IAIC MiBACT DGBIC CREDA

Diritto Mercato Tecnologia

FONDATA E DIRETTA DA
Alberto M. Gambino

COMITATO DI DIREZIONE
Valeria Falce, Giusella Finocchiaro, Oreste Pollicino,
Giorgio Resta, Salvatore Sica

30 novembre 2023

Governo dei dati personali nell'impiego dell'intelligenza artificiale e della *blockchain* da parte della sanità pubblica

Fernanda Faini

Nuova Editrice Universitaria

La rivista è stata fondata nel 2009 da Alberto M. Gambino ed è oggi pubblicata dall'Accademia Italiana del Codice di Internet (IAIC) sotto gli auspici del Ministero dei beni e delle attività culturali e del turismo - Direzione generale biblioteche e istituti culturali (DGBIC) e dell'Università Europea di Roma con il Centro di Ricerca di Eccellenza del Diritto d'Autore (CREDA).

Norme di autodisciplina

1. La pubblicazione dei contributi sulla rivista "Diritto Mercato Tecnologia" è subordinata alla presentazione da parte di almeno un membro del Comitato di Direzione o del Comitato Scientifico e al giudizio positivo di almeno un membro del Comitato per la Valutazione Scientifica, scelto per rotazione all'interno del medesimo, tenuto conto dell'area tematica del contributo. I contributi in lingua diversa dall'italiano potranno essere affidati per il referaggio ai componenti del Comitato Scientifico Internazionale. In caso di pareri contrastanti il Comitato di Direzione assume la responsabilità circa la pubblicazione.
2. Il singolo contributo è inviato al valutatore senza notizia dell'identità dell'autore.
3. L'identità del valutatore è coperta da anonimato.
4. Nel caso che il valutatore esprima un giudizio positivo condizionato a revisione o modifica del contributo, il Comitato di Direzione autorizza la pubblicazione solo a seguito dell'adeguamento del saggio.

La Rivista adotta un Codice etico e di buone prassi della pubblicazione scientifica conforme agli standard elaborati dal Committee on Publication Ethics (COPE): Best Practice Guidelines for Journal Editors.

Sede della Redazione

Accademia Italiana del Codice di Internet, Via dei Tre Orologi 14/a, 00197 Roma, tel. 06.8088855, fax 06.8070483, www.iaic.it, info@iaic.it

GOVERNO DEI DATI PERSONALI NELL'IMPIEGO DELL'INTELLIGENZA ARTIFICIALE E DELLA *BLOCKCHAIN* DA PARTE DELLA SANITÀ PUBBLICA

Fernanda Faini

SOMMARIO: 1. Il volto della sanità pubblica digitale – 2. Il valore delle tecnologie emergenti e la tutela del diritto alla protezione dei dati personali; 2.1. Intelligenza artificiale e *data protection*; 2.2. *Blockchain* e *data protection* – 3. Il governo dei dati e delle tecnologie emergenti: direzioni e scenari

1. Il volto della sanità pubblica digitale

Nell'evoluzione da strumento statico a dimensione dinamica e pervasiva, la rete è diventata il più grande spazio pubblico di condivisione, sviluppo e aggregazione di informazioni, relazioni e servizi, capace di indurre mutamenti nella società, caratterizzata in modo determinante dalla realtà digitale e dai suoi servizi.

La rinnovata fisionomia della società contemporanea, innescata dall'avvento e dall'evoluzione delle tecnologie informatiche e caratterizzata dal ruolo centrale assunto dai dati, determina una correlata trasformazione delle relazioni e la genesi di nuovi modelli di governo; di conseguenza muta il volto dell'amministrazione pubblica, attore protagonista dei processi di riferimento della società, e, parallelamente, cambia la fisionomia dalla sanità pubblica.

Il profondo sviluppo della società tecnologica è, dunque, all'origine dell'evoluzione dell'amministrazione pubblica nel senso della digitalizzazione, sviluppo necessario per rispondere efficacemente ai bisogni espressi dalla collettività. Del resto la finalità profonda delle istituzioni risiede nell'effettivo riconoscimento dei diritti dei cittadini e nella realizzazione del benessere della collettività: a tali fini le amministrazioni, nello svolgimento delle funzioni e nell'erogazione dei servizi, devono essere capaci di com-

prendere le esigenze della collettività, interagire con le modalità relazionali più idonee e realizzare la soddisfazione degli utenti[1]; nel perseguire tali obiettivi, al fine di compiere in modo adeguato il proprio ruolo, i poteri pubblici sono chiamati ad evolvere insieme alla società, trovandosi pertanto chiamati a guidare e governare lo sviluppo digitale nei diversi settori di competenza, tra cui quello sanitario[2].

Di conseguenza, il diritto, chiamato a regolare l'innovazione, si è occupato di disciplinare principi, finalità e strumenti di quella che viene definita come amministrazione pubblica digitale, in relazione a cui, proprio per la natura del soggetto, si pongono esigenze stringenti di garantire certezza del diritto e validità giuridica delle attività espletate in modalità digitale.

Con il termine amministrazione digitale si intende l'adozione estesa e integrata delle tecnologie informatiche nello svolgimento delle funzioni e nell'erogazione dei servizi della pubblica amministrazione. Il concetto stesso si riferisce all'innovazione in senso ampio come evoluzione dell'amministrazione pubblica attivata dalle tecnologie informatiche, che, lungi dall'esaurirsi in queste, si esplica altresì in un conseguente e necessario cambiamento di logiche e processi dell'*agere* pubblico. Realizzare la pubblica amministrazione digitale non significa una semplice automazione dei procedimenti, ma implica un'accurata riorganizzazione delle strutture, la razionalizzazione delle attività, la reingegnerizzazione dei processi e la configurazione di un nuovo rapporto con la cittadinanza, a sua volta "digitale": tali aspetti si traducono in un profondo ed esteso ripensamento di relazioni, attività, processi e procedimenti, in cui le tecnologie informatiche non costituiscono il fine ultimo, ma rappresentano lo strumento idoneo a raggiungere gli obiettivi che caratterizzano l'azione pubblica, con lo scopo finale di accrescere la soddisfazione e il benessere della collettività, garantendo i diritti dei cittadini[3]. Le motivazioni e gli obiettivi principali

[1] Cfr. D'ORLANDO, *Profili costituzionali dell'amministrazione digitale*, in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2011, 213 ss.

[2] Cfr. OTRANTO, *Internet nell'organizzazione amministrativa. Reti di libertà*, Bari, 2015, 104, secondo cui i poteri pubblici, nel guidare lo sviluppo digitale della società, devono creare «le condizioni più favorevoli per l'attuazione, attraverso la rete, del principio personalista nella sua nuova e sempre più complessa dimensione».

[3] In merito MANCARELLA (a cura di), *Lineamenti di informatica giuridica*, Trento, 2017, 71 ss. parla di *eGovernment* come *iGovernment* per sottolineare la necessaria innovazio-

dell'attenzione, anche normativa, alla costruzione della pubblica amministrazione digitale hanno radici proprio nelle finalità cui è diretta l'azione pubblica: efficacia ed efficienza; migliore qualità dei servizi; maggiore soddisfazione degli utenti; semplificazione idonea a snellire e rendere più tempestiva l'azione amministrativa; riduzione dei tempi e dei costi; partecipazione dei cittadini. Del resto, la *ratio* profonda della regolazione in materia si situa proprio nel suo porsi quale strumento atto a garantire il buon andamento della pubblica amministrazione, ricavando preziosa, anche se indiretta, fonte costituzionale nell'art. 97, comma 1, Cost.[4].

Per mezzo del processo di trasformazione digitale tra la pubblica amministrazione e la collettività può prendere forma un nuovo rapporto di fiducia, grazie a un'interazione maggiormente diretta e a una relazione inedita di collaborazione, che permette di ridurre le asimmetrie e gli squilibri e poggia sui principi di trasparenza[5], ascolto[6] e partecipazione[7]. L'ordinamento giuridico si occupa esplicitamente della cittadinanza digitale, concetto teso a individuare la configurazione stessa dei diritti dei cittadini nei confronti delle istituzioni, resa possibile dalle nuove tecnologie, che, pertanto, si compone di diritti eterogenei verso i poteri pubblici: in alcuni casi si tratta di nuove modalità di esercizio di diritti già parte della dotazione di ogni cittadino, in altri casi della possibilità di agire nuovi diritti, quelli resi possibili dalle tecnologie informatiche.

---

ne procedurale e organizzativa della pubblica amministrazione per raggiungere i parametri di efficacia, efficienza ed economicità.

[4] Ai sensi dell'art. 97 Cost. «*i pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione*».

[5] Gli strumenti digitali ontologicamente favoriscono la trasparenza e, di conseguenza, attribuiscono ai cittadini un potere di controllo democratico sullo svolgimento dell'attività amministrativa, idoneo a favorire buon andamento ed imparzialità.

[6] L'attenzione alla collettività si traduce nel passaggio dalla logica del provvedimento a quella del servizio, incentivando strumenti tesi a misurare il grado di soddisfazione dell'utenza; cfr. CAROTTI, *L'amministrazione digitale e la trasparenza amministrativa (commento alla legge 7 agosto 2015, n. 124)*, in *Giornale di diritto amministrativo*, fasc. 5, 2015, 625-629.

[7] Le tecnologie informatiche agevolano la creazione di momenti e luoghi di partecipazione e collaborazione con gli utenti, in merito alle decisioni e ai servizi delle amministrazioni.

In materia il riferimento normativo principale è costituito dal Codice dell'amministrazione digitale (CAD), il d.lgs. 82/2005, che è stato oggetto di ripetute modifiche e integrazioni nel corso degli anni, alcune delle quali particolarmente incisive. L'attenzione alla cittadinanza digitale è stata evidenziata dalla riforma di riorganizzazione delle pubbliche amministrazioni recata dalla cosiddetta "legge Madia", la cui *ratio* consiste proprio nello spostamento di prospettiva dalla digitalizzazione delle amministrazioni ai diritti digitali dei cittadini: l'art. 1 della legge delega 124/2015 e i relativi d.lgs. n. 179/2016 e d. lgs. n. 217/2017 esprimono l'intenzione del legislatore di fortificare e rendere effettivi i diritti digitali nei confronti delle amministrazioni, modificando e integrando il Codice nella direzione del rafforzamento della cittadinanza digitale[8].

