla persona, del welfare sociale e di equo accesso alle risorse di base oltre che della stessa concezione del benessere sociale e collettivo. L'autore in particolare modo definendo la Smart City per sottrazione di ciò che essa non è o non è soltanto ( non è soltanto una città digitalizzata né una città green) cerca di orientare l'approccio ricognitivo prediligendo un recupero di coerenza della definizione di Smart City alla luce della rilevanza degli obiettivi di sostenibilità, sociale in particolare prima ancora che economica ed ambientale, nell'ottica della fondazione e consolidamento di un modello di vivibilità urbana all'altezza delle complesse sfide conseguenti ai processi di metropolizzazione in atto che conduranno nel 2050 circa il 70% della popolazione terrestre a vivere in città o aree metropolitane. Un modello che intende la città come spazio/luogo oggetto di diritti di cittadinanza e allo stesso tempo come complesso organizzato degli strumenti e delle dotazioni per l'esercizio attivo di questi diritti, coadiuvato dalle infrastrutture tecnologiche e digitali. Un vero e proprio diritto alla città socialmente sostenibile, in sintesi. Una direzione questa che secondo l'Autore appare coerente con il paragrafo 11 della New Urban Agenda delle Nazioni Unite nella parte in cui afferma in maniera programmatica il «diritto alla città giusta, inclusiva, sicura, sana, accessibile, resiliente e sostenibile. Ma che soprattutto appare coerente con l'Agenda 2030 che nel nutrito elenco dei 17 obiettivi di sviluppo sostenibile per migliorare lo sviluppo dell'umanità, dedica il "goal 11" proprio a "Città e comunità sostenibili" con la finalità di "Rendere le città e gli insediamenti umani inclusivi, sicuri, duraturi e sostenibili». L'Autore conclude la sua analisi proponendo un approccio costituzionalmente orientato alla Smart City sul presupposto che la sostenibilità e per essa i fattori ESG – a cui la città intelligente non può sottrarsi – rappresentano una essenziale modalità applicativa del principio-dovere di solidarietà costituzionale in forza del quale lo Stato e per esso gli Enti territoriali secondo differenti livelli di partecipazione – sono chiamati ad attuare e dar conto dei diversi valori costituzionali riconducibili al benessere collettivo, richiamando a tal fine gli articoli della Costituzione: 9, comma 3 che assegna alla Repubblica, tra l'altro, il compito di tutelare «l'ambiente, la biodiversità e gli ecosistemi, anche nell'interesse delle future generazioni», l'art. 41 per il quale l'iniziativa economica privata non può svolgersi in modo da recare danno, oltre che alla sicurezza, alla libertà, alla dignità umana, alla salute e all'ambiente, ma soprattutto l'art. 2 che riconosce e garantisce diritti inviolabili dell'Uomo non solo come singolo ma anche nelle formazioni sociali ove si svolge la personalità dell'individuo, in adempimento dei doveri inderogabili di solidarietà politica, economica e sociale.

*The Author proposes to carry out a systematic review of the areas of conceptual relevance of the "smartness" of the city, seeking to favor a multidisciplinary approach whose driving force is represented by an overall rethinking of the conception of social and collective welfare. The Author particularly by defining the Smart City by subtraction of what it is not or is not only ( it is not only a digitized city nor a green city) intends to recover a proper consistency of the definition of Smart City in the light of the implementation of the goals of sustainability, social ones in particular before economic and environmental ones, with a view to the foundation and consolidation of a model of urban livability that is up to the complex challenges resulting from the ongoing processes of metropolization that will lead in 2050 to about 70 percent of the earth's population living in cities or metropolitan areas. A model that intends the city as a space/place subject to citizenship rights and at the same time as an organized complex of tools and endowments for the active exercise of these rights, assisted by technological and digital infrastructure. A perfect right to the "socially sustainable city", in short. This is a direction that, according to the Author, appears consistent with paragraph 11 of the United Nations' New Urban Agenda which programmatically affirms the "right to the city' just, inclusive, safe, healthy, accessible, resilient and sustainable. More importantly, it appears consistent with the 2030 Agenda, which in its extensive list of 17 Sustainable Development Goals to improve human development, dedicates the "Goal 11" precisely to "Sustainable Cities and Communities" with the aim of "Making cities inclusive, safe, durable and sustainable." The Author concludes his analysis by proposing a constitutionally oriented approach to the Smart City on the assumption that sustainability and for it the ESG factors-which the smart city cannot evade-represents an essential mode of application of the principle-duty of constitutional solidarity by virtue of which the State and for it the territorial bodies according to different levels of administrative participation-are called upon to implement and account for the constitutional values traceable to the collective well-being, recalling for this purpose the articles of the Constitution: 9, paragraph 3 which assigns to the Republic, among other things, the task of protecting "the environment, biodiversity and ecosystems, also in the interest of future generations," Art. 41 for which private economic initiative cannot be carried out in such a way as to cause damage not only to security, freedom, human dignity, health and the environment, but above all Article 2, which recognizes and guarantees the inviolable rights of Man not only as an individual but also in the social formations where the personality of the individual takes place, in fulfillment of the inalienable duties of political, economic and social solidarity.*

(*) Si tratta, con alcuni ampliamenti, di un capitolo del volume Cassano - Costantino - Tripodi (a cura di), *Smart City. Innovazione, impatto sociale, sostenibilità ambientale, profili giuridici*, Pisa, 2024.

## 1. Premessa metodologica e inquadramento sistematico

Nella linguistica, i cd. "prestiti di lusso" sono termini di cui esiste già un perfetto equivalente in italiano, o che si potrebbe facilmente trovare, ma che vengono impiegati con una evidente connotazione stilistica per snobismo, pigrizia o ignoranza, nella convinzione che la lingua da cui sono per l'appunto presi in prestito, per lo più quella inglese, sia di per sé più autorevole o espressiva (1), e così ponendo in essere non un arricchimento dell'italiano ma un fenomeno sottrattivo che lo depaupera.

Contrariamente ai cd. prestiti di necessità, non evitabili essendo il termine straniero (es. *patata*, *caffè*, *sauna*, *canoa*, *cacao*, *juke-box*) l'unico termine possibile per definire o designare la peculiarità di un oggetto, un'idea, un sentimento, un'azione o un fatto, i prestiti di lusso sono espressione di fenomeni di esotismo o forestierismo evitabili, teoricamente superflui in quanto esiste già nella lingua madre un termine col medesimo significato.

Alla classe dei prestiti di lusso appartiene indubbiamente il termine Smart (2). E tuttavia pur potendo utilizzare l'espressione Città Intelligente per indicare una specifica modalità di organizzazione socio-territoriale, politica ed economica della città contemporanea capace, attraverso il ricorso alle nuove tecnologie, di attivare processi di semplificazione e di inclusione tra i cittadini, le istituzioni e le imprese, continueremo ad usare nello sviluppo del presente contributo il termine Smart City per pura convenienza onomasiologica, in ragione della brevità e della capacità fono-espressiva del lemma e della sua connotazione stilistica ormai diffusa nell'uso comune a livello mondiale.

Non dimenticando però che di per sé il termine Smart non ama puntuali attribuzioni di significato e appare fortemente condizionato dal contesto di riferimento, culturale economico e sociale, in cui è inglobato.

Il termine "Smart", in effetti, con buona pace dei puristi della lingua, complici l'avvento delle tecnologie intelligenti e dell'era del digitale, è diventato uno dei termini anglosassoni più presenti e abusati nel nostro quotidiano con una portata di possibili significati che si rivela estremamente cangiante e quanto mai evanescente, con un inevitabile effetto di polisemia e quindi di incapacità definitoria specifica (3).

Ma le parole sono importanti, la scelta in sé delle parole è importante, perché è *nelle* e *attraverso* le parole che in un dato momento storico e sociale si definiscono le interazioni qualificate tra individui e tra sistemi semplici e complessi, si attribuiscono ruoli e compiti, si articolano strutture culturali e valoriali identitarie, facendo esistere le cose in un modo piuttosto che in un altro. Lo dicevano filosofi e poeti come Heidegger, Wittgenstein, Pierce che nelle loro riflessioni sulla struttura e funzione del linguaggio in rapporto all'Uomo hanno mostrato come nelle parole si origina e si compie la ricerca e la creazione di noi stessi, degli altri, delle cose e del mondo (4).

Con questa presa di coscienza, va attentamente quindi considerato che la vocazione del termine Smart ad essere tra l'altro un iperonimo (5) polisemico, anche se ad una superficiale valutazione può apparire di portata neutra, in realtà è in grado di giocare un ruolo assolutamente condizionante la riflessione dottrinale sulla Smart City, proprio perché la sua ampiezza e genericità di significato rende possibile un approccio di studio trasversale a numerosi ambiti disciplinari (urbanistica, sociologia, informatica, ITC, scienza dell'amministrazione, economia, diritto, filosofia) determinando una eterogenea e variegata produzione bibliografica a livello

(1) Gli esempi sono infiniti e una gran parte di essi riguardano il mondo del lavoro con una peculiarità che è tutta italiana non osservandosi la stessa tendenza in altri paesi europei più inclini ad adoperare la propria lingua locale di appartenenza: *leader, workforce solutions, full time equivalent, business, brand, talent shortage, cyber security, Job title, Industry o Skills, work-life balance, retention, attraction, value chain, prize-money, user friendly e eco friendly, upstream supplier*, etc.

(2) Se nell'era predigitale il termine "smart" alludeva per lo più ad una condizione di prontezza di spirito e di intelletto, nel corso dell'ultimo decennio con il consolidarsi del capitalismo consumeristico a trazione tecnologica, l'uso del termine smart è diventato una sorta di automatismo lessicale per definire particolari categorie di prodotti tecnologici interattivi capaci di connettersi con altri utenti ed altri dispositivi smart con un certo grado di autonomia e "intelligenza" operativa, come ad esempio gli smart-phone, le smart-tv, gli smart-glass e gli smart-watch. Per ulteriori approfondimenti cfr. TRIPODI, *Le prospettive potenziali della smart city "evoluta": la digital twin city*, in questa ***Rivista***, 2024, 23 ss.

(3) Recentemente anche nell'ambito delle politiche di gestione manageriale dell'organizzazione del lavoro il termine ha trovato la sua utile collocazione, definendosi smart working una modalità alternativa della prestazione di lavoro subordinato, più flessibile e agile, non vincolata ad un luogo fisico prefissato ed alla misurazione del tempo della prestazione e quindi in grado di favorire un "intelligente" punto di incontro tra bisogni aziendali ed esigenze personali del prestatore di lavoro (cd. work-life balance). Va precisato tuttavia che il mondo anglosassone non associa alcun specifico significato al concetto di Smart working, anzi a volte sollevando un dubbio sul senso proprio dell'espressione. Non è un caso del resto che la Legge 22 maggio 2017, n. 81 recante "Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato", nessun riferimento faccia allo Smart working, essendo invece l'art. 18 più italicamente rubricato "Lavoro Agile".

(4) DI MARTINO, *Segno, gesto, parola, Da Heidegger a Mead e Merlau-Ponty*, Pisa, 2005.

(5) Secondo la definizione rinvenibile in Treccani, in linguistica, il termine "iperonimo" indica un'unità lessicale di significato più generico ed esteso rispetto ad una o più altre unità lessicali che sono in essa incluse (per es., fiore è iperonimo, ossia «superordinato», rispetto a rosa, viola, garofano); è quindi l'inverso di iponimo e corrisponde a quello che da altri linguisti è talora chiamato arcilessema o archilessema.

internazionale che a sua volta ha generato uno specifico campo di ricerca intersettoriale (6).
Tornando all'ambito di trattazione nel presente saggio, l'indagine che in questa sede si cercherà di sviluppare si pone l'obiettivo di fornire una risposta critica al quesito su cosa sia una Smart City e se possa realmente discutersi di una Smart City intesa quale comunità urbana intelligente con al centro una "macchina-cervello" in grado di gestire in autonomia perfetta, per il tramite di infrastrutture digitali e tecnologiche in continua evoluzione e dei sistemi di AI, ogni aspetto della vita cittadina secondo logiche preordinate di efficienza e ottimizzazione. O se piuttosto non debba guardarsi alla Smart City, e tale conclusione cercheremo di argomentare, come un modello di città costituzionalmente conformato e il risultato specifico di scelte politiche dei decisori pubblici, a livello sia locale sia sovranazionale apertamente mirate a rifondare il sistema socio-economico delle città facendo leva su una nuova concezione di benessere umano, il più possibile tarato sulla specificità e diversità dei bisogni espressi in una data area urbana.
Il che implicitamente equivale a dire che non esiste un modello ever-green di Smart City applicabile indistintamente a prescindere dalle condizioni sito specifiche e che non possono darsi Smart City prescindendo da un indirizzo strategico di politiche pubbliche intelligenti tese a rendere sostenibile la fruizione del contesto urbano e l'accesso efficiente alle sue risorse limitate, con un immediato vantaggio per cittadini e del sistema impresa locale, pubblico e privato, in attuazione degli obiettivi di sviluppo sostenibile dell'Agenda 2030 dell'ONU (7).
La Smart City dunque come un nuovo modello di politica sociale in grado di evitare l'appiattimento della dimensione poli-valoriale dell'esistenza personale alla mono-dimensionalità della quantificazione della convenienza economica, attraverso l'incardinamento di obiettivi di sostenibilità, coesione e inclusione sociale, partecipazione riflessiva/attiva, vita quotidiana e empowerment.
Un paradigma evoluto capace di determinare un reale ripensamento del sistema sociale, economico e produttivo in armonia con il principio dello sviluppo sostenibile e della tutela dei diritti fondamentali del cittadino e dell'individuo, attraverso i) da un lato investimenti mirati in grado di favorire soluzioni energetiche, edilizie, ambientali, di gestione dei servizi essenziali, integrate le une con le altre, innovative ed inclusive e ii) dall'altro lato, attraverso il ricorso all'automazione e all'impiego dei sistemi e delle infrastrutture ITC e quindi delle nuove tecnologie digitali, non solo per migliorare la logistica, il traffico urbano, la qualità dei servizi pubblici essenziali e la mobilità degli abitanti e il loro accesso *attivo e partecipato* alla vita della città stessa ma anche per assicurare una puntuale e funzionale gestione, monitoraggio, analisi statistica ed elaborazione delle innumerabili informazioni proprie del capitale umano rappresentato dalla miriade di individui destinatari delle scelte dei decisori pubblici, anche in ottica di assesment continuo e miglioramento nelle dinamiche di soddisfazione degli obiettivi di sostenibilità. Informazioni cosi capillari ed estremamente significanti dal punto di vista del "valore" e del "potere politico" generato che il loro insieme, potenziato e sofisticato dalla elaborazione tramite l'uso dei sistemi ITC, rappresenta a sua volta una sorta di *intelligenza data driven* (8) o di intelligenza collettiva guidata da livelli accresciuti di interazione sociale (9).
Indubbiamente, almeno secondo gli insegnamenti di Tönnies, Durkheim, Weber, Simmel e in particolare della cd. Scuola di Chicago (10), la città in quanto atomo privilegiato della sociologia e laboratorio esclusivo per l'analisi delle dinamiche trasmutazionali del tessuto sociale, dello spazio pubblico e degli aspetti socio-territoriali, costituisce un ambito elettivo per lo studio degli impatti delle politiche di sviluppo sostenibile, tenuto conto che i Comuni e ancor di più le Città Metropolitane, costituiscono gli enti territoriali di governo più vicini alle esigenze ed ai bisogni di una collettività locale ed essendo, almeno in astratto, più idonei a provvedere al relativo soddisfacimento in ragione della loro autonomia normativa, amministrativa e finanziaria secondo i principi fissati dalla Costituzione italiana, dalla Carta dei Diritti Fondamentali dell'Unione Europea, dalla Dichiarazione Universale dei Diritti dell'Uomo, dalla Carta Europea delle autonomie locali.
In questa prospettiva si innesta poi lo sforzo di comprendere se la *smartness* tecnologica e digitale della città

(6) Komninos - Mora, *Exploring the Big Picture of Smart City Research*, Scienze Regionali, 2018.

(7) L'Agenda 2030 per lo Sviluppo Sostenibile è un programma d'azione per le persone, il pianeta e la prosperità sottoscritto nel settembre 2015 dai governi dei 193 Paesi membri dell'ONU. Essa ingloba 17 Obiettivi per lo Sviluppo Sostenibile – *Sustainable Development Goals*, SDGs – in un grande programma d'azione per un totale di 169 'target' o traguardi.

(8) Komninos - Mora, *Exploring the Big Pictuure of Smart City Research*. Scienze Regionali, 2018.

(9) Levy, *L'intelligenza collettiva. Per un'antropologia del cyberspazio*. Milano, 1996.

(10) Conosciuta anche come Scuola dell'ecologia sociale urbana, la scuola di Chicago rappresenta una delle espressioni più autorevoli della sociologia intesa come metodo di analisi e ricerca sul campo attraverso l'osservazione dei fenomeni sociali nel loro ambiente naturale con il fine di applicare le conoscenze prodotte alla riorganizzazione e al controllo dei cosiddetti *Social Problem*. È grazie alla Scuola di Chicago e alla pubblicazione del saggio La Città nel 1925, composto dai sociologi Ernest Burgess, Robert Ezra Park e Roderick McKenzie che la sociologia urbana si affermò come scienza sociale autonoma.