Il Codice, pertanto, rende centrale il paradigma della cittadinanza digitale, alla luce del quale declina il rapporto con i pubblici poteri. Nonostante l'assoluta centralità in materia, l'amministrazione digitale non esaurisce le proprie disposizioni di riferimento nel Codice, ma rilevano ulteriori norme: alcune maggiormente settoriali, altre trasversali; in particolare, il Codice è integrato dalla normativa in materia di trasparenza e, in specifico, dal d.lgs. 33/2013, come modificato dalla profonda riforma del d.lgs. 97/2016[9]: nell'art. 1 del d.lgs. 33/2013 viene esplicitamente chiarito che la trasparenza concorre alla realizzazione di un'amministrazione aperta, al servizio del cittadino. Il collegamento tra le due anime emerge con chiarezza nella riforma in materia di riorganizzazione delle pubbliche amministrazioni, recata dalla legge 124/2015, che contiene al suo interno sia la delega alle modifiche e integrazioni del d.lgs. 82/2005 (art. 1), attuata con il d.lgs. 179/2016 e il d.lgs. 217/2017, sia la delega alla riforma del d.lgs. 33/2013 (art. 7), attuata con il

[8] La sezione II del capo I del CAD, dedicata ai diritti dei cittadini, è significativamente rubricata proprio con l'espressione «*Carta della cittadinanza digitale*».

[9] Il d.lgs. 33/2013 è stato approvato in attuazione della legge 190/2012 (cosiddetta legge Anticorruzione) e ha riordinato le disposizioni in materia di pubblicità, trasparenza e diffusione delle informazioni. Secondo CALZOLAIO, Digital (and privacy) by default. *L'identità costituzionale della amministrazione digitale*, in *Giornale di storia costituzionale*, fasc. 31, 2016, 190-192 la disciplina sulla trasparenza «non è che la più rilevante e vistosa etero-disciplina dell'amministrazione digitale rispetto al CAD».

d.lgs. 97/2016, cosiddetto *Freedom of Information Act* italiano, la cui novità più significativa riguarda proprio l'ampiezza del diritto a conoscere[10].

La connessione tra le due direttrici di riforma della pubblica amministrazione, costituite dalla digitalizzazione e dalla trasparenza, discende dalla centralità assunta dai dati, che a sua volta esige la protezione e la sicurezza dei dati stessi e la correlata tutela assicurata dal regolamento (UE) 2016/679 e dal d.lgs. 196/2003, come modificato dal d.lgs. 101/2018[11]; il processo di digitalizzazione, *disclosure* e apertura realizza, infatti, anche un significativo ed esteso fenomeno di trattamento di dati[12].

Le norme in materia di protezione dei dati personali conducono a una digitalizzazione che non solo si sposa a trasparenza e apertura, ma che cambia "pelle" e che già *by design* e *by default*[13] deve essere capace di tutelare i dati personali, proteggendo in modo preventivo tale diritto fondamentale della persona, rafforzando l'*accountability*, garantendo la sicurezza e definendo obblighi e responsabilità dei titolari del trattamento, ossia le pubbliche amministrazioni[14].

Pertanto, sotto la spinta evolutiva della società di riferimento, nel quadro normativo l'amministrazione pubblica muta nella rinnovata fisionomia dei diritti di riferimento della cittadinanza digitale: diritto all'uso delle tecnologie, diritto a conoscere, diritto alla protezione dei dati personali. Alla luce delle riforme e in considerazione dell'emersione delle anime costituite da digitalizzazione, trasparenza e *data protection*, determinate dalla relativa affermazione

[10] Secondo CARDARELLI, *Amministrazione digitale, trasparenza e principio di legalità*, in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2015, 227 ss. un «nucleo normativo su cui poggia l'amministrazione digitale si è articolato sulla declinazione positiva ed applicativa del principio di trasparenza».

[11] Secondo CALZOLAIO, *op. cit.*, p. 185 ss. dall'interazione tra i due processi di riforma costituiti da una parte dalla digitalizzazione, dalla semplificazione amministrativa e dalla trasparenza (cosiddetta legge Madia) e dall'altra dalla protezione e sicurezza dei dati (il "pacchetto europeo" di protezione dei dati personali) «emerge l'identità costituzionale dell'amministrazione digitale».

[12] Lo stesso art. 2, comma 5, d.lgs. 82/2005 prevede che le disposizioni del Codice «*si applicano nel rispetto della disciplina in materia di trattamento dei dati personali e, in particolare, delle disposizioni del Codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196*».

[13] Art. 25, reg. (UE) 2016/679.

[14] Artt. 24 e 32, reg. (UE) 2016/679.

dei diritti digitali di cui sono espressione, negli ultimi anni il volto dell'amministrazione pubblica matura sotto alcune significative linee direttrici.

In primo luogo, l'amministrazione pubblica matura sotto il profilo della *data governance* mostrando un connubio tra digitalizzazione, trasparenza e apertura in linea con la tendenza alla circolazione dei dati per i benefici di cui è latrice. L'amministrazione si caratterizza per una maggiore apertura verso la collettività, cui sono conferiti strumenti di accesso più ampi ed incisivi capaci di dare vita ad una vera e propria *freedom of information* e di garantire non solo la conoscenza, ma anche il riutilizzo del patrimonio informativo pubblico grazie agli *open data*.

In tale evoluzione i principi di digitalizzazione, trasparenza e apertura si pongono come cardini del nuovo modello di governo che emerge dalla recente evoluzione normativa. In particolare la profonda riforma che ha interessato il d.lgs. 82/2005, realizzata con la legge delega 124/2015, attuata dai relativi d.lgs. 179/2016 e d.lgs. 217/2017, ha previsto tra i criteri ispiratori, accanto ai principi *digital by default* e *digital first*, proprio la «*realizzazione di un'amministrazione digitale e aperta*»[15], che ha declinato nel rafforzamento dei principi di trasparenza, partecipazione e collaborazione; la riforma espressamente pone come propria finalità principale garantire a cittadini e imprese «*il diritto di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale*»[16]. Del resto il connubio tra trasparenza e digitalizzazione è *in nuce* al concetto stesso di *disclosure*, dal momento che gli strumenti digitali e la rete, con le sue caratteristiche intrinseche di ubiquità, semplicità e immediatezza nella diffusione, favoriscono ontologicamente la trasparenza.

La *disclosure* assurge a fattore fondamentale nella riforma delle istituzioni per il suo essere strumentale alla conoscenza e, altresì, per riuscire a creare maggiore simmetria fra governanti e governati, permettendo controllo e partecipazione "dal basso", contrastando possibili squilibri. Di conseguenza, l'amministrazione, che nel suo operare deve essere digitale, è tenuta a porsi, altresì, in modo ontologicamente trasparente.

[15] Art. 1, comma 1, lett. n), legge 124/2015.
[16] Art. 1, comma 1, legge 124/2015.

Il principio di trasparenza si è evoluto anche a seguito dello sviluppo della società di riferimento e dei suoi paradigmi sotto la spinta delle nuove tecnologie: *disclosure* e *openness* si sono integrate a definire un nuovo modello di *open government*. Di conseguenza, nel quadro normativo vigente la trasparenza si collega, altresì, in modo significativo con l'apertura: non è sufficiente una conoscenza "passiva" delle informazioni, dei dati e dei documenti resi disponibili, seppur maggiormente ampia e incisiva, ma si configura il bisogno di una trasparenza "attiva", realizzata con il riutilizzo dei dati messi a disposizione, grazie agli *open data*.

Accanto a questo mutamento che lega digitalizzazione, trasparenza e apertura, nell'evoluzione normativa la digitalizzazione si "radicalizza" e, oltre ai criteri ispiratori *digital by default* e *digital first*, evolve verso il principio di esclusività digitale, una sorta di *digital only*, ossia la previsione di un vero e proprio *switch off* dall'analogico al digitale. Per disegnare il volto delle istituzioni pubbliche e costruire i servizi online, il percorso di evoluzione normativa che ha interessato il CAD ha previsto tra i criteri ispiratori dell'amministrazione digitale i significativi principi *digital by default* e *digital first*, di cui alla legge delega 124/2015, attuata dai relativi d.lgs. 179/2016 e d.lgs. 217/2017. L'art. 1, comma 1, lett. b), legge 124/2015 prevede la ridefinizione e la semplificazione dei procedimenti amministrativi, in relazione alle esigenze di celerità, certezza dei tempi e trasparenza nei confronti dei cittadini e delle imprese «*mediante una disciplina basata sulla loro digitalizzazione e per la piena realizzazione del principio "innanzitutto digitale" (digital first)*»[17]. Nella prima parte della disposizione può essere letto il principio *digital by default*, ossia la modalità digitale per impostazione predefinita, e nella seconda il principio *digital first*, fondato sulla preferenza per la modalità digitale più che sull'esclusività della stessa.

[17] Secondo CARLONI, *Tendenze recenti e nuovi principi della digitalizzazione pubblica*, in *Giornale di diritto amministrativo*, fasc. 2, 2015, 153 ss. anche se a volte il principio *digital first* sembra qualificarsi nei termini di un passaggio all'esclusività digitale, va inteso come «proiezione verso la piena e prioritaria digitalizzazione dei servizi, con una loro articolazione centrata sulla loro erogazione digitale prima ancora che secondo modalità tradizionali, senza che resti esclusa questa possibilità» (pp. 155-156). Secondo l'Autore il principio coincide, di conseguenza, con il principio *digital by default* ed è contiguo al principio di esclusività digitale, che parimenti plasma le politiche recenti e si basa su meccanismi di *switch off*.

I principi *digital first* e *digital by default* si pongono come criteri ispiratori del processo di digitalizzazione dell'amministrazione pubblica e si distinguono dal principio di esclusività digitale, ossia un vero e proprio *switch off* verso l'esclusivo utilizzo di modalità digitali, da considerare come ipotesi eccezionale che necessita di un'esplicita previsione normativa[18]. Nonostante la rilevanza dei principi *digital first* e *digital by default* si scorge un'interessante evoluzione successiva operata dal d.lgs. 217/2017[19] e anche, da ultimo, dal d.l. 76/2020, convertito con modificazioni dalla legge 120/2020, che hanno riformato il d.lgs. 82/2005.

In aspetti strategici e cruciali, infatti, a seguito delle modifiche del d.lgs. 217/2017, il Codice ricorre al principio di esclusività digitale e al relativo meccanismo di *switch off*, la cui attuazione concreta viene rimessa a norme secondarie: è il caso della previsione di comunicazioni esclusivamente digitali tra i soggetti ai quali si applica il CAD e i cittadini (art. 3-bis, comma 3-bis, d.lgs. 82/ 2005)[20] e dell'utilizzo esclusivo da parte dei soggetti ai quali si applica il CAD delle identità digitali ai fini dell'identificazione degli utenti dei propri servizi online (art. 64, comma 2-quater, d.lgs. 82/2005).