sia un fattore generativo in sé di sostenibilità sociale e di benessere umano o piuttosto un mero fattore abilitante e "di supporto" alle strategie di sostenibilità sociale, non imprescindibile né determinante.
Proporremo infine una più adatta e appropriata definizione di tale nuovo paradigma di città, in cui la smartness affrancata da un esclusivo orientamento di matrice tecnologica trovi un aggancio qualificato nel paradigma dello sviluppo socialmente sostenibile delle politiche pubbliche nel rapporto con la cura degli interessi degli stakeholders rilevanti, evolvendo il paradigma della Smart City a quello della Social Sustainable Smart City in una prospettiva ermeneutica costituzionalmente orientata dal dovere di solidarietà sociale e dal principio di utilità sociale.
Ma avvertendo sin d'ora che proprio il paradigma della sostenibilità porrà il dubbio (non risolvibile per principio originandosi e muovendosi esso nello spinoso agone del confronto tra Etica e Tecnologia) se l'automazione crescente introdotta nel contesto urbano attraverso le infrastrutture ITC, possa univocamente rappresentare un elemento certo di inclusione, di partecipazione democratica ed elevazione della qualità della vita dei cittadini o se al contrario non rechi con se il rischio di fenomeni di tecnocrazia e derive di controllo totalitario sulle masse, in danno delle libertà fondamentali dell'individuo e con effetti di esclusione e discriminazione sociale (11) indotti dal conflitto tra coloro che detengono il capitale economico (i mezzi, gli strumenti) per accedere alle tecnologie e coloro che invece sono privati dall'usufruirne e ancora fra chi "possiede" e chi "non possiede" le tecnologie (12).
Un dubbio più che legittimo e per certi versi doveroso che ha spinto autori incisivi come Marcuse (13) a ritenere, già diversi decenni fa e con assoluta lungimiranza, che la tecnologia abbia una sua intima vocazione a determinare nuove forme di controllo sociale e che la società tecnologica costituisca un perfetto sistema di dominio in grado di permeare ogni aspetto della esistenza dell'individuo sin dal momento in cui le tecniche sono concepite ed elaborate di modo che "*una confortevole, levigata, ragionevole, democratica non-libertà prevale nella civiltà industriale avanzata, segno di progresso tecnico*".
O ancora, più recentemente autori come la Sassen (14) che equipara la città contemporanea ad una "lente" attraverso la quale osservare e analizzare i mutamenti dei sistemi presenti per mano delle tecnologie di massa prima e digitali poi che modificano le pratiche e i comportamenti degli individui, l'intersoggettività della vita quotidiana, il rapporto tra pubblico e privato, tra *elites* e masse, aprendo la strada a nuove forme di esclusione e di brutalità sociale attraverso un inasprimento delle asimmetrie nella distribuzione dei redditi e della ricchezza guidato dal *digital divide* nelle sue varie declinazioni in rapporto a differenti clusters: i soggetti anziani (cd. "digital divide intergenerazionale"), le donne non occupate o in particolari condizioni (cd. "digital divide di genere"), gli immigrati (cd. "digital divide linguistico-culturale"), le persone con disabilità, le persone detenute e in generale coloro che, per insufficienti livelli di reddito, o per bassi livelli di scolarizzazione e di istruzione, non sono in grado di utilizzare gli strumenti informatici, patendo una grave discriminazione sul piano dell'uguaglianza dei diritti della società digitale esercitabili online e conseguentemente uno svantaggio specifico di tipo socio-economico e culturale.

## 2. La questione definitoria. Ricognizione in negativo degli ambiti di rilevanza della *smartness* della città

Il termine Smart City viene usato per la prima volta all'inizio degli anni '90 in una pubblicazione collettanea dal titolo "*The Technopolis Phenomenon: Smart Cities, Fast Systems, Global Networks*" (15) in cui viene presentata la prospettiva di una *techno-polis* intelligente in grado di legare la tecnologia allo sviluppo di iniziative efficaci del settore pubblico e privato con l'obiettivo di creare città intelligenti e reti globali per adiuvare la crescita economica, la diversificazione e la competitività globale.
Contemporaneamente, l'uso del termine Smart connota il nuovo approccio lessicale e concettuale attraverso cui le compagnie informatiche americane provano in maniera roboante e altisonante a descrivere le nuove tecnologie ITC quale strumento e fine privilegiato per rispondere alle problematiche delle grandi metropoli: dalla gestione del traffico e dei trasporti allo smaltimento dei rifiuti, dall'efficienza delle reti di distribuzione di energia e di acqua alla sicurezza e alla salute dei cittadini.

(11) Pettirossi, *Smart City: la Città autonoma*, in *Rivista Trimestrale di Scienza dell'Amministrazione*, n. 3/2020.

(12) Sennett, *Costruire e abitare. Etica per la città*, Milano, 2018

(13) Marcuse. *L'uomo a una dimensione. L'ideologia della società industriale avanzata*, Torino, 1967.

(14) Sassen, *Espulsioni*. Bologna, 2015: "è difficile spiegare come queste capacità (ndr. tecniche e digitali) che sarebbero dovute servire a sviluppare gli aspetti sociali, ad ampliare e rafforzare il benessere della società, per il quale è determinante il rispetto della biosfera, troppo spesso invece siano servite a smembrare la realtà sociale per mezzo di una diseguaglianza estrema, a vanificare gran parte della vita promessa alla classe media dalla democrazia liberale, a espellere non soltanto le fasce povere e vulnerabili dalla loro terra, dai posti di lavoro, dalle case, ma persino parti di biosfera dal loro spazio vitale".

(15) Gibson - Kozmetsky - Smilor, *The Technopolis Phenomenon: Smart Cities, Fast Systems, Global Networks*, Boston, 1992

Dal punto di vista delle nuove strategie di progettazione urbana invece il concetto di "Smart City" nasce nel 2009 a Rio de Janeiro, con la presentazione del primo piano urbanistico a livello mondiale incentrato sul ricorso alla innovazione tecnologica per la gestione dei rifiuti e degli sprechi al fine di migliorare la qualità della vita nella città.
Nel 2014, poi, con l'organizzazione dell'*Intelligent Community Forum* svoltosi a New York, si iniziano a definire quelli che sono i criteri per poter considerare una città come intelligente, ovvero il miglioramento della qualità della vita attraverso la sostenibilità, il risparmio dovuto all'utilizzo dell'energia rinnovabile, l'inclusività, la partecipazione attiva e, in generale, l'utilizzo dei mezzi tecnologici per poter rendere più agile la vita dei cittadini.
Parallelamente, tenuto conto della innegabile contiguità delle città alle istanze di trasformazione sostenibile del contesto cittadino il paradigma della Smart City, che tuttavia ancora oggi non trova espressa definizione e tipizzazione nei testi legislativi, è prepotentemente entrato a far parte del lessico comune delle organizzazioni politiche e dei legislatori nazionali e sovranazionali.
Un percorso progressivo che prende le mosse dalla Carta di Lipsia del 2007, documento sullo sviluppo sostenibile delle città e sull'incentivazione di politiche urbane integrate, per poi perfezionarsi con la strategia europea "*Europa 2020*" per la rigenerazione urbana attraverso una economia "intelligente", "sostenibile" e "inclusiva" per conseguire elevati livelli di occupazione, produttività e coesione sociale a cui si affiancano ulteriori obiettivi di sviluppo sostenibile e in particolare quelli più recentemente contenuti nell'Agenda territoriale dell'Unione europea 2030 (16), come la sostenibilità dello sviluppo dei territori urbani e la progressiva riduzione del consumo del suolo, definendo il quadro per una pianificazione spaziale in grado di affrontare le sfide di sviluppo sostenibile in tutti i territori dell'Unione e di ridurre le disparità tra regioni.
Va precisato che l'UE non ha una competenza *ratione materiae* in tema di Smart City, e di conseguenza gli interventi europei consistono o in incentivi e finanziamenti collegati alla realizzazione di programmi settoriali (città, ambiente, energia, trasporti, ecc.) oppure in iniziative specifiche con riferimento al partenariato pubblico-privato come ad esempio l'*European Innovation Partnership on Smart cities and Communities* (17), disciplinati da comunicazioni e da atti di *soft law* non giuridicamente vincolanti e con il fine di orientare gli enti territoriali e gli operatori economici ad adottare soluzioni smart.
Inoltre, nonostante l'ampio e concreto interesse sovranazionale di matrice europea sul tema, non risulta agevole delineare un inquadramento giuridico o individuare una definizione esaustiva di Smart City, dato che non esiste una definizione normativa in senso stretto, essendo quella di Smart City una nozione ampia dai confini giuridicamente incerti, che deriva soprattutto, come già evidenziato, da fonti di soft law e da perimetrazioni definite nell'ambito di specifici programmi, progetti o azioni settoriali.
Utile ai fini di una ricognizione del perimetro concettuale e definitorio di Smart City può essere il riferimento allo studio del Parlamento Europeo denominato "*Mapping smart cities in the EU*" (18), da cui è possibile cogliere le 6 connotazioni essenziali e irrinunciabili di una Smart City, ovvero: smart economy, smart mobility, smart environment, smart people, smart living e smart governance, i quali interattivamente e unitariamente considerati contribuiscono all'emersione di una nozione di sintesi di Smart City, intesa come: "*A city seeking to address public issues via ITC-based solutions on the basis of a multi-stakeholder, municipally-based partnership. These solutions are developed and refined through Smart City initiatives*".
Sempre basata sulle connotazioni essenziali della "smartness", per quanto concettualmente più articolata, è la definizione che di Smart City fornisce la Commissione Europea (19): "*a Smart City is a place where the traditional networks and services are made more efficient with the use of digital and telecommunication technologies, for the benefit of its inhabitants and businesses*" e ancora un luogo che "*goes beyond the use of digital technologies for better resource use and less emissions*" e che implica soprattutto "*a more interactive and responsive city administration, safer public spaces and meeting the needs of an ageing population*".

(16) <https://territorialagenda.eu/wp-content/uploads/TA2030_jul2021_it.pdf>.

(17) L'intento dell'EIP-SCC è di creare cluster di città europee, aziende e rappresentanti della società civile per avviare una significativa trasformazione digitale, per realizzare soluzioni sostenibili dal punto di vista dell'ambiente, della società e della salute. Alla fine del 2017, l'EIP-SCC ha visto più di 370 progetti nei settori dell'energia, dell'ITC e della mobilità. Tra le città europee impegnate nella trasformazione smart sono presenti: Copenaghen, Amsterdam, Vienna, Barcellona, Parigi, Stoccolma, Londra, Amburgo, Berlino, Helsinki. Tali città sono state classificate partendo dall'analisi dei successi ottenuti in base a 28 indicatori che spaziano tra la mobilità sostenibile, la green economy, la qualità della vita, la governance, l'ambiente e il costruito. A livello nazionale i fondi strutturali sono stati utilizzati eminentemente dando inizio ai Programmi Operativi Nazionali 2014 - 2020 «Città Metropolitane» e «Infrastrutture e Reti», in cui sono inquadrati progetti di diverso respiro che scaturiscono da differenti esigenze di sviluppo territoriale.