Pertanto, nel momento dell'identificazione informatica per accedere ai servizi online e nella disciplina del domicilio digitale e delle relative comunicazioni telematiche con i cittadini, aspetti essenziali del rapporto che lega amministrazioni pubbliche e collettività, la riforma pare ritenere "insufficiente" il principio guida del *digital first* e si spinge verso il principio di

[18] Cfr. CALZOLAIO, *op. cit.*, 194 ss.; CARLONI, *op. cit.*, 153 ss.; LEONE, *Il principio "digital first": obblighi e diritti in capo all'amministrazione e a tutela del cittadino. Note a margine dell'art. 1 della legge 124 del 2015*, in *GiustAmm.it*, fasc. 6, 2016, 1 ss.

[19] Il d.lgs. 217/2017, seppur nelle intenzioni "correttivo" del precedente d.lgs. 179/2016, da instradare di conseguenza nei principi della legge delega, pare superarne lo spirito e traghettare l'amministrazione in modo più deciso verso la digitalizzazione.

[20] «*Con decreto del Presidente del Consiglio dei ministri o del Ministro delegato per la semplificazione e la pubblica amministrazione, sentiti l'AgID e il Garante per la protezione dei dati personali e acquisito il parere della Conferenza unificata, è stabilita la data a decorrere dalla quale le comunicazioni tra i soggetti di cui all'articolo 2, comma 2, e coloro che non hanno provveduto a eleggere un domicilio digitale ai sensi del comma 1-bis, avvengono esclusivamente in forma elettronica*» (art. 3, comma 3-bis, d.lgs. 82/2005).

esclusività digitale, si indirizza verso un *digital only*, un vero *switch off*, affidato a norme secondarie deputate a prevederne modalità e tempi[21].

Il volto dell'amministrazione digitale *by default*, che lascia sopravvivere una fisionomia analogica se necessaria, evolve così tramite *switch off* verso una fisionomia esclusivamente digitale nel rapporto tra amministrazioni e cittadini digitali. In modo intuitivo le ragioni delle riforme si annidano nella necessità di garantire effettività alle norme e agli strumenti previsti, volendo assicurare concretezza a quel diritto all'identità digitale e al domicilio digitale, di cui all'art. 3-bis del d.lgs. 82/2005.

Il dovere delle amministrazioni pubbliche di rendere effettivo il diritto si estremizza provocando un'esclusività del mezzo e facendo diventare il diritto un dovere anche per i cittadini, con i connessi problemi che la norma non omette di considerare. Lo spettro consiste, infatti, nel *digital divide*, declinazione moderna della disuguaglianza, il cui superamento è necessario per affermare i diritti previsti.

Il mutamento del volto dell'amministrazione digitale non è soltanto nella trasparenza collegata all'apertura e nella tendenza all'esclusività, ma anche in un cambiamento profondo che riguarda "come" l'amministrazione digitale debba essere realizzata. La connessione tra le due direttrici di riforma della pubblica amministrazione, costituite dalla digitalizzazione e dalla trasparenza, deriva dalla centralità assunta dai dati, che a sua volta esige la protezione dei dati stessi e la correlata tutela assicurata dal regolamento (UE) 2016/679 e dal d.lgs. 196/2003, come modificato dal d.lgs. 101/2018.

Il regolamento europeo (UE) 2016/679 e il d.lgs. 101/2018, che ha adeguato alla regolazione europea il d.lgs. 196/2003, delineano un approccio sistematico, un atteggiamento proattivo e una ponderazione *ex ante* dell'impatto e dei rischi sulla *data protection*, grazie al principio di *accountability* (il titolare del trattamento è competente del rispetto dei principi previsti e deve essere in grado di comprovarlo)[22], al rilievo conferito alla sicurezza[23] e a una serie di prin-

[21] Su questa strada il d.l. 76/2020, convertito con modificazioni dalla legge 120/2020, che ha modificato il d.lgs. 82/2005 ha rafforzato questi aspetti, ponendo obblighi alle amministrazioni e conseguenze in caso di violazione delle norme stesse.
[22] Art. 5, par. 2, e art. 24, reg. (UE) 2016/679.
[23] Art. 32, reg. (UE) 2016/679.

cipi caratterizzanti la disciplina quali *data protection by design* e *by default*[24], accompagnati dal c.d. *Data Protection Impact Assessment*[25]. I principi *data protection by design* e *by default* conducono, infatti, a una digitalizzazione che cambia "pelle" e realizzano un concetto di protezione dei dati personali all'interno della stessa tecnologia, una *privacy* per impostazione predefinita: il diritto si serve della tecnologia per assicurare il suo rispetto e garantire la tutela della dignità e dello sviluppo della persona. L'approccio preventivo, trasparente e proattivo, che responsabilizza il titolare del trattamento, emerge anche da altri strumenti innovativi, quali la consultazione preventiva (art. 36), il *data breach* (artt. 33-34) e la figura del *Data Protection Officer* (art. 37)[26].

Di conseguenza la tendenza a una digitalizzazione non solo *by default*, ma quasi esclusiva in certi suoi gangli e a una trasparenza ampia e profonda deve

[24] Il principio *data protection by design* prevede che, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare debba mettere in atto «*misure tecniche e organizzative adeguate, quali la pseudonimizzazione*», «*volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati*», ai sensi dell'art. 25, par. 1, reg. (UE) 2016/679. A tale criterio si lega il principio *data protection by default*, di cui al par. 2 dell'art. 25 del reg. (UE) 2016/679: il titolare deve mettere in atto «*misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*».

[25] Il c.d. *Data Protection Impact Assessment* (DPIA) è previsto nell'art. 35 del regolamento (UE) 2016/679: quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali; una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

[26] La nomina del DPO è prevista con la funzione di garantire una corretta gestione dei dati in una serie di casi, uno dei quali è proprio il trattamento effettuato da un'autorità pubblica o da un organismo pubblico, eccetto le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali. Si tratta di una figura prevista con la funzione di garantire un corretto trattamento dei dati personali, sorvegliando il rispetto della normativa, fornendo consulenza al titolare o al responsabile del trattamento, cooperando e fungendo da punto di contatto per l'autorità di controllo.

allo stesso tempo mantenere al centro la persona, proteggendola nei suoi dati in modo preventivo, per impostazione predefinita: l'amministrazione pubblica deve essere *by default* e *by design* non solo digitale, trasparente e aperta, ma anche idonea a proteggere la persona e i suoi dati. Questo significa una poderosa opera di analisi e valutazione dei sistemi informativi, delle infrastrutture, degli strumenti e dei servizi nei quali prende forma l'amministrazione digitale per renderla *compliant* alle norme in materia di *data protection*, con le difficoltà dovute al complesso bilanciamento tra i sottesi diritti, il diritto a conoscere e il diritto a proteggere i propri dati, che ontologicamente rischiano di scontrarsi, dal momento che il primo si nutre di disponibilità e il secondo fa inevitabilmente leva sul controllo. In tale trasformazione, che richiede risorse finanziarie e umane, è necessario altresì garantire omogeneità al volto dell'amministrazione a livello nazionale.

Pertanto l'amministrazione pubblica è chiamata a tenere insieme istanze particolarmente diverse quali circolazione/apertura, da una parte, per rispondere alle istanze di digitalizzazione, trasparenza e apertura, ma anche protezione/controllo, dall'altra per garantire la tutela dei dati personali; per riuscire in questa opera di bilanciamento l'amministrazione deve impiegare strumenti che mirano a garantire prevedibilità e certezza del diritto, ma anche ad assicurare flessibilità e adattabilità per essere efficaci.

Le riforme europee e nazionali di riferimento in materia di protezione dei dati personali disegnano la *data protection* come profilo integrato nella digitalizzazione e nell'apertura, necessario al fine di garantire i diritti dei cittadini e la persona digitale, scopo della stessa normativa sull'amministrazione digitale.

Pertanto il volto dell'amministrazione pubblica muta parallelamente all'evoluzione dei diritti dei cittadini, che è tenuta a realizzare, e al concretizzarsi di quella cittadinanza digitale, che è chiamata a soddisfare e che esige di usare le tecnologie nel rapporto con le amministrazioni (art. 3, d.lgs. 82/2005), reclama un effettivo e ampio diritto a conoscere, che diventa anche diritto a riutilizzare informazioni e dati (artt. 3 e 7, d.lgs. 33/2013) e, allo stesso tempo, richiede il rispetto dei propri dati personali da parte della stessa amministrazione "responsabilizzata" dalla normativa di riferimento (rego-

lamento UE 2016/679 e d.lgs. 196/2003, come modificato dal d.lgs. 101/2018).

In tale contesto che mostra ontologicamente delle criticità nell'assicurare equilibrio tra istanze diverse, ma parimenti significative è opportuno soffermarsi sulle tecnologie emergenti come intelligenza artificiale e *blockchain*, dove queste problematiche dell'amministrazione pubblica e quindi anche della sanità digitale si estremizzano ulteriormente in conseguenza delle stesse caratteristiche tecniche di queste tecnologie e del faticoso adattamento delle norme in materia di *data protection* in tale contesto.

2. Il valore delle tecnologie emergenti e la tutela del diritto alla protezione dei dati personali

Alla luce dell'esaminata trasformazione che involge il volto dell'amministrazione e della sanità pubblica digitale, nella gestione dei dati emergono le tecnologie emergenti che caratterizzano la società odierna, come l'intelligenza artificiale, capace di trarre valore dai dati per mezzo di algoritmi al prezzo di un'ontologica opacità che rischia di travolgere il valore della trasparenza e il diritto alla comprensione, e la *blockchain*, definita *lex cryptographia*[27], che trasforma il modo di scambiarsi valore e muta i meccanismi di fiducia (detta per questo anche Internet *of value*)[28], di cui un'applicazione è lo *smart contract*, in cui norme giuridiche e regole informatiche si intersecano significativamente, determinando esigenze e problematiche inedite.

Nell'impiego di tali tecnologie emergenti da parte della sanità pubblica digitale, che si connota per i profili esaminati, risulta particolarmente complessa la protezione dei dati personali; emergono aspetti critici

[27] WRIGHT, DE FILIPPI, *Decentralized Blockchain Technology and the Rise of* Lex Cryptographia, in *https://ssrn.com/abstract=2580664*, 2015, 1-58.

[28] Se Internet ha trasformato il modo di scambiarsi informazioni e connettersi agli altri, la *blockchain* trasforma il modo di scambiarsi valore. Cfr. GIULIANO, *La blockchain e gli* smart contracts *nell'innovazione del diritto nel terzo millennio*, in *Il diritto dell'informazione e dell'informatica*, fasc. 6, 2018, 989 ss.; CASTELLANI, POMI, TIBERTI, TURATO, *Blockchain. Guida pratica tecnico giuridica all'uso*, Firenze, 2019, 16 ss.

dell'interazione tra tecnologia e diritto, ma non mancano strumenti utili per affrontarli, capaci di determinare un modello di governo della tecnologia in ambito pubblico, che sarà oggetto di analisi.