(18) Directorate-general for internal polices, Policy Department economic and scientific policy, Brussels, January 2014, 21, in <www.europarl.europa.eu>.

(19) <https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en>.

Alla luce delle definizioni appena richiamate, si può in prima battuta inferire che in linea di principio, il concetto di «Smart City» indica una città centrata su politiche di crescita sostenibile, anche dal punto di vista ambientale, in cui le dinamiche di gestione della cosa pubblica vengono integrate da sistemi, infrastrutture e mezzi tecnologicamente avanzati (Internet of Things, i Big Data e Analytics, e così anche la Virtualizzazione, il Rendering e Simulazione 3D, l'Artificial Intelligence, il Cloud) al fine di assicurare una pianificazione e fruizione intelligente delle risorse pubbliche e dei servizi essenziali e ottenere attraverso più elevati tassi di inclusione e partecipazione dei cittadini, un miglioramento degli standard qualitativi della vita umana.

Si resta però ancora nell'alveo di uno sforzo definitorio vago ed evanescente e che in ragione di tale vaghezza di significato non rende conto delle complessive potenzialità di valore di cui è intrisa di principio una Smart City, legittimando approcci esegetici e applicativi limitati e limitanti, come sovente accade allorché il paradigma della Smart City viene adoperato, specie nei paesi sviluppati a cd. democrazia stabilizzata, nel contesto delle crisi economiche e delle politiche di *climate change*, legando l'obiettivo prioritario della smartness della città allo sviluppo di nuove tecnologie per un rilancio della competitività economica o per la salvaguardia dell'ambiente.

È di tutta evidenza, per certi versi lapalissiano, che limitare l'ambito di declinazione del paradigma della Smart City ad un obiettivo di salvaguardia dell'ambiente o di recupero di competitività economica, attraverso il ricorso strategico alle soluzioni ITC sarebbe metodologicamente e concettualmente non corretto.

Ma il tema del recupero di una definizione appropriata in grado di orientare in maniera coerente i possibili scenari applicativi del paradigma della Smart City, deve innanzitutto passare attraverso una ricognizione sistematica degli ambiti di rilevanza della *smartness* della città, cercando di privilegiare un approccio multidisciplinare il cui traino è rappresentato da un ripensamento complessivo delle scelte strategiche della politica nel settore dei servizi essenziali alla persona, del welfare sociale e di equo accesso alle risorse di base oltre che della stessa concezione del benessere sociale e collettivo.

In questo senso, un indubbio punto di partenza dell'analisi è stabilire quali sono gli ambiti a cui la Smart City non può essere ridotta in via prevalente o esclusiva.

Certamente il concetto di città smart non può essere fatto coincidere con quello di città digitale: quest'ultima riporta al grado di informatizzazione nonché di *readiness* e destrezza digitale presente su un dato territorio, mentre la Smart City nel suo portato più comprensivo implica un livello superiore di pianificazione strategica delle politiche sociali tese a garantire la partecipazione attiva dei cittadini ai processi legati alla vivibilità della comunità urbana, alla qualità dei servizi resi e all'inclusione sociale.

Del resto, come per altro desumibile dalla letteratura di riferimento, ove il connotato innovativo e originale della città evoluta è stato ritenuto riducibile alla sola predominanza della dimensione ITC e delle dinamiche tecnologiche-digitali, sono state coerentemente enucleate e adottate altre più mirate terminologie come Digital City (20), Informational City (21), City of Bits (22), Cybernetic City (23), Media City (24), Ubiquitos City (25), Senseable City (26), Augmented City (27).

E non coincide nemmeno con il concetto di Green City apparendo chiaro che la smartness di una città è connotato per così dire ontologico che racchiude una molteplicità di fattori abilitanti, non riducibili in via esclusiva o anche solo preponderante alla tutela ambientale.

Per le stesse ragioni la Smart City non può essere ridotta a mero strumento di recupero o rilancio della competitività economica del sistema attraverso la realizzazione di sinergie tra lo sviluppo di nuove tecnologie, applicazioni di economia circolare e la crescente salvaguardia dell'ambiente.

### 3. Smart City ed approccio multidisciplinare. Il focus sulla sostenibilità sociale quale ambito di possibile rilevanza specifica del paradigma della Smart City in relazione agli SDGs e alla luce dei nuovi indici di rilevazione del benessere collettivo

L'avere indicato nel precedente paragrafo quali non sono gli ambiti concettuali di identificazione esclusiva di una Smart City, sebbene tutti parzialmente rilevanti e non antinomici tra loro, sembrerebbe quasi condurre ad una aporia insormontabile in ragione della quale ritenere obbligata una definizione ampia di Smart City, dai confini incerti anche in merito all'inquadramento giuridico, nonostante l'evoluzione sovranazionale e nazionale che pare al momento descrivere una mera utopia

(20) Foth-Brynskov - Ojal, *Citizen's Right to the Digital City. Urban Interfaces, Activism and Placemaking*, Singapore, 2015.

(21) Castells, *The Informational City. Information Technology, Economic Restructuring, and the Urban-Regional Process*, Oxford, 1989.

(22) Mitchell, *City of Bits. Space, Place, and the Infobahn*, Cambridge, 1996.

(23) Schoffer, *Cybernetic City*, London, 2009.

(24) McQuire, *The Media City: Media, Architecture and Urban Space*, Los Angeles, 2008.

(25) Wood, *City Ubiquitos. Place, Communication, and the Rise of Omnitopia*, Cresskill, 2009.

(26) Ratti - Claudel, *The City of Tomorrow: Sensors, Networks, Hackers, and the Future of Urban Life*, Yale, 2016.

(27) Carta, *Augmented City. A paradigm shift*, Trento, 2017.

urbanistica, anzi una *eterotopia* (28), un luogo-non luogo della nostra contemporaneità, ideale e idealizzato sebbene in realtà sovraesposto a contraddizioni insanabili, che dà per scontato la reale partecipazione/inclusione di tutti i cittadini *habitans* all'utilizzo degli apparati digitali e all'accesso alle risorse essenziali ma che nei fatti non è in grado di *cum-prehendere* gli esclusi, i vulnerabili e tutti coloro che vivono una condizione di diseguaglianza sostanziale per una molteplicità di fattori, migratori, economici, culturali, anagrafici e legati alla condizione di salute (fisico-psichiche).

Di fatto una città dei vivi e dei morti o come Foucault scriveva "*un luogo senza luogo, che vive per se stesso, che si autodelinea e che è abbandonato, nello stesso tempo*" (29).

Da qui prendendo le mosse, e venendo al punto di riflessione che si intende privilegiare, un possibile recupero di specificità identitaria della definizione di Smart City può e deve acquisirsi attraverso la valorizzazione degli obiettivi di sostenibilità (e degli obiettivi di sostenibilità sociale in particolare prima ancora che degli obiettivi di sostenibilità economica ed ambientale), nella costruzione di un modello di sperimentazione urbanistica all'altezza delle complesse sfide conseguenti ai processi di metropolizzazione in atto che condurranno nel 2050 circa il 70% della popolazione terrestre a vivere in citta o aree metropolitane.

Sia chiaro che la prospettiva analizzata non intende sottovalutare la criticità delle sfide sottese ai complessi e pressanti obiettivi di sostenibilità ambientale degli agglomerati urbani a cui oggi, sebbene essi occupino solo il 3% della superfice terrestre, vanno imputati il 60-80% del consumo di energia e il 75% delle emissioni di sostanze nocive oppure sottese agli obiettivi di sostenibilità economica intesi come intervento di contrasto al declino economico che interessa in maniera sempre più crescente e progressiva, in ragione dell'incremento dei tassi di metropolizzazione, persino i Paesi occidentali cd. a democrazia stabilizzata (30).

E tuttavia ove si adotti un approccio critico al concetto di Smart City teso a valorizzare un modello di urbanizzazione socialmente sostenibile, coerente con il goal 11 dell'Agenda 2030, che porti ad una effettiva prosperità inclusiva, la sfida più urgente che emerge è quella di fondare e consolidare una nuova concezione della città come spazio/luogo oggetto di diritti di cittadinanza e allo stesso tempo come complesso organizzato degli strumenti e delle dotazioni per l'esercizio attivo di questi diritti, coadiuvato dalle infrastrutture tecnologiche e digitali.

Un vero e proprio diritto alla città socialmente sostenibile, in cui gli abitanti siano messi in condizione di riappropriarsi di spazi di interazione sociale e di partecipazione attiva, riscrivendo il rapporto tra attori sociali e istituzioni urbane/politiche e rifondando il diritto di proprietà all'interno del contesto urbano per ripensare la funzione tipica della proprietà dello spazio urbano e ristrutturare i ruoli e le gerarchie all'interno della città.

In sintesi, una sorta di "*urbanism for all*" in grado di curare i mali ricorrenti delle città odierne rinvenibili nei sempre più estesi fenomeni di gentrificazione (31), inaccessibilità, segregazione e disuguaglianza.