2.1. Intelligenza artificiale e *data protection*

L'intelligenza artificiale (IA) ha acquisito il ruolo di protagonista nella contemporanea società tecnologica, in considerazione delle possibilità che garantisce all'uomo[29]. Il termine intelligenza artificiale si riferisce alla capacità della macchina di «riprodurre o attuare operazioni tipiche delle funzioni cognitive umane, quali per esempio l'apprendimento, il *problem solving*, il riconoscimento di volti, la traduzione del linguaggio, etc.»[30]. L'Unione europea include nella definizione di IA i «sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi»: i sistemi basati sull'intelligenza artificiale possono consistere in «software che agiscono nel mondo virtuale (per esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale)» oppure «incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose)»[31]. In considerazione della sua applicabilità in contesti eterogenei, sono molteplici gli ambiti di utilizzo dell'IA, tra cui salute e medicina, in particolare nella diagnosi e nella cura delle malattie; esempio celebre al riguardo è Watson, sistema elaborato da IBM per l'assistenza nel settore sanitario, a supporto delle decisioni cliniche e quale strumento teso a risolvere problemi.

Nell'implementazione di soluzioni di IA in ambito pubblico devono essere tenute in debita considerazione le caratteristiche tecniche di riferimento.

---

[29] Dal 2010 l'intelligenza artificiale ha vissuto un'accelerazione nel suo sviluppo anche grazie alla convergenza di *big data*, *machine learning* e *cloud computing*; cfr. SARTOR (a cura di), *L'intelligenza artificiale e il diritto*, in *Rivista di filosofia del diritto*, fasc. 1, 2020, 65 ss.

[30] SIMONCINI, SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di Filosofia del diritto*, fasc. 1, 2019, 88.

[31] Comunicazione della Commissione europea «*L'intelligenza artificiale per l'Europa*», COM (2018)237 *final* del 25 aprile 2018.

L'autonomia, infatti, connota e differenzia l'intelligenza artificiale dalla logica dei software tradizionali, dove l'impostazione deterministica *if this*, *than that* indica un funzionamento del tutto predeterminato nel programma, che prevede gli *input* e gli *output*: in questo aspetto si scorge la natura "intelligente" della macchina, che è capace di apprendere attraverso i dati in modo autonomo. Nell'apprendimento automatico (*machine learning*), anziché fornire tutta la conoscenza alla macchina, l'uomo le fornisce un metodo di apprendimento, da applicare ai dati cui la macchina ha accesso, per estrarre automaticamente da quei dati le indicazioni su come svolgere il compito ad essa affidato[32]. A differenza degli algoritmi condizionali o deterministici (*if this*, *than that*), che si limitano ad applicare regole informatiche predefinite ed espresse in linguaggio di programmazione, negli algoritmi di *machine learning* e *deep learning* l'intelligenza artificiale stessa estrapola le nozioni necessarie per l'assunzione di una determinazione, analizzando grandi quantità di dati ed apprendendo da questi i parametri numerici (la rappresentazione matematico-numerica, il cosiddetto modello, generato nella fase di apprendimento o *training*), necessari per adottare decisioni e utilizzarli nella successiva fase di esecuzione; il modello solitamente non è direttamente intelligibile da parte dell'essere umano (*black box*), aspetto che rileva particolarmente sotto la lente giuridica[33].

Pertanto, il concetto di intelligenza artificiale abbraccia al suo interno sistemi molto eterogenei, che però presentano alcune caratteristiche tecniche comuni: per sviluppare soluzioni di intelligenza artificiale sono necessari ingenti volumi di dati, che sono elaborati da algoritmi, al fine di raggiungere il risultato cui sono rivolte. *Big data* e algoritmi, potenziati dal *cloud*, sono gli elementi fondamentali che danno vita all'intelligenza artificiale[34].

---

[32] LAGIOIA, SARTOR, *L'intelligenza artificiale per i diritti dei cittadini: il progetto Claudette*, in *Ragion pratica*, fasc. 1, 2020, 88 ss.: negli anni più recenti hanno avuto particolare rilevanza le tecniche di apprendimento profondo (*deep learning*), basate su reti neurali a molti strati, che riproducono alcune caratteristiche astratte del cervello umano.

[33] Cfr. CARULLO, *Decisione amministrativa e intelligenza artificiale*, in *Il diritto dell'informazione e dell'informatica*, fasc. 3, 2021, 434 ss.

[34] La stessa Unione europea evidenzia che l'intelligenza artificiale combina dati, algoritmi e potenza di calcolo nel «*Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*», COM(2020) 65 *final* del 19 febbraio 2020.

Nelle caratteristiche stesse di funzionamento di *big data* e algoritmi emergono criticità ontologiche che rischiano di minare i fondamenti stessi del *framework* giuridico europeo in materia di *data governance*, teso ad una protezione effettiva ed efficace dell'individuo, dal momento che rischiano di scontrarsi apertamente con alcuni principi fondamentali della disciplina, finalizzati a garantire il rispetto della persona e della sua libertà di autodeterminazione.

L'intelligenza artificiale si basa su elaborazioni e inferenze distanti dal ragionamento umano e ha bisogno di un'enorme mole eterogenea di dati per condurre a risultati significativi: una maggiore quantità di dati, infatti, rende maggiormente accurate le relazioni tra gli stessi. Di conseguenza, può risultare complesso il rispetto del principio di limitazione della finalità, che prevede la raccolta dei dati personali per finalità determinate, esplicite e legittime e il successivo trattamento in modo che non sia incompatibile con tali finalità[35]. Il volume dei dati, la varietà delle fonti e il modo di operare degli algoritmi rendono, inoltre, difficile il rispetto del criterio di minimizzazione dei dati e dei relativi principi di adeguatezza, pertinenza e limitazione dei dati personali a quanto necessario rispetto alle finalità del trattamento e rischiano di inficiare qualità, esattezza e accuratezza dei dati[36]. Pertanto, i principi cardine della disciplina in materia di *data protection*, costituiti da limitazione della finalità, esattezza e minimizzazione dei dati, rischiano di essere depotenziati in tale contesto.

Il concetto di "dato personale", su cui si basa anche la dicotomia tra i regolamenti europei 2016/679 e 2018/1807, dedicati rispettivamente alla protezione dei dati personali e alla libera circolazione dei dati non personali, può risultare insufficiente, dal momento che i dati afferenti a gruppi o comunità, appartenenti quindi a più persone, oltre ai metadati e ai dati inferiti, possono risultare estremamente significativi nel contesto dei *big data* nell'identificazione della persona o quanto meno nell'impatto sulla stessa, determinando l'esigenza della correlata tutela[37]. Gli stessi dati anonimi possono non rimanere tali e le tecniche di anonimizzazione possono sollevare

[35] Art. 5, par. 1, lett. b), reg. (UE) 2016/679.
[36] Art. 5, par. 1, lett. c) reg. (UE) 2016/679.
[37] Cfr. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Bologna, 2015, 28 ss.

criticità: il pericolo sta nelle inferenze che possono essere tratte, grazie anche alla disponibilità di dati ausiliari riferibili alla persona: ogni dato può finire per essere identificativo e quindi personale, soprattutto nel tempo e nelle correlazioni tra moltitudini di dati diversi[38].

Nell'universo dei "grandi dati" vacilla nella sostanza anche il paradigma basato sulla trasparenza, sull'informativa da parte del titolare del trattamento[39] e sul consenso libero, preventivo, specifico, inequivocabile e revocabile dell'interessato[40]: proprio per le esaminate caratteristiche distintive, il funzionamento degli algoritmi può rendere complesso ricostruire i passaggi logici e motivare le conclusioni cui arrivano ed è dubbio che in tale contesto le informazioni rese siano capaci di fornire una conoscenza completa e profonda sul trattamento, sul funzionamento degli algoritmi, sull'impatto e sulle conseguenze sulla persona e che, di conseguenza, il consenso possa considerarsi libero. Pertanto ciò può inficiare la trasparenza e l'apertura che connotano il volto dell'amministrazione e della sanità pubblica quando impiegano tale tecnologia.

La qualificazione del consenso individuale come elemento capace di legittimare il trattamento e perfino, laddove esplicito, il processo decisionale automatizzato è particolarmente dubbia[41]: il consenso preventivo, libero ed esplicito può essere ottenuto a fronte di vantaggi perseguibili e perdere così le caratteristiche che devono connotarlo[42]. La condizione dell'individuo rischia di essere una libertà apparente e non autentica, dal momento che il mancato consenso espone all'indubbio pregiudizio di non fruire delle possibilità offerte dai servizi digitali offerti: al riguardo, è particolarmente significativo il considerando 42, secondo cui «*il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare*

[38] Cfr. D'ACQUISTO, NALDI, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017, 34 ss.
[39] Artt. 12-14, reg. (UE) 2016/679.
[40] Art. 7, reg. (UE) 2016/679. Cfr. CATE, MAYER-SCHÖNBERGER, *Notice and consent in a world of Big Data*, in *International Data Privacy Law*, vol. 3, n. 2, 2013, 67-73.
[41] Artt. 7 e 22, reg. (UE) 2016/679.
[42] Cfr. COLANGELO, Big data*, piattaforme e antitrust*, in *Mercato Concorrenza Regole*, fasc. 3, 2016, 448 ss.

una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio».

Nella consapevolezza di tali profonde criticità, che rischiano di minare le basi stesse del quadro giuridico di riferimento, alcuni principi della disciplina europea in materia di *data protection* sono maggiormente adeguati all'intelligenza artificiale. In particolare possono essere letti sotto tale ottica i principi *data protection by design* e *by default*, previsti nell'art. 25, paragrafi 1 e 2, accompagnati dal *data protection impact assessment*, regolato nell'art. 35 del regolamento (UE) 2016/ 679[43]. Tali disposizioni prevedono che il diritto si serva della tecnologia per garantire *by design* e *by default* il rispetto delle norme e danno forma a un approccio proattivo e a una valutazione preventiva dell'impatto e dei rischi dei trattamenti sulla *data protection*. L'approccio proattivo è presente anche in altri strumenti, come la consultazione preventiva (art. 36)[44], il *data breach* (artt. 33-34)[45], la logica di *accountability* e responsabilizzazione dei soggetti che trattano i dati personali (art. 24), la figura del *Data Protection Officer* (DPO) (artt. 37-39) e la previsione della contitolarità, accompagnata dalla definizione delle rispettive responsabilità (art. 26), disposizioni coadiuvate sia dall'attenzione alla sicurezza (art. 32), sia dall'effettività e dall'efficacia del sistema sanzionatorio (artt. 82-84).

---

[43] La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti, che paiono alludere ai *big data*: «*a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche*; *b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10*; *c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*».

[44] Il titolare, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio.

[45] Il titolare del trattamento ha l'obbligo di notificare eventuali violazioni dei dati personali all'autorità di controllo nei tempi e nelle modalità previste e, se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, deve comunicare la violazione all'interessato senza ingiustificato ritardo, tranne nei casi previsti dalla norma.