Un diritto che in un'ottica liberale altro non è che "*an incremental addition to existing liberal-democratic rights*" (32) la cui applicazione deve essere garantita dall'attore istituzionale e sociale per eccellenza ossia lo Stato.

In questo senso, molteplici sono le iniziative volte a riconoscere un diritto alla città. Primo tra tutti, il *City Statute*, adottato in Brasile nel 2001 come legge federale, a tutela del diritto alla città per gli abitanti delle favelas, che riconosce il il valore sociale del territorio in aggiunta a quello economico.

E ancora: *La Carta mondiale per il Diritto alla Città* approvata nel 2005, *La Carta per il Diritto alla Città* adottata a Città del Messico nel 2010 e *La Carta Europea per la salvaguardia dei Diritti umani nella Città del 2012* adottata da oltre 300 città europee – di cui più di 100 italiane.

Anche le Nazioni Unite riconoscono e invocano il rispetto del diritto alla città, attraverso proprie agenzie satelliti come UN-Habitat, l'Unesco o il *World Urban Forum* includendo il diritto alla città tra le declinazioni naturali dei diritti fondamentali dell'uomo.

Un approccio quello del diritto alla città, come declinazione dei diritti fondamentali dell'Uomo, che va confermato e preteso ad avviso di chi scrive e che appare

(28) Foucault, *Le parole e le cose. Un'archeologia delle scienze umane*, Milano, 1996.

(29) Foucault, *Spazi altri. I luoghi delle eterotopie*, Milano, 2011. Il termine eterotopia coniato dal filosofo francese M. Foucault indica quegli spazi che hanno la particolare caratteristica di essere connessi a tutti gli altri spazi, ma in modo tale da sospendere, neutralizzare o invertire l'insieme dei rapporti che essi stessi designano, riflettono o rispecchiano.

(30) Si tratta di quei paesi (gli Stati Uniti e molti di quelli appartenenti all'Unione Europea) che si fondano sulle ragioni del costituzionalismo, che dimostrano una convinta difesa dei diritti di libertà e delle garanzie costituzionali, e il cui sistema di governo privilegia il criterio della separazione dei poteri quale baluardo dell'effettività della democrazia liberale. Frosini (a cura di), *Diritto pubblico comparato. Le democrazie stabilizzate*, Bologna, 2022.

(31) Aa.Vv., *Gentrificazione. Profili e saperi per l'analisi del cambiamento sociale delle città italiane*, Milano, 2022. Il concetto di "gentrificazione" è mutuato dalle analisi sociologiche e può essere definito come processo di borghesizzazione di aree urbane un tempo appannaggio della classe operaia o di ceti non abbienti, progressivamente rimpiazzati non potendo più economicamente sostenere i nuovi standard qualitativi del luogo di residenza con conseguente emarginazione sociale

(32) Purcell, *Possible worlds: Henri Lefebvre and the right to the city*, in *Journal of Urban Affairs*, 2014.

del tutto coerente con la tassonomia disegnata dal paragrafo 11 della New Urban Agenda delle Nazioni Unite nella parte in cui afferma in maniera programmatica il "diritto alla città' giusta, inclusiva, sicura, sana, accessibile, resiliente e sostenibile. Ma che soprattutto appare coerente con l'Agenda 2030 che nel nutrito elenco dei 17 obiettivi di sviluppo sostenibile da raggiungere entro il 2030 per migliorare lo sviluppo dell'umanità, dedica il "goal 11" specificatamente a "*Citta e comunità sostenibili*" con la finalità di "rendere le città e gli insediamenti umani inclusivi, sicuri, duraturi e sostenibili".

In questo solco, la prospettiva epistemologica sottesa alla valorizzazione del connotato della sostenibilità sociale diviene in altri termini un potente criterio teleologicamente orientato per un ripensamento delle strategie di urbanizzazione e per la risoluzione delle cause della cd. *new urban crisis* (33) sostanzialmente riconducibili alla i) plutocratizzazione delle cd. *superstar cities* (34) nelle quali vive e lavora solo il 7% della popolazione che genera il 40% dell'economia mondiale, ii) la scomparsa della classe media che unitamente alla crisi delle periferie, genera crescente disuguaglianza e segregazione (35), e iii) la crisi dell'urbanizzazione nei Paesi in via di sviluppo.

Sotto un altro angolo visuale, è un recuperare il punto di vista della sociologia urbana, fondata con la Scuola di Chicago, per il quale dirimente non è lo studio di ciò che succede all'interno delle città, ma lo studio sul modo in cui gli elementi e le dinamiche che strutturano le relazioni fra attori, istituzioni e gruppi sociali costituiscono la città come un unico ed esclusivo ecosistema e sul rapporto tra questo ecosistema e tutti gli altri ecosistemi specifici rilevanti al di fuori del contesto metropolitano.

Punto di vista la cui compiutezza, concettuale e metodologica, deve essere agevolata da alcune preliminari considerazioni sui concetti di metropolizzazione del territorio e di benessere collettivo.

Con il termine metropolizzazione (36) si fa riferimento ad un macrofenomeno di urbanizzazione caratterizzato da una tendenza espansiva esponenziale: se all'inizio del diciottesimo secolo, soltanto il 3% della popolazione terrestre viveva in città; oggi, quasi una persona su due, ed entro il 2050 si prevede che il 70% degli 8 miliardi di abitanti del pianeta vivranno nelle città.

Il risultato fisico più evidente di tale fenomeno è quello della dilatazione del sistema insediativo-infrastrutturale con prevalenti caratteri di dispersione e diffusione producendo effetti di frammentazione territoriale sempre più vistosi oltre ad alcune peculiari problematiche sostanzialmente riconducibili a tre dinamiche che rappresentano la *contradictio in adjecto* del principio della sostenibilità dello sviluppo: 1) il progressivo aumento del consumo di suolo, 2) un sistema di mobilità diffuso ma basato quasi solo sulla mobilità su gomma delle persone (in maggior parte individuale) e delle merci e quindi debole, congestionante e inquinante; 3) un modello energivoro e che produce sempre maggiore spreco energetico.

La metropolizzazione afferisce dunque per lo più, e fatta eccezione per pochi esempi virtuosi, ad un processo di diffusione insediativa rapida e disordinata, senza una pianificazione urbanistica adeguata e sostenibile (37) che sia concretamente connotata da azioni e politiche perseguibili mediante processi di governance e percorsi di pianificazione strategica.

Un fenomeno altrimenti definito di dispersione urbana o invasione urbana (38) (*urban sprawl* e *urban encroachment*) da cui si origina la città diffusa o espansa, opposta alla città *pubblica e partecipata*, in cui gli spazi e servizi pubblici o di uso pubblico, quando ci sono, non sono percepibili e fruibili come tali e dal quale emerge la drammatica incapacità dei paradigmi di sviluppo urbano attualmente in voga a fornire risposte efficaci alle grandi sfide del secolo in tema di sostenibilità sociale.

Gli effetti di segregazione e diseguaglianza sociale, unitamente alla disomogenea distribuzione del reddito e dell'accesso alle risorse essenziali, al diritto all'abitazione, alla istruzione e più in generale l'assenza di partecipazione attiva alla vita pubblica, sono tutti indici di un declino economico e sociale sempre più contiguo

(33) Florida, *The New Urban Crisis: How Our Cities Are Increasing Inequality, Deepening Segregation, and Failing the Middle Class, and What We Can Do About It*, 2017.

(34) Le Galès - Pierson, *Superstar Cities and the Generation of Durable Inequality*, 2019.

(35) Petrillo, *La periferia nuova. Disuguaglianza, spazi, città*, Milano, 2018.

(36) Ferrero, *Le smart cities nell'ordinamento giuridico*, in *Foro Amministrativo*, Anno II, Fasc. 4, 2015.

(37) Si tratta di problematiche fra loro fortemente interrelate: se l'organizzazione del sistema insediativo e del suo sviluppo non è basato sul trasporto collettivo (ove possibile, costituito da linee di forza su ferro) esistente o programmato, si sviluppa lo *sprawl urbano* ovvero il consumo di suolo che ha come conseguenza la impossibilità di affrontare la domanda di mobilità conseguente con un'offerta di trasporto collettivo; la dispersione-frammentazione a sua volta impedisce importanti forme di efficienza e risparmio energetico (si pensi ad esempio al teleriscaldamento, alla lunghezza e capillarità delle reti, ecc.). Il tema dell'urban sprawl ha dovuto aspettare il 2006 per entrare finalmente nel dibattito europeo grazie ad un report dell'Agenzia Europea dell'Ambiente (*Urban Sprawl – the ignored challenge*) nel quale viene dettagliatamente analizzato il fenomeno e si raccomanda un attento monitoraggio del consumo di suolo e degli impatti socioeconomici ed ambientali, che potrebbero rivelarsi catastrofici nel lungo periodo.

(38) Bencardino, *Consumo di suolo e sprawl urbano. Drivers e politiche di constrasto*, in *Bollettino della Società geografica italiana*, 2015, 217.

alla metropolizzazione anche nei Paesi occidentali a democrazia stabilizzata, che ha indotto in ambito internazionale e da oltre cinquant'anni un ripensamento complessivo degli indici di misurazione del benessere sociale e collettivo, grazie anche ad un approccio critico delle organizzazioni sovranazionali (39) nell'ottica del superamento dei tradizionali indicatori economici concepiti per misurare la capacità produttiva del singolo o dello Stato, come il reddito pro-capite e il prodotto interno lordo (PIL).