Tali norme si attagliano in modo efficace alla filiera di soggetti diversi che spesso caratterizza la gestione di soluzioni di intelligenza artificiale.

Al riguardo rileva particolarmente l'art. 22 del regolamento (UE) 2016/679, dedicato al «*processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*», che attribuisce all'interessato «*il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*»[46]. La portata del diritto, però, viene ridotta nel paragrafo 2 della norma, dal momento che la disposizione non si applica al verificarsi di alcune ampie condizioni, in particolare laddove la decisione sia necessaria per la conclusione o l'esecuzione di un contratto, sia autorizzata dal diritto europeo o nazionale (che deve precisare altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato) o si basi sul consenso esplicito dell'interessato, che anche in tale contesto, seppur rafforzato nel suo dover essere "esplicito", è ritenuto dalla normativa strumento capace di legittimare il trattamento (strumento che in realtà può essere improprio, come sopra esaminato).

Nel caso del consenso esplicito e in quello di necessità per la conclusione o l'esecuzione del contratto, la norma bilancia le eccezioni obbligando il titolare del trattamento ad attuare comunque «*misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione*»[47]. Pertanto, in tali fattispecie il diritto "si attenua" e prende la forma del diritto di esigere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione, che necessita della possibilità di conoscere i dati utilizzati e gli algoritmi impiegati; emergono però anche in tal caso le difficoltà scaturenti dalle caratteristiche tecniche, in particolare il funzionamento degli algoritmi, che può rendere difficile comprendere le decisioni e, di conseguenza, contestarle.

[46] Rileva anche il relativo considerando 71.
[47] Art. 22, par. 3, reg. (UE) 2016/679.

2.2.*Blockchain* e *data protection*

Accanto all'intelligenza artificiale, anche l'impiego della *blockchain* in ambito sanitario pubblico può destare problemi nella concreta applicazione della normativa in materia di *data protection*.

La *blockchain* è una tecnologia in grado di trasformare il modo di scambiarsi valore, la gestione delle transazioni e i meccanismi di fiducia: la *blockchain* è foriera di un mutamento potenzialmente *disruptive*[48]; in tal caso, significativamente a livello lessicale si parla di *lex cryptographia*[49].

La *blockchain* è una *species* del *genus* delle *distributed ledger technologies* (DLT), ossia tecnologie di registro distribuito e disintermediato *peer-to-peer*, in cui le voci del *database* sono replicate in una serie di nodi e la regolazione avviene mediante meccanismi di consenso condiviso; le DLT si distinguono dalle architetture centralizzate *client-server*, basate invece sul controllo di un'autorità di gestione. In specifico la *blockchain* consiste in una "catena di blocchi", ciascuno contenente una o più transazioni: i dati, inseriti per mezzo di crittografia asimmetrica, sono allocati in blocchi, accompagnati da *hash* e *timestamp*, concatenati tra loro attraverso il richiamo dell'*hash* del blocco precedente in quello successivo[50]; questo aspetto determina la caratteristica dell'immutabilità unilaterale[51]. Ogni nuovo blocco è validato da alcuni nodi (cosiddetti *miners*) per mezzo della risoluzione di un problema matematico complesso, che vale una ricompensa; tale meccanismo incentiva la corretta validazione dei blocchi[52]. Le transazioni sono validate con il consen-

[48] Cfr. GIULIANO, *op. cit.*, 989 ss.; CASTELLANI, POMI, TIBERTI, TURATO, *op. cit.*, 16 ss.
[49] WRIGHT, DE FILIPPI, *op. cit.*, 1-58.
[50] Dato che ogni *hash* contiene l'*hash* del blocco precedente, il tentativo di modificare un blocco comporterebbe la modifica di tutti quelli successivi, determinando una "rottura" della catena.
[51] L'immodificabilità deve essere intesa da un punto di vista unilaterale (un singolo da solo non può modificare i dati), ma non è una caratteristica valida in assoluto: laddove si pervenisse a un controllo sulla maggioranza del consenso la modifica diventerebbe possibile; cfr. PALLADINO, *L'equilibrio perduto della blockchain tra* platform revolution *e* GDPR compliance, in *Rivista di diritto dei media*, fasc. 2, 2019, 152 ss.
[52] La risoluzione del problema matematico richiede un notevole impiego di capacità computazionale e di energia. Cfr. GIULIANO, *op. cit.*, 989 ss.; PAROLA, MERATI,

so della maggioranza degli utenti; i meccanismi di consenso sono diversi[53]: *Proof of Work* (utilizzato da Bitcoin), *Proof of Stake*, etc.

Pertanto la tecnologia *blockchain*, in modo immutabile, conserva la memoria storica delle transazioni e, in modo distribuito e paritetico, garantisce a ciascun partecipante una copia di ciascuna operazione: in tal modo sono garantite sicurezza e resistenza rispetto a potenziali attacchi[54]. Di conseguenza la *blockchain* è assimilabile a un registro o a un libro mastro digitale, che non necessita di un intermediario o di un soggetto terzo certificatore[55]; il controllo distribuito si sostituisce al paradigma tradizionale, in cui la certezza è garantita da un terzo, che controlla la transazione e che ne assume la responsabilità[56].

Pertanto, volendo individuare i tratti distintivi, le caratteristiche principali della *blockchain* sono costituite da disintermediazione, decentralizzazione, distribuzione e vocazione transnazionale; immutabilità, inalterabilità e persistenza dei dati; meccanismo distribuito *peer-to-peer* di consenso, fiducia e incentivazione; trasparenza, tracciabilità e sicurezza; funzioni di *hash*, validazione temporale e crittografia asimmetrica[57].

GAVOTTI, Blockchain *e* smart contract*: questioni giuridiche aperte*, in *I Contratti*, fasc. 6, 2018, 681; GAMBINO, BOMPREZZI, *Blockchain e protezione dei dati personali*, in *Il diritto dell'informazione e dell'informatica*, fasc. 3, 2019, 619 ss.; PIRANI, *Gli strumenti della finanza disintermediata:* Initial Coin Offering *e* blockchain, in *Analisi Giuridica dell'Economia*, fasc. 1, 2019, 329 ss.; LEMME, *Gli* smart contracts *e le tre leggi della robotica*, in *Analisi Giuridica dell'Economia*, fasc. 1, 2019, 129 ss.

[53] Per una rassegna dei meccanismi di consenso si rinvia a SARZANA DI S. IPPOLITO, NICOTRA, *Diritto della blockchain, intelligenza artificiale e IoT*, Milano, 2018, 26 ss.

[54] Cfr. WRIGHT, DE FILIPPI, *op. cit.*, 1-58.

[55] Al riguardo, come sottolinea GAMBINO, *Vizi e virtù del diritto computazionale*, in *Il diritto dell'informazione e dell'informatica*, fasc. 6, 2019, 1169 ss., «la *blockchain* permette di ottenere la fiducia e l'affidabilità che nel passato erano necessariamente legate ad una figura terza, un notaio o un pubblico ufficiale».

[56] Le transazioni possono avere ad oggetto dati oppure beni, sotto forma di *token*, ossia *asset* digitali, che rappresentano un insieme di diritti e che possono esistere solo in forma digitale o essere la rappresentazione digitale di un altro *asset;* i *token* sono rappresentazioni digitali di diritti relativi a beni, corporali e incorporali, a crediti o a titoli; cfr. CAPPIELLO, *Dallo "*smart contract*"* computer code *allo* smart (legal) contract*. I nuovi strumenti (para)giuridici alla luce della normativa nazionale e del diritto internazionale privato europeo: prospettive* de jure condendo, in *Diritto del commercio internazionale*, fasc. 2, 2020, 477 ss.

[57] Si tratta di un sistema a doppia chiave pubblica e privata: la chiave privata è conosciuta e utilizzata dal soggetto titolare per cifrare i dati e la chiave pubblica è utilizzata dal

Nelle differenti tipologie di *blockchain* tali aspetti si declinano in maniera parzialmente diversa: le *blockchains permissionless* o *unpermissioned* o pubbliche si distinguono per essere aperte e liberamente accessibili da chiunque senza autorizzazioni (es. Bitcoin ed Ethereum[58]); le *blockchains permissioned* o private sono chiuse e non accessibili pubblicamente, dal momento che le autorizzazioni sono gestite da un'autorità centrale e, pertanto, prevedono una forma di *governance*[59]; le *blockchains ibride*, dette altresì consorzi, sono parzialmente decentrate, dal momento che esiste un controllo sul meccanismo di consenso da parte di alcuni nodi preselezionati, che hanno maggiore influenza degli altri.

In tale contesto, lo *smart contract* è un'applicazione significativa della *blockchain*, foriera di numerose applicazioni, in cui regole informatiche e norme giuridiche si intersecano significativamente[60]. Nello *smart contract*, evoluzione "intelligente" del contratto, infatti, nel momento in cui sono soddisfatte le condizioni contrattuali tradotte dal codice informatico nel lin-

---

destinatario per decifrare i dati e verificare l'utente (ciò non consente la diretta riferibilità all'identità del soggetto, in particolare nelle *permissionless*); le due chiavi sono correlate e indipendenti.

[58] Bitcoin è la prima applicazione pratica della tecnologia *blockchain*, impiegata per la creazione di una moneta elettronica basata su un protocollo decentralizzato *peer-to-peer*; cfr. NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, in *bitcoin.org*, 2008. Ethereum è un protocollo con lo scopo principale di fornire una piattaforma *open source* per incentivare lo sviluppo di applicazioni decentralizzate (*decentralized applications* – DApps), come gli *smart contracts*; cfr. BUTERIN, *Ethereum White Paper. A next generation smart contract & decentralized application platform*, in *https://ethereum.org*, 2013, 1-37.

[59] Cfr. GIULIANO, *op. cit.*, 989 ss.; GAMBINO, BOMPREZZI, *op. cit.*, 619 ss., secondo i quali gli aspetti principali di differenza tra *blockchains permissionless* e *permissioned* consistono nei seguenti: identificabilità dei soggetti; modalità di selezione dei nodi e grandezza della rete; meccanismo di consenso condiviso; trasparenza del contenuto dei blocchi. La distinzione tra *blockchains* pubbliche e private fa riferimento alla gestione dell'infrastruttura informatica: le pubbliche non sono gestite da nessuno, le private invece sono gestite da una persona, da un'organizzazione o da un gruppo di individui. Seppur in tale contributo siano usati come sinonimi, nella letteratura in materia non manca chi precisa che, mentre la distinzione tra *blockchains* pubbliche e private si riferisce alla possibilità di accesso ai dati, la differenza tra *permissionless* e *permissioned* riguarda più propriamente la possibilità di "scrivere" nel registro.