Un superamento del PIL come unico indicatore di misurazione del benessere causalmente determinato dalla consapevolezza che i parametri sui quali valutare il progresso di una società non possono essere esclusivamente di carattere economico, ma devono tenere conto anche delle fondamentali dimensioni sociali e ambientali del benessere, rilevanti ai fini dell'elaborazione, dell'adozione e della valutazione delle politiche pubbliche, al fine di integrare l'uso degli indicatori macroeconomici, ritenuti non più sufficienti a misurare il grado di benessere di una comunità e, perciò, ad orientare in maniera più coerente ed efficace le politiche pubbliche.

Un approccio innovativo e dinamico che prende le mosse dal carattere eterogeneo della dimensione del benessere collettivo, declinabile attraverso la manifestazione concorrente di molteplici fattori quali, esemplificativamente, gli standards materiali di vita (reddito, consumi e ricchezza), qualità sociale e parità tra i sessi, salute, istruzione di qualità, sviluppo della persona (compreso il lavoro), governabilità, integrazione e relazioni sociali, ambiente e sicurezza (economica così come fisica).

Su questo solco si pone anche l'approccio multidimensionale del benessere equo e sostenibile, cd. BES, teorizzato nel 2010 da un'iniziativa congiunta Istat–Cnel, con l'obiettivo di valutare il progresso del Paese e dei territori verso l'incremento del benessere dei cittadini e della società non soltanto dal punto di vista economico, ma anche sociale e ambientale e finalizzato ad integrare i tradizionali indicatori economici, reddito pro-capite e PIL, con altri indicatori di vario genere, compresi quelli relativi alle disuguaglianze ed alla sostenibilità per quantificare la distribuzione del reddito disponibile e la sostenibilità ambientale del benessere (40).

Il BES considera 12 dimensioni (41), articolate in 130 indicatori nell'ambito dei quali con decreto del MEF 16 ottobre 2017, sulla scorta dei criteri e le modalità stabiliti dalla legge 4 agosto 163 del 2016, sono stati selezionati 12 indicatori di benessere equo e sostenibile: reddito medio disponibile aggiustato pro capite; indice di diseguaglianza del reddito disponibile; indice di povertà assoluta; speranza di vita in buona salute alla nascita; eccesso di peso; uscita precoce dal sistema di istruzione e formazione; tasso di mancata partecipazione al lavoro, con relativa scomposizione per genere; rapporto tra tasso di occupazione delle donne di 25-49 anni con figli in età prescolare e delle donne senza figli; indice di criminalità predatoria; indice di efficienza della giustizia civile; emissioni di CO2 e altri gas clima alteranti; indice di abusivismo edilizio.

Il ripensamento degli indici di misurazione del benessere sociale e collettivo, ha come effetto primario quello di etero-determinare in maniera ancora più dirimente una definizione di Smart City finalisticamente orientata verso obiettivi specifici di sostenibilità sociale economica e ambientale che è esattamente il paradigma enunciato, come già indicato, nell'Agenda 2030 per lo Sviluppo Sostenibile e in particolare nell'obiettivo numero 11 intestato a "*Citta e comunità sostenibili*" e finalizzato a "*Rendere le città e gli insediamenti umani inclusivi, sicuri, duraturi e sostenibili*".

Il Goal 11, si focalizza su come affrontare le sfide che affliggono le città di oggi, in particolare ponendo attenzione al ripensamento in chiave di sostenibilità delle dimensione tipiche di un contesto urbano e di una comunità cittadina e quindi l'accesso agli alloggi e ai servizi di base, al sistema di trasporto sostenibile, all'urbanizzazione sostenibile, all'accesso agli spazi pubblici, alla creazione di edifici sostenibili, all'impatto ambientale pro capite delle città e alle politiche per fronteggiare il cambiamento climatico, al fine di ottimizzare la efficienza delle risorse e la riduzione del rischio di disastri naturali.

Tutti i 17 Goal sono fortemente interconnessi l'uno con l'altro, ma il Goal 11 è particolarmente legato ai temi della presenza e della organizzazione dell'uomo sulla

(39) Risale al 2003 il progetto OCSE di revisione del concetto di benessere denominato *Global Project on Measuring the Progress of Societies*, disponibile alla pagina web <http://www.oecd.org/statistics/measuring-well-being-and-progress.htm>. In seguito, anche l'Unione Europea ha espresso la propria adesione ad un simile mutamento culturale prima ancora che economico, come si evince dalla Comunicazione della Commissione al Consiglio e al Parlamento Europeo del 20 agosto 2009, n. 433, denominata *Non solo PIL. Misurare il progresso in un mondo in cambiamento*, consultabile all'indirizzo <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0433:FIN:IT:PDF>.

(40) Con la legge n. 163/2016 di riforma della legge di contabilità n. 196 del 2009, gli indicatori di benessere equo e sostenibile sono entrati nell'ordinamento italiano, venendo inclusi tra gli strumenti di programmazione e valutazione della politica economica nazionale. Maggiori approfondimenti su <https://temi.camera.it/leg17/temi/benessere_equo_e_sostenibile>.

(41) Le 12 dimensioni sono: Salute, Istruzione e formazione, Lavoro e conciliazione tempi di vita, Benessere economico Relazioni sociali, Politica e istituzioni, Sicurezza, Benessere soggettivo, Paesaggio e patrimonio culturale, Ambiente, Ricerca e innovazione, Qualità dei servizi.

terra ed all'impatto antropico sulle risorse naturali. In particolare il legame lo si rinviene con il Goal 3 (salute e benessere degli individui), il Goal 6 (migliore qualità dell'acqua e riduzione dell'inquinamento idrico), il Goal 9 (infrastrutture resilienti, industrializzazione inclusiva e sostenibile e favorire l'innovazione), il Goal 10 (riduzione delle diseguaglianze), il Goal 13 (azione contro il cambiamento climatico) e il Goal 15 (vita sulla terra).

Va tuttavia precisato, però, che tra gli obiettivi dell'Agenda 2030, il Goal 11 è quello in cui l'Agenda 2030 registra a livello globale i ritardi più significativi il che comporta la presa d'atto di quanto ancora utopistica sia la concretizzazione del paradigma della citta inclusiva che guarisce le disuguaglianze e le esclusioni dei suoi abitanti nel rispetto della biosfera e in generale degli ecosistemi che interagiscono con la città stessa.

È una circostanza oggettiva conclamata dalle relazioni annuali dell'OCSE (Organizzazione per la cooperazione e lo sviluppo economico).

Del resto diversi sono i fattori che ostacolano una piena attuazione del Goal 11 a livello globale. Innanzitutto ci sono numerose differenze strutturali tra le città dei Paesi sviluppati e quelle dei Paesi in via di sviluppo.

Non a caso, oggi gli 830 milioni di persone che vivono in baraccopoli ai margini delle grandi città, sono diffusi principalmente in tre aree geografiche molto povere: Est e Sud-Est Asiatico (370 milioni), Africa Sub-Sahariana (238 milioni) e Asia Centrale (226 milioni).

Va poi considerato il grande impatto in termini di inquinamento prodotto dalle città, dato che esse pur occupando solo il 3% della superficie terrestre, sono responsabili del 60-80% del consumo di energia e del 75% delle emissioni di sostanze nocive.

Da ultimo, va considerato al livello dei decisori politici il grado di incidenza ed efficacia della programmazione delle strategie di implementazione degli obiettivi di sviluppo sostenibile dell'Agenda 2030.

Secondo il *Sustainable Development Report 2023*, infatti, c'è ancora una significativa discrepanza tra il sostegno politico espresso per gli SDGs e l'integrazione degli obiettivi nei processi strategici di politica pubblica, in particolare nei bilanci nazionali. Meno della metà dei Paesi intervistati nel Report (20 su 48) menziona gli SDGs o usa termini correlati nel loro ultimo documento di bilancio ufficiale, o include gli SDGs in una sezione dedicata dei loro bilanci nazionali.

Per quanto riguarda la performance dell'Italia rispetto all'Obiettivo 11, stando ai dati diffusi dall'ASviS (Alleanza italiana per lo sviluppo sostenibile) nel Rapporto 2023 su Città e Comunità Sostenibili e dall'Istat nel Rapporto SDGs 2023, il Paese deve ancora migliorare sotto diversi aspetti. L'Italia, infatti, si posiziona, ancora oggi come nel 2019, al di sotto della media europea, soprattutto a causa del maggiore tasso di sovraffollamento delle abitazioni (28,3% contro il 17,1% dell'UE) e a una maggiore esposizione alle Pm10 (25,5 µg/m3 rispetto a 20,5 dell'Ue).

## 4. Il rapporto tra smartness (ITC driven) e sostenibilità sociale. La aporia definitoria del concetto di sostenibilità sociale e il riflesso sulla difficoltà di una elencazione esaustiva delle dimensioni della sostenibilità sociale e dei suoi indicatori

Interrogarsi sulla sostenibilità sociale della Smart City non significa però solo cercare di capire quali scelte politiche e strategie i decisori pubblici, a livello nazionale e comunitario, possono e devono pianificare ed adottare per tutelare e applicare il diritto alla città inclusiva e partecipativa e rispettosa della biosfera.

Significa anche, e soprattutto, porsi la questione di come e quanto lo sviluppo della *smartness* (in senso tecnologico e digitale) della città incida effettivamente sull'implementazione della dimensione della sostenibilità sociale.