[60] Cfr. SZABO, *Smart Contracts: Building Blocks for Digital Markets*, in *EXTROPY: The Journal of Transhumanist Thought*, 16, 18, 1996, 2 ss.; SZABO, *The idea of Smart Contracts*, in *Nick Szabo's Papers and Concise Tutorials*, 6, 1997; SZABO, *Formalizing and Securing Relationships on Public Networks*, in *First Monday*, vol. 2, n. 9, 1997.

guaggio macchina, si attivano automaticamente gli effetti conseguenti con le caratteristiche tipiche della *blockchain*, in particolare l'immutabilità e l'irreversibilità: gli effetti contrattuali si eseguono automaticamente al verificarsi delle condizioni predeterminate dalle parti e descritte sotto forma di codice informatico secondo la logica "*if this then that*"[61]; tramite una sorta di sillogismo giuridico si determina così un meccanismo di *self-enforcement* delle regole[62]. Proprio in ragione del suo funzionamento, si parla di contratto "intelligente", capace di eseguirsi automaticamente in modo deterministico.

Le caratteristiche tecniche distintive della *blockchain* e degli *smart contracts*, quali inalterabilità, tracciabilità e sicurezza, le rendono applicabili proficuamente in molteplici settori in ambito pubblico, tra cui la sanità, ma allo stesso tempo determinano una difficile interazione con la disciplina in materia di protezione dei dati personali[63]. La difficoltà di tale interazione può aggravarsi in caso di impiego in ambito sanitario, come sarà esaminato di seguito.

Sotto il profilo della *data protection*, infatti, le caratteristiche tecniche distintive della *blockchain*, punti di forza di tale tecnologia, rischiano di trasformarsi in punti di debolezza, capaci di creare criticità nel rispetto dei principi e delle norme previste[64].

---

[61] Il determinarsi degli effetti può dipendere da elementi interni al codice (es. una data, un termine, etc.) o da circostanze esterne; in tale ultimo caso interviene una fonte di informazione esterna, un "oracolo", che interpreta la realtà esterna e permette di verificare se siano soddisfatte le clausole previste (es. le condizioni atmosferiche, l'avvenuta consegna di un bene, l'orario di un mezzo di trasporto, etc.). Cfr. PAROLA, MERATI, GAVOTTI, *op. cit.*, 683 ss.; SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 94 ss.

[62] Cfr. PARDOLESI, DAVOLA, Smart contract*. Lusinghe ed equivoci dell'innovazione purchessia*, in *Il Foro Italiano*, fasc. 4/5, 2019, 195 ss.; GAMBINO, STAZI, MULA, *Diritto dell'informatica e della comunicazione*, III ed., Torino, 2019, 182 ss.

[63] Al riguardo cfr., *inter alia*, BERBERICH, STEINER, *Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?*, in *European Data Protection Law Review*, fasc. 3, 2016, 422-426; MOEREL, *Blockchain & Data Protection…and Why They Are Not on a Collision Course*, in *European Review of Private Law*, fasc. 6, 2019, 825-852.

[64] Cfr. GAMBINO, BOMPREZZI, *op. cit.*, 619 ss.; PALLADINO, *op. cit*., 153 ss. In merito cfr. lo studio «*Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?*» dell'*European Parliamentary Research Service* (EPRS), completato nel luglio 2019, e il documento «*Solutions for a*

Nella tecnologia *blockchain* la funzione di *hash*, snodo cruciale del funzionamento, può essere qualificata come un'operazione di pseudonimizzazione[65], che come tale comporta l'applicazione della normativa in materia di protezione dei dati personali[66]. A differenza dell'anonimizzazione, i dati restano personali a seguito della pseudonimizzazione, che costituisce una misura di sicurezza al fine di proteggere i dati oggetto di trattamento: la persona fisica è identificabile, dal momento che i dati non sono direttamente riconducibili alla persona, ma possono diventarlo con l'utilizzo di informazioni aggiuntive[67].

L'applicazione della normativa in materia di *data protection* in caso di utilizzo della *blockchain* comporta il necessario rispetto dei principi applicabili al trattamento dei dati personali previsti dal regolamento europeo 2016/679, in specifico dall'art. 5, tra i quali rilevano la minimizzazione dei dati[68] e la limitazione della conservazione[69]. Le difficoltà sorgono dal momento che la *blockchain* per il suo funzionamento replica i dati nei vari nodi, scontrandosi così con il principio di minimizzazione, e conserva i dati in modo perpetuo, confliggendo di conseguenza con il principio della limitazione della conservazione.

Oltre al rispetto dei principi previsti in materia, le caratteristiche della *blockchain* determinano ulteriori complesse problematiche in materia di pro-

---

responsible use of the blockchain in the context of personal data» della *Commission Nationale de l'Informatique et des Libertés* (CNIL), pubblicato nel novembre 2018.

[65] La pseudonimizzazione indica il trattamento che avviene in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile (art. 4, par. 1, n. 5, reg. UE 2016/679).

[66] In tal senso si esprime anche il Parlamento europeo nella risoluzione del 3 ottobre 2018.

[67] Cfr. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Rivista trimestrale di diritto e procedura civile*, fasc. 2, 2018, 441 ss.; GAMBINO, BOMPREZZI, *op. cit.*, 619 ss.; GIULIANO, *op. cit.*, 989 ss.

[68] Art. 5, par. 1, lett. c), reg. (UE) 2016/679, secondo cui i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

[69] Art. 5, par. 1, lett. e), reg. (UE) 2016/679, secondo cui i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

tezione dei dati personali, afferenti alla *governance* e all'applicazione normativa, in specifico relative all'individuazione delle figure soggettive e all'esercizio dei diritti dell'interessato.

La disciplina in tema di *data protection* individua alcune figure di riferimento, fondamentali ai fini della *governance* e dell'applicazione della disciplina normativa: accanto all'interessato, ossia la persona fisica identificata o identificabile, cui i dati personali si riferiscono[70], il titolare, ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, che, singolarmente o insieme ad altri titolari, determina le finalità e i mezzi del trattamento di dati personali, e il responsabile, ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, eventualmente preposto dal titolare, che tratta dati personali per suo conto[71].

L'individuazione di queste figure è determinante per l'attuazione della disciplina, dal momento che a tali soggetti si applicano obblighi a tutela della persona e dei suoi dati, come il principio fondamentale di responsabilizzazione, secondo cui il titolare è competente per il rispetto dei principi previsti e deve essere in grado di comprovarlo[72].

Sotto il profilo soggettivo, rileva la specifica tipologia di *blockchain*: nelle *permissioned* il titolare è individuabile nel soggetto che governa l'infrastruttura e nel caso dei consorzi si può fare leva sulla contitolarità del trattamento, ma nelle *permissionless* diventa complesso individuare tali figure, a causa delle caratteristiche di disintermediazione e distribuzione.

In tal caso sono state ipotizzate diverse ricostruzioni, che spaziano da chi decreta in tali casi l'assenza di titolari, con il conseguente problema di applicazione della disciplina[73], a chi suggerisce una preventiva individuazione del

[70] Art. 4, par. 1, n. 1), reg. (UE) 2016/679.
[71] Art. 4, par. 1, nn. 7) e 8), reg. (UE) 2016/679.
[72] Art. 5, par. 2, reg. (UE) 2016/679. Il titolare è tenuto a garantire *accountability* e sicurezza, ai sensi degli artt. 24 e 32, reg. (UE) 2016/679, dal momento che deve mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento.
[73] Cfr. GAMBINO, BOMPREZZI, *op. cit.*, 619 ss.; GIULIANO, *op. cit.*, 989 ss.

titolare[74] o a chi qualifica tutti i nodi come contitolari o responsabili o, ancora, titolari per sé e responsabili per gli altri[75]. In tale ipotesi, però, risulta difficile individuare la determinazione "congiunta" delle finalità e dei mezzi del trattamento posta come condizione normativa necessaria a qualificare i soggetti come contitolari[76]: si determina una conseguente difficoltosa individuazione pratica degli stessi e una correlata problematica distribuzione di responsabilità che rischia di compromettere l'efficacia della tutela[77]. Anche nella variante interpretativa che li prevede quali responsabili, questi lo sarebbero *de facto*, mancando il previsto atto di designazione da parte del titolare[78]. Un'altra interpretazione, invece, individua il titolare nello sviluppatore del software, ma anche questa posizione non convince perché in concreto tale soggetto può limitarsi a fornire la soluzione senza determinare finalità e mezzi del trattamento; in alcuni casi può elaborare dati per conto di un altro soggetto e atteggiarsi quale responsabile[79]. In tale contesto, risulta più convincente l'orientamento che suggerisce una preventiva individuazione del titolare, come lo studio in materia prodotto dall'*European Parliamentary Research Service*[80].

Non mancano problemi anche per quanto riguarda l'esercizio dei diritti dell'interessato, quali il diritto all'accesso a dati e informazioni (art. 15), il diritto di rettifica e integrazione (art. 16), il diritto alla cancellazione (diritto all'oblio) (art. 17), il diritto di limitazione di trattamento (art. 18), il diritto alla portabilità dei dati (art. 20), il diritto di opposizione al trattamento (art.

[74] In tal senso il citato studio «*Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?*» dell'*European Parliamentary Research Service* (EPRS), luglio 2019.
[75] In tal senso MAXWELL, SALMON, *A guide to blockchain and data protection*, Brussels, 2017, 11; FINCK, *Blockchains and Data Protection in the European Union*, in *European Data Protection Law Review*, fasc. 1, 2018, 17 ss.
[76] L'art. 26, reg. (UE) 2016/679 prevede la possibilità della contitolarità del trattamento, nel caso in cui due o più titolari determinino congiuntamente le finalità e i mezzi del trattamento.
[77] Cfr. PALLADINO, *op. cit.*,153 ss.
[78] Cfr. GAMBINO, BOMPREZZI, *op. cit.*, 619 ss.
[79] Cfr. GIULIANO, *op. cit.*, 989 ss.
[80] Lo studio «*Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?*» dell'*European Parliamentary Research Service* (EPRS), luglio 2019.

21) e il diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (art. 22). La difficoltà di individuazione del titolare, infatti, rischia di impedire l'effettivo esercizio dei diritti da parte dell'interessato, che sarà in difficoltà nell'identificazione del soggetto cui rivolgersi, designato dalla normativa come colui che deve assicurare effettività ai diritti stessi[81].