Sebbene molto si sia scritto sul tema dello sviluppo ambientale ed economico della città, e sulle interazioni tra queste due dimensioni, lo stesso non si può dire per il pilastro dello sviluppo sostenibile sociale che rimane ancor oggi per lo più un concetto non puntualmente qualificato e definito che lascia spazio a continue interpretazioni.

La ragione delle difficoltà di delimitazione del suo "campo" specifico è probabilmente da rinvenire nella circostanza per cui le tre dimensioni dello sviluppo sostenibile tendono a sovrapporsi e questo può innescare difficoltà nel discernere dove inizia una e finisce l'altra. Tale circostanza si riflette a sua volta anche nella difficoltà ad individuare una definizione univoca e condivisa di sostenibilità sociale.

Nella letteratura dedicata le definizioni di sostenibilità sociale sono molto variegate, e in una certa misura semanticamente orientate dalla prevalenza di un paradigma valoriale piuttosto che un altro coinvolgendo di volta in volta in maniera caratterizzante ora la dimensione economica, ora quella politica e ancora quella più strettamente sociale, etica, culturale o ancora la connotazione istituzionale e normativa ancorata al diritto positivo. Ad esempio una nozione di sostenibilità sociale centrata sui paradigmi economico e politico e sul bisogno di una loro rifondazione in ottica di recupero della dignità dell'essere umano è quella di Jeffrey Sachs (42), economista di fama internazionale e tra i massimi esperti di sviluppo sostenibile, oltre che docente alla Columbia

(42) Sachs, *L'era dello sviluppo sostenibile*, Milano, 2015.

University dove dirige il Center for Sustainable Development: «*La sostenibilità sociale prevede il raggiungimento di un giusto grado di omogeneità sociale, un'equa distribuzione del reddito, un'occupazione che permetta la creazione di mezzi di sussistenza dignitosi e un equo accesso alle risorse e ai servizi sociali, un equilibrio tra rispetto della tradizione e innovazione*» e ancora «*Una definizione forte di sostenibilità sociale deve poggiare sui valori fondamentali di equità e democrazia, quest'ultima intesa come l'effettiva appropriazione di tutti i diritti umani – politici, civili, economici, sociali e culturali – da parte di tutte le persone*».

Una definizione invece incentrata sul fattore sociale, etico e culturale e sulla valorizzazione delle diversità dei gruppi di appartenenza, è quella di Polese e Stren (43): «*La sostenibilità sociale è uno sviluppo (e/o una crescita) compatibile con l'evoluzione armoniosa della società civile, che alimenta un ambiente favorevole alla coabitazione di gruppi culturalmente e socialmente diversi, e allo stesso tempo favorisce l'integrazione sociale, con miglioramenti nella qualità della vita per tutti i segmenti della popolazione*»

Una nozione decisamente orientata dal criterio istituzionale-normativo è quella di Kostantinos Alexandris Polomarkakis (44): «*La sostenibilità sociale è «l'insieme delle politiche, delle regole e dei principi stabiliti nell'ordinamento giuridico dell'UE, che mirano a rafforzare la dimensione sociale dell'UE come soluzione a lungo termine, mettendola al riparo da qualsiasi ricaduta in una posizione di subordinazione gerarchica ai mercati, in modo che l'Europa sociale possa essere percepita inequivocabilmente come un contraltare alla costituzione economica*» Com'è possibile desumere già da queste definizioni, proposte a titolo esemplificativo, e dalla differenziazione che ciascuna di esse presenta rispetto all'altra, arrivare ad una ricomposizione che soddisfi tutte le peculiarità che ciascuna di esse ha cercato di mettere in risalto è un'operazione tutt'altro che semplice.

Invero il concetto di sostenibilità sociale e più in generale di sviluppo sostenibile in sé non tollera una definizione statica essendo per sua attitudine un concetto dinamico, adattabile a più settori disciplinari e contesti non omogenei.

Va inteso quindi sia come principio giuridico aperto e applicabile a diversi contesti, sia come obiettivo di politiche ambientali e di sviluppo economico sia come obiettivo di equità, di solidarietà sociale e lotta alla povertà, sia come processo globale di cambiamento etico - culturale.

Queste difficoltà di tracciamento netto dei confini definitori del concetto di sostenibilità sociale risultano a loro volta sovrapponibili alle difficoltà nel giungere ad un modello di classificazione comune delle dimensioni e degli indicatori rilevanti ai fini di identificazione e misurazione degli obiettivi di sviluppo socialmente sostenibile nell'ambito della Smart City.

Un tentativo degno di nota è stato compiuto da Susan Opp (45) che, attraverso un'analisi della letteratura accademica, delle ricerche applicate e dei documenti governativi provenienti da varie parti del mondo, Stati Uniti, Canada, Finlandia, Svezia, Norvegia, Australia, è riuscita a proporre una modellazione della sostenibilità sociale della Smart City basata su quattro dimensioni estremamente interrelate tra loro con indicatori mirati a misurarne il livello di soddisfazione: *equal access and opportunity, environmental justice, community and the value of place, basic human needs*.

Un quadro che, sul piano teorico, lega ontologicamente il riconoscimento della condizione di *smartness* cittadina ad obiettivi tipici della sostenibilità sociale, a prescindere da un ruolo guida della tecnologia smart.

Altre recenti analisi (46) sulla modalità di applicazione del paradigma Smart City hanno evidenziato che le potenzialità di sviluppo delle politiche di sostenibilità sociale dipendono, più che dall'utilizzo massiccio di strumenti e infrastrutture ITC, dall'adozione di una chiara strategia di programmazione di interventi ad alto impatto sociale nell'ambito del tessuto urbano che parta e tenga conto delle specificità dei diversi contesti per giungere ad un ventaglio coerente e dedicato di azioni integrate da applicare ai diversi ambiti di intervento.

Il che equivale a dire che la smartness tecnologica e digitale di una città non è un fattore generativo in se di sostenibilità sociale ma un mero fattore abilitante e di supporto alle strategie di sostenibilità sociale non imprescindibile né determinante.

Ed equivale anche a dire che la strategia della sostenibilità sociale della città intelligente può essere affidata ad un piano di sviluppo completamente differente ed autonomo rispetto alla strategia di implementazione della

(43) Polese-Stren, *The Social Sustainability of Cities: Diversity and the Management of Change*, Toronto, 2000

(44) Polomarkakis, *The European Pillar of social rights and the Quest for EU Social Sustainability*, London, 2020.

(45) Opp, *The forgotten pillar: a definition for the measurement of social sustainability* in American cities, 2017 <https://www.researchgate.net/publication/304028677_The_forgotten_pillar_a_definition_for_the_measurement_of_social_sustainability_in_American_cities>. L'attendibilità del modello di OPP non va tuttavia confusa con un consenso unanime sulle quattro dimensioni e i loro relativi indicatori. Tuttavia, da esso emerge che, nella modellazione della sostenibilità sociale, la *smartness* giochi un ruolo estremamente importante, costituendo il substrato tecnologico/comunicativo di base per l'implementazione degli indicatori di equo accesso del cittadino alle opportunità offerte dalla comunità urbana.

(46) Gurashi, *Esplorando la sostenibilità sociale delle smart city. I casi di Sydney e Okayama*, in *Rivista Trimestrale di Scienza dell'Amministrazione*, 1/2021.

smartness basata prioritariamente e/o esclusivamente sul potenziamento delle infrastrutture ITC.
La Smart City, insomma, è intelligente dal punto di vista della sostenibilità sociale nella misura in cui riesce a innescare un processo di miglioramento continuo della qualità della vita (nel senso di migliore fruizione della città e dei suoi servizi), che tenga conto delle differenze sociali, economiche e culturali tra i gruppi sociali e che sono basilari per l'individuazione di strategie specifiche di intervento ai fini di inclusione sociale.
Entro tale perimetro, diviene poi fondamentale distinguere i bisogni individuali dai bisogni dei gruppi sociali per intervenire in maniera efficace su alcune macro-aree rilevanti in rapporto di integrazione circolare tra loro: i) diritti individuali (assicurare ai singoli l'accesso ai diritti costituzionali, al cibo e alla salute), ii) equità e coesione sociale (azioni che riducono le disparità per soggetti vulnerabili), iii) costruzione di comunità (iniziative volte a formare e dare solidità al legame sociale tra persone e gruppi anche a fronte di fattori di forte cambiamento culturale e sociale).
Le politiche strategiche di creazione di sostenibilità sociale che si concentrano su tali aree di intervento, declinano nei fatti un approccio metodologico che recupera il senso più intimo e proprio del termine sostenibilità che da un punto di vista etimologico origina (47) dal verbo latino *sustineo* nel suo duplice significato, quello proprio di "sostenere" e quello figurato di "proteggere/difendere, in rapporto di evidente biunivoco condizionamento.
In questo senso è evidente il riferimento all'idea di rimozione degli ostacoli per garantire la progressione del benessere individuale e collettivo.
Garantire in particolare la sostenibilità sociale dello sviluppo significa tutelare le generazioni future, permettendo loro di avere le stesse possibilità nel rapporto con le risorse naturali e significa anche dare il giusto rilievo alla dimensione etica e socio-culturale della sostenibilità per la quale è necessaria una partecipazione attiva dei cittadini e una maggior presa di coscienza e di responsabilità da parte dell'intera collettività.