Inoltre, in considerazione delle caratteristiche di immodificabilità, inalterabilità e persistenza dei dati, in relazione alla tecnologia *blockchain* concretamente non risultano esercitabili i diritti di rettifica[82], limitazione e cancellazione dei dati stessi da parte dell'interessato, dal momento che tali diritti risultano sostanzialmente inattuabili a fronte delle specifiche caratteristiche tecniche della *blockchain*, in specifico l'immodificabilità. Come precisato in dottrina, in merito è opportuno operare una distinzione: riguardo ai diritti che prevedono aggiornamento, rettifica e integrazione, mantenendo la conservazione dei dati, la tecnologia *blockchain* rende complesso garantirne il rispetto, ma non osta necessariamente, dal momento che è possibile validare un nuovo blocco di dati contenente l'aggiornamento, la rettifica e l'integrazione operate dall'interessato, mentre i diritti che prevedono una demolizione del dato, quali cancellazione e limitazione di trattamento, risultano tendenzialmente inconciliabili con tale tecnologia, che si basa sull'immodificabilità e persistenza dei dati stessi[83].

Peraltro in questa tecnologia il procedimento porta alle conseguenze tramite automatismi: di conseguenza, può non risultare agevole neppure il rispetto del diritto dell'interessato a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato o, almeno, del diritto di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione[84]. Infine, la vocazione transnazionale della *blockchain*, unita alla

[81] Cfr. GAMBINO, BOMPREZZI, *op. cit.*, 619 ss.
[82] In tal senso FINCK, *op. cit.*, p. 21 ss. Proprio in considerazione del funzionamento, la rettifica dei dati è difficilmente esercitabile ed è possibile realizzarla solo con la creazione di un nuovo blocco che riporti la rettifica dei dati inseriti e validati; l'impossibilità di esercitare il diritto di rettifica si traduce, altresì, nel mancato rispetto del principio di esattezza, di cui all'art. 5, par. 1, lett. d), reg. (UE) 2016/679.
[83] PALLADINO, *op. cit.*, 155 ss.
[84] Si tratta di quanto previsto dall'art. 22, reg. (UE) 2016/679.

pseudonimizzazione, rende difficile stabilire il luogo del trattamento e la distribuzione dei nodi può allargarsi fuori dall'ambito territoriale europeo: emergono difficoltà concrete nell'applicazione della disciplina, che si estende anche fuori dai confini dell'Unione europea[85], e prendono vita dubbi in merito all'applicazione delle norme relative al trasferimento dei dati all'estero, prevista dal regolamento (UE) 2016/679[86].

Tali criticità giuridiche derivano direttamente dalle caratteristiche tecniche distintive della *blockchain*; più ampiamente, l'approccio concettuale del regolamento europeo in materia di *data protection*, che prevede un trattamento centralizzato dei dati personali fondato sul controllo e sulla responsabilizzazione, risulta faticosamente adattabile a una tecnologia che si caratterizza invece proprio per decentralizzazione, disintermediazione e distribuzione[87].

Un ambito che desta particolare interesse per l'utilizzo della *blockchain* è proprio quello della sanità, in considerazione dei vantaggi che garantisce tale tecnologia emergente. Al riguardo, però, i punti di frizione tra *blockchain* e *data protection* possono aggravarsi per la presenza di dati relativi alla salute[88], che rientrano nelle categorie particolari di dati personali[89], dal momento che in tal caso si eleva il livello di protezione giuridica alla luce della particolare invasività nella sfera intima della persona[90]. In questi casi, infatti, il regolamento europeo 2016/679 prevede la necessità di condizioni di liceità specifiche per effettuare il

---

[85] Il regolamento si applica «*al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione*» (art. 3, par. 2, reg. (UE) 2016/679).

[86] Cfr. PALLADINO, *op. cit.*,153 ss.; GIULIANO, *op. cit.*, 989 ss.

[87] Cfr. FINCK, *op. cit.*, 17 ss.; SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 68 ss.

[88] Ai sensi dell'art. 4, paragrafo 1, n. 15), reg. (UE) 2016/679 si tratta dei «*dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*».

[89] Si tratta dei dati personali idonei a rivelare «*l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale*», nonché «*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*», ai sensi dell'art. 9, par. 1, reg. (UE) 2016/679.

[90] Art. 4, par. 1, n. 15), e art. 9, reg. (UE) 2016/679.

trattamento, altrimenti di norma vietato, tra le quali il consenso esplicito, motivi di interesse pubblico rilevante, motivi di interesse pubblico nel settore della sanità pubblica, archiviazione nel pubblico interesse, ricerca scientifica o storica o a fini statistici[91]. In tali casi il trattamento deve avvenire alle condizioni e con le modalità previste dall'art. 9 del regolamento europeo.

In merito è attribuita agli Stati membri la possibilità di emanare disposizioni dettagliate, sia requisiti specifici per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, sia per mantenere o introdurre condizioni con riguardo a dati relativi alla salute[92]. Nella normativa italiana, adeguata alla regolazione europea, sono previste disposizioni riguardo a specifiche tipologie di dati negli articoli 2-sexies, 2-septies, 2-octies e 2-novies del d.lgs. 196/2003, come modificato dal d.lgs. 101/2018. In caso di trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante[93], si eleva il livello di protezione alla luce della particolare invasività e il relativo trattamento è ammesso qualora sia previsto dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento, 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[94]: il trattamento quindi deve essere legittimato da una fonte normativa che in modo espresso dettagli dati, operazioni e motivazione, oltre alle misure per tutelare i diritti fondamentali dell'interessato.

---

[91] Art. 9, par. 2, lett. a), g), i), j) reg. (UE) 2016/679.

[92] Considerando 10 e art. 9, par. 4, reg. (UE) 2016/679: «*Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute*».

[93] L'interesse pubblico rilevante è previsto nell'art. 9, par. 2, lett. g), reg. (UE) 2016/679: «*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*».

[94] Art. 2-sexies, comma 1, d.lgs. 196/2003, introdotto dal d.lgs. 101/2018. Il secondo comma, fermo quanto previsto nel primo comma, considera rilevanti una serie di interessi pubblici relativi a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle materie espressamente previste nel secondo comma.

In caso di dati genetici, biometrici e relativi alla salute il trattamento deve avvenire nel rispetto delle misure di garanzia disposte dal Garante, previste dall'art. 2-septies, d.lgs. 196/2003[95]; tali tipologie di dati personali non possono essere diffuse[96].

L'applicazione di norme e condizioni maggiormente stringenti per il trattamento di dati relativi alla salute può rendere maggiormente critici gli esaminati aspetti di frizione tra tecnologia e diritto, quali il complesso rispetto dei principi normativi, la difficile individuazione del titolare e il correlato complesso esercizio dei diritti da parte dell'interessato, ma al riguardo è necessario evidenziare che l'utilizzo della *blockchain* nel settore della sanità riserva anche numerosi punti di forza, che hanno motivato l'elaborazione di applicazioni interessanti, quali a titolo di esempio *My Health My Data*[97] e *Patientory*[98] per gestire e trasferire dati sanitari o *MedRec* relativo alle cartelle cliniche elettroniche[99].

In specifico, ferma restando la necessità di rispettare le condizioni specifiche previste, la *blockchain* può essere impiegata proficuamente in ambito sanitario, facendo leva sui punti di forza che la connotano e che possono rivelarsi di particolare utilità in tale contesto: tale tecnologia, infatti, consente esattezza e aggiornamento dei dati; permette l'accesso ai dati anche da remoto da parte dell'interessato, consentendogli il controllo; favorisce trasparenza e tracciabilità; costituisce garanzia di autenticità, arginando contraffazioni; assicura sicurezza e resistenza rispetto a potenziali attacchi e agevola l'interoperabilità tra sistemi, la condivisione e lo scambio dei dati, riducendo errori. Quest'ultimo aspetto è di particolare interesse, considerando che il Servizio Sanitario Nazionale è federato e decentralizzato. Inoltre l'integrazione della *blockchain* con l'intelligenza artificiale può rivelarsi strategica in tale settore per la ricerca e lo sviluppo.

Le problematiche giuridiche esaminate derivano direttamente dalle caratteristiche tecniche distintive della *blockchain*, quali disintermediazione, de-

[95] Art. 2-sexies, comma 3, e art. 2-septies, d.lgs. 196/2003, introdotti dal d.lgs. 101/2018.
[96] Art. 2-septies, comma 8, d.lgs. 196/2003, introdotto dal d.lgs. 101/2018.
[97] Cfr. *http://www.myhealthmydata.eu*.
[98] Cfr. *https://patientory.com*.
[99] Cfr. *https://medrec.media.mit.edu*.

centralizzazione e immutabilità, che devono faticosamente essere coordinate con un sistema di tutele fondato, invece, sulla centralizzazione, sul controllo e sulla responsabilizzazione, basato sulla presenza di soggetti cui imputare scelte e responsabilità[100].

Al fine di cercare di superare i profili di criticità da un punto di vista giuridico, in primo luogo è opportuna un'attenta valutazione e una conseguente scelta in merito all'utilizzo o meno della *blockchain* e alla specifica tipologia (*permissionless*, *permissioned*, ibrida)[101], in base al contesto di riferimento, alle finalità perseguite e ai dati che sono trattati; dovrà essere attentamente valutata la presenza di dati personali e la tipologia degli stessi, in particolare se sono presenti categorie particolari di dati personali come i dati relativi alla salute, soggetti, come esaminato, a una disciplina specifica. L'impatto e le relative problematiche, infatti, saranno intuitivamente molto differenti in ambito sanitario e, in tale contesto, saranno graduate diversamente laddove si tratti di fascicolo sanitario elettronico, ricerca scientifica, farmaci, etc.

In secondo luogo, al fine di superare le criticità, il diritto può fare leva sulla stessa tecnologia, costruendo un "diritto nella tecnica", ossia immaginando di incorporare all'interno del codice informatico clausole, misure correttive e strumenti rimediali proattivi e reattivi, al fine di regolare le eventuali responsabilità in caso di problematiche[102].

In terzo luogo, nella *blockchain* emerge l'esigenza di garantire trasparenza, il diritto alla comprensione e alla spiegabilità e, di conseguenza, il diritto alla sindacabilità e alla contestabilità da parte degli interessati e del giudice, necessari per applicare pienamente le norme di riferimento e per evitare asimmetrie tra chi gestisce queste soluzioni e chi se ne serve: questi diritti possono declinarsi in tale contesto anche nell'esigenza concreta di un "inter-

[100] Cfr. FINCK, *op. cit.*, 17 ss.; SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 68 ss.; PAROLA, MERATI, GAVOTTI, *op. cit.*, 688; GIULIANO, *op. cit.*, 989 ss.

[101] Cfr. CUCCURU, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, in *La Nuova giurisprudenza civile commentata*, fasc. 1, 2017, 115 ss., secondo cui, in ragione delle esigenze di governabilità e controllabilità da soddisfare, le *blockchains* ibride rappresentano la soluzione più feconda per il futuro.