## 5. Conclusioni. Dalla "Smart City" alla "Social Sustainable Smart City". Una prospettiva costituzionalmente orientata

Questa visione di città intelligente e sostenibile, integrata in tutte le sue componenti di valore, ma nella quale la sostenibilità sociale è agevolata dalla tecnologia senza dipendere in via esclusiva da essa, induce alla necessità di dar conto di un passaggio evolutivo dal concetto di Smart City a quello di *Social Sustainable Smart City* valorizzando il principio di fondo per eccellenza della sostenibilità sociale, il "*Leave No One Behind*".
Emerge cioè l'idea di una città tesa a fortificare gli spazi, i luoghi e le formazioni sociali entro i quali si svolge il *proprium* della persona umana in attuazione dell'art. 2 della costituzione italiana, nel rispetto della Carta dei diritti fondamentali dell'Unione Europea e della Dichiarazione Universale dei diritti dell'Uomo.
Una città in cui non trovano spazio e legittimazione differenti livelli di cittadinanza con differenziati livelli di accesso a determinate risorse sulla base di differenti capacità reddituali; una città tesa a ricostruire un significato di spazio pubblico inclusivo e non discriminante, definito attraverso la partecipazione effettiva e compiuta ai beni collettivi di tutti i cittadini a prescindere dal gruppo sociale di appartenenza e del profilo reddituale posseduto.
Sotto questo profilo, la Social Sustainable Smart City diventa una nuova potente forma di democrazia che parte dal riconoscimento di una comunità urbana intelligente e sostenibile in cui il cittadino è soggetto attivo, corresponsabile di nuovi modi di governare la res pubblica, e non un mero passivo fruitore-consumatore di beni e servizi, come è preponderante negli attuali modelli di comunità urbana.
Un nuovo modello di governo della collettività in termini di sostenibilità capace di rifondare l'architrave della società, della politica, dell'economia e della produzione, dando il giusto senso e priorità alle connessioni sociali e relazionali tra sistemi umani e sistemi non umani.
È insomma il luogo ideale che rende possibile la ricostruzione in termini di sostenibilità del rapporto tra la Natura, gli ecosistemi e l'Uomo, inteso aristotelicamente nel suo connotato di Homo Politicus, rispetto al quale Scienza e Tecnica devono essere asservite in quanto strumenti finalisticamente e operativamente orientati alla creazione di soluzioni responsabili di benessere dell'individuo e della società.
Non a caso negli studi di sociologia e antropologia più recenti, si è incominciato a parlare più correttamente di "*ecodomia del comune*" (48), con una espressione che trae origine dall'Etica Nicomachea (II, 10-11), allorchè Aristotele scrive: *eu oikodomein agathoi oikodòmoi èsontai/* Il ben costruire fa il buon costruttore.
E a ben vedere il futuro della prospettiva umana in generale e delle città intelligenti sostenibili in particolare è tutto nella capacità dell'Uomo di saper ben costruire lo spazio comune delle relazioni attraverso la cura della convivialità e dei beni e servizi funzionali allo sviluppo dell'individuo.

(47) Zupi, *Significati, idee e politiche di sostenibilità*, Roma, 2014.

(48) Capone, *Ecodomia del comune. Note su come rifare il mondo restando felici*, Verona, 2022

Si comprende quindi l'importanza di un urbanesimo conscio e consapevole che passi attraverso il ripensamento in ottica di sostenibilità sociale delle attività antropiche e delle comunità urbane metropolitane, piegando Scienza e Tecnica alla ricerca di soluzioni finalisticamente orientate al perseguimento degli obiettivi di governo responsabile della comunità degli uomini così come della Natura e delle sue risorse, con il fine ultimo della salvezza del genere umano dal rischio della estinzione biologica.

A pensarla diversamente nel perpetuarsi delle condizioni di miope intendimento e gestione delle criticità degli ecosistemi urbani e di tutti gli altri ecosistemi intorno a noi, si perpetuerebbero anche le dinamiche utilitaristiche proprie delle convenienze contingenti che mai nella storia dell'Uomo e del pensiero politico moderno hanno contribuito a creare superiori pratiche del bene comune, anzi avendo piuttosto generato particolarismi e individualismi egoistici e iniqui, come lo specismo, il classismo, il sessismo e il razzismo, latori di disagio sociale e distruttori di quei legami solidaristici da cui una società equa, libera, democratica, inclusiva e partecipata, dipende in via esclusiva.

Si tratta di una prospettiva sistemica che disancorando il paradigma della città da quello di *ente-ordinamento* connotato da rigidi confini amministrativi territoriali (49) e riconducendolo anzi al più esteso e articolato concetto di "*ente-sistema*" (50) o di "*ordinamento di ordinamenti*" (51) (prendendo in prestito una espressione del giurista Santi Romano, padre del diritto amministrativo italiano nonché fondatore della teoria istituzionalistica del diritto), è in grado di permeare ed educare l'orientamento di "*una citta organica, un sistema di sistemi, che nello spazio urbano affronta la sfida della globalizzazione in termini di aumento della competitività, dell'attrattività, dell'inclusività*" (52)

Tale approccio ermeneutico consente di ricondurre la *Social Sustainable Smart City* in un ambito costituzionalmente orientato sul presupposto che la sostenibilità e per essa i fattori ESG – a cui la città intelligente non può sottrarsi – rappresentano il terreno elettivo per una gestione conformata del rapporto/conflitto/concorrenza tra i diversi valori costituzionali riconducibili al benessere collettivo, richiamandosi a tal fine gli articoli della Costituzione: 9, comma 3 che assegna alla Repubblica, tra l'altro, il compito di tutelare «l'ambiente, la biodiversità e gli ecosistemi, anche nell'interesse delle future generazioni» (53), l'art. 41 per il quale l'iniziativa economica privata non può svolgersi in modo da recare danno, oltre che alla sicurezza, alla libertà, alla dignità umana, alla salute e all'ambiente, ma soprattutto l'art. 2 che riconosce e garantisce diritti inviolabili dell'Uomo non solo come singolo ma anche nelle formazioni sociali ove si svolge la personalità dell'individuo, richiedendo l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale.

E nel bilanciamento di interessi e valori ESG occorrerà applicare tutti i parametri propri del bilanciamento tra valori costituzionali quali ragionevolezza, proporzionalità e non arbitrarietà, sottoponendo l'eventuale apposizione di limiti al criterio rigoroso dell'utilità sociale con la conseguenza che nel conflitto tra interessi patrimoniali e non patrimoniali devono prevalere, di regola, i secondi, affinché si voglia garantire l'obiettivo della sostenibilità (54).

Ciò perché l'analisi del bilanciamento non può prescindere dalla considerazione preminente del principio costituzionale della solidarietà poc'anzi citato e di cui la stessa prospettiva della sostenibilità deve considerarsi una declinazione applicativa (55).

Il che equivale anche a dire che nella concorrenza tra i fattori ESG, in ragione del principio costituzionale di solidarietà e del limite inderogabile della utilità sociale, il fattore S (social) deve sempre prevalere, esprimendo senza equivoci il valore della preminenza della persona sulle logiche del mercato.

Concludendo, emerge un dovere di conformazione costituzionale della Social Sustainable Smart City, in virtù della incidenza degli obiettivi ESG – e di sostenibilità sociale in particolare – più propriamente intesi come una essenziale modalità applicativa del principio-dovere di solidarietà costituzionale in forza del quale lo Stato è chiamato "*alle proprie ineludibili responsabilità sul piano della concreta attuazione delle istanze della sostenibilità, stimolandolo ad esercitare il proprio potere di indirizzo e di intervento ab externo*" (56).

Come l'iniziativa economica privata ex art. 41 Cost, cosi anche la creazione di comunità urbane "ESG conforma-

(49) Pettirossi, *Smart City: la Città autonoma*, in *Rivista Trimestrale di Scienza dell'Amministrazione*, n. 3/2020.

(50) Carrozza, *Le province della post-modernita: la citta territoriale*, in <Federalismi.it>, 2018

(51) Romano, *L'ordinamento giuridico*, Firenze, 1977.

(52) Bonomi - Masiero, *Dalla smart city alla smart land*, Venezia, 2014.

(53) Fimmanò, *Art. 41 della Costituzione e valori ESG*, in *Giurisprudenza Commerciale*, Anno L Fasc. 5, 2023: "L'espressa previsione di tale finalità di tutela nella carta costituzionale permette al bene giuridico "ambiente" di passare dall'incerto status giuridico di «valore» a quello più granitico, non solo sul piano dogmatico, di «principio fondamentale» con tutte le conseguenze del caso".

(54) Perlingieri, *Sostenibilità», ordinamento giuridico e «retorica dei diritti». A margine di un recente libro*, in *Foro nap.*, 2020, 106.

(55) Alpa, *Solidarietà. Un principio normativo*, Bologna, 2023.

(56) Palmieri, *Crisi dell'impresa e responsabilità sociale*, in *Riv. corte conti*, 2023, 70.

te" non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana dovendo anche i modelli di urbanizzazione essere piegati alla realizzazione dei fini sociali dello Stato, nella prospettiva del benessere per la comunità, anche dal punto di vista ambientale, e del rispetto dei più elementari diritti della persona umana (57).

(57) CARIELLO, *Per un diritto costituzionale della sostenibilità (oltre la "sostenibilità ambientale")*, in *Orizzonti dir. comm.*, 2, 2022, 413, secondo cui la sostenibilità in senso lato o tout court è un paradigma del diritto societario ma può divenire paradigma del diritto costituzionale, grazie ad un'attenta attività interpretativa operata con l'impiego di specifiche regole interpretative, così da delineare le basi per un diritto costituzionale della sostenibilità.