[102] Cfr. DIMATTEO, PONCIBÒ, *Quandary of Smart Contracts and Remedies: The Role of Contract Law and Self-Help Remedies*, in *European Review of Private Law*, fasc. 6, 2019, 805-824.

prete" delle regole informatiche. L'approccio preventivo e proattivo di incorporazione del diritto nella tecnica può essere proficuamente accompagnato dall'attribuzione del diritto alla comprensibilità e alla contestabilità della tecnologia e da una logica di responsabilizzazione dei soggetti, in linea con la logica che guida il regolamento europeo 2016/679.

Pertanto, sotto il profilo specifico della protezione dei dati personali, al fine di risolvere i problemi afferenti al rispetto della relativa disciplina, la direzione efficace nel caso della *blockchain* può essere individuata nella relazione che lega diritto e tecnica, norme giuridiche e codice informatico. Nella consapevolezza che le problematiche si atteggiano diversamente in caso di *blockchains permissioned* o *permissionless*, dove sono più evidenti, al fine di superare le criticità, la strada è individuabile nell'approccio preventivo, proattivo e tecnico, previsto dallo stesso regolamento (UE) 2016/679, facendo leva sull'incorporazione dei principi e delle regole giuridiche nella tecnologia e facendo assolvere al diritto la sua funzione: la regolazione giuridica può servirsi della tecnologia per garantire il suo rispetto, svolgendo un'azione preventiva sul *design* dell'architettura tecnologica, adattandola e adeguando alcune caratteristiche distintive della *blockchain*, quali disintermediazione e immutabilità[103], al fine di perseguire i principi *data protection by design* e *by default*.

In particolare è opportuno immaginare soluzioni in grado di conciliare la tecnologia con i principi della *data protection*, quali la memorizzazione dei dati personali *off-chain* (fuori dalla catena di blocchi), memorizzando sulla stessa un mero riferimento, al fine di garantire l'esercizio dei diritti dell'interessato, oppure tecniche atte ad evitare la re-identificazione dei soggetti che non permettano di ricondurre i dati a un solo soggetto o coppie di chiavi diverse per ciascuna transazione o tecniche per rendere i dati inaccessibili[104]. In taluni casi, al fine di garantire effettività ai diritti dell'interessato, la *blockchain* può fare leva sulla funzione di autodistruzione "*kill switch*" o

[103] Misure capaci di ovviare all'immutabilità unilaterale conducono inevitabilmente a rinunciare, almeno parzialmente, ad aspetti costitutivi della tecnologia, che ne determinano anche le potenzialità; cfr. GAMBINO, BOMPREZZI, *op. cit.*, 619 ss.; PALLADINO, *op. cit.*, 155 ss.; SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 89 ss.

[104] Si tratta di tecniche quali le *secure multi-party computation*, *ring signatures*, *zero knowledge proof*, *one-time accounts*, etc.

"*self destruct*"[105] o può implementare funzioni di modifica del contenuto del codice informatico[106].

Inoltre è opportuno avvalersi di linee guida di interpretazione, codici di condotta e sistemi di certificazione, strumenti previsti dalla disciplina in materia di *data protection*, oltre a far leva sulla ricerca interdisciplinare in materia[107].

Peraltro, è necessario non dimenticare che la *blockchain* favorisce l'integrità e la sicurezza dei dati, la resistenza ad attacchi e il controllo distribuito sugli stessi, in linea con le previsioni in materia di protezione dei dati personali[108]: questa tecnologia garantisce tali aspetti fin dalla progettazione per impostazione predefinita e, di conseguenza, sotto tali profili risulta conforme agli obiettivi perseguiti dai principi e dagli strumenti previsti dal regolamento europeo 2016/679.

Pertanto nella *blockchain* le problematiche determinate dal rapporto tra tecnologia e diritto possono cercare e trovare soluzione proprio in questa relazione, grazie all'incorporazione di principi, regole e rimedi nella tecnologia e nel suo *design*, in modo da mantenere il ruolo strumentale della tecnologia rispetto all'uomo e permettere al diritto di assolvere la sua funzione nella società, tutelando i diritti della persona e la sua libertà.

3. Il governo dei dati e delle tecnologie emergenti: direzioni e scenari

Nelle tecnologie emergenti costituite dall'intelligenza artificiale e dalla *blockchain* problematiche e criticità conseguono alle caratteristiche tecniche di tali tecnologie. Pertanto alla base della complessa interazione tra intelligenza artificiale e *blockchain* con l'applicazione della *data protection* nel

[105] Così SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 111 ss.
[106] In tal senso anche POLETTI, *L'intelligenza artificiale e le prove di resistenza delle regole contrattuali*, in RUFFOLO (a cura di), *XXVI lezioni di diritto dell'intelligenza artificiale*, Torino, 2021, 193-202.
[107] Cfr. il citato studio «*Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?*» dell'*European Parliamentary Research Service* (EPRS), luglio 2019.
[108] Cfr. GAMBINO, BOMPREZZI, *op. cit.*, 619 ss.

settore pubblico e, in specifico, in quello della sanità sono presenti più ampiamente le scelte fondamentali del modello europeo di governo della tecnologia che si intende disegnare, che coinvolge il ruolo della persona, gli interessi collettivi, la società, il rapporto tra pubblico e privato. Come esaminato, vengono in gioco, infatti, i connotati del volto della sanità pubblica digitale che è necessario far convivere in equilibrio, quali digitalizzazione, trasparenza, apertura al fine di soddisfare i diritti della cittadinanza, ma anche protezione dei dati personali e, più ampiamente, tutela della persona.

Con quale forma del diritto devono essere regolati tali fenomeni perché le norme possano essere effettive[109]? Quale nuovo modello di *governance* delle autorità coinvolte è adeguato al mutato contesto in cui il diritto alla protezione dei dati personali disvela criticità ad essere efficacemente tutelato in caso di tecnologie emergenti? A quale orizzonte giuridico di Internet, per dirla con le parole del Maestro Frosini[110], è necessario guardare?

Nel rispondere a questi interrogativi che caratterizzano la fisionomia della futura dimensione digitale vengono in gioco gli strumenti e la forma del diritto.

Nel quadro regolatorio europeo, per quanto attiene agli strumenti giuridici, emerge l'esigenza di una sorta di "convergenza" di discipline normative a tutela della persona nelle sue vesti di interessato, utente e cittadino, al fine di proteggerla in modo effettivo ed efficace, che va a sommarsi alla convergenza tra protezione/controllo, da una parte, e circolazione/apertura, dall'altra, oltre a una convergenza anche da un punto di vista soggettivo tra il settore pubblico e quello privato, chiamati a una collaborazione e cooperazione atte a questi fini. Proprio al fine di garantire il diritto del singolo al controllo e al governo dei propri dati con la necessità di una loro circolazione e apertura, circoscrivendo e limitando al tempo stesso il potere dei colossi digitali, sono stati approvati i recenti regolamenti europei tesi a disciplinare la dimensione digitale, come il *Digital Services Act* (regolamento UE

[109] Al riguardo lo stesso strumento del consenso nella dimensione digitale mostra i suoi limiti e rischia di non proteggere concretamente l'individuo, che si rivela spesso inconsapevole e non autenticamente libero per i motivi richiamati precedentemente.

[110] FROSINI, *L'orizzonte giuridico dell'Internet*, in *Il diritto dell'informazione e dell'informatica*, n. 2, 2000, 271 ss.

2022/2065), il *Digital Markets Act* (regolamento UE 2022/1925), il *Data Governance Act* (regolamento UE 2022/868), etc.

Sotto il profilo della forma, emerge nel *framework* regolatorio europeo recente e, più in generale, nelle norme che trattano il rapporto tra diritto, diritti e tecnologia, la tensione costante tra certezza e prevedibilità[111], da un lato, e flessibilità e adattabilità, dall'altro, necessarie per garantire efficacia[112]. Questo aspetto consegue alla necessità di un complesso articolato di regole diverse atte a costruire un diritto complessivamente sostenibile e, a tal fine, tese a garantire certezza del diritto, tutelando i diritti delle persone, ma anche ad assicurare adattabilità allo sviluppo e ai cambiamenti della tecnologia, riuscendo a trovare un virtuoso equilibrio tra interessi diversi grazie a un approccio *multistakeholder*, in cui gli Stati sono chiamati a nuove forme di cooperazione e collaborazione.

In tale contesto, la sfida è proprio quella di trovare un punto di caduta, un ragionevole bilanciamento tra diritti, istanze e interessi diversi, in cui si colloca anche la necessità di equilibrio tra protezione della persona, digitalizzazione, trasparenza e apertura, valori perseguiti parimenti dalla normativa in materia, che esplicitamente non interpreta la protezione dei dati personali come un valore assoluto, ma considera la funzione sociale e l'interesse generale che può limitarla[113]. Il giurista è chiamato ad operare un ragionevole bilanciamento e giungere ad un'interpretazione del sistema normativo che renda possibile conciliare le esigenze di digitalizzazione, trasparenza e apertura con il diritto fondamentale alla protezione dei dati personali e le sue caratteristiche di indisponibilità, imprescrittibilità ed assolutezza, tutelando l'individuo allo stesso tempo come persona, ma anche come utente e cittadino.

[111] Tale istanza emerge nello stesso cambiamento di approccio dell'Unione europea, che negli ultimi anni per regolare la dimensione digitale sceglie lo strumento del regolamento dotato di maggiore *vis* sugli Stati membri rispetto alla direttiva.

[112] Questa esigenza si traduce nella presenza non solo di norme strettamente intese, ma anche di *soft law*, atti di indirizzo, linee guida, strategie di istituzioni, autorità, organismi fino a forme di *co-regulation* e di *self-regulation*, oltre a meccanismi di flessibilità nelle norme, quali obblighi di valutazione e revisione degli atti, procedure più snelle anche al di fuori del procedimento legislativo e meccanismi come le *regulatory sandboxes*.

[113] Considerando 4, reg. (UE) 2016/679.

Pertanto la riflessione deve concentrarsi sul modello di governo della tecnologia e sulle fondamenta su cui basarlo.

Un primo aspetto, che emerge dal *framework* giuridico, riguarda il rapporto tra diritto e tecnologia, che muta e matura. La direzione intrapresa poggia sulla costruzione di una *governance* umanocentrica, capace di conferire piena centralità alla persona, per tutelare la quale è necessario un adeguato contesto istituzionale e un bilanciamento mobile tra diritti in una logica che mantenga la tecnologia strumento nelle mani dell'uomo. L'approccio orientato a una *governance* umanocentrica emerge dagli atti a livello sovranazionale; è sufficiente pensare agli atti di *soft law* e *hard law* relativi all'intelligenza artificiale[114]. Emerge un approccio olistico, in cui la persona con la sua identità funge da prisma i cui riflessi sono costituiti dai diversi diritti in gioco, indivisibili, seppur nella loro conflittualità. Tale approccio umanocentrico può essere realizzato e implementato concretamente sfruttando la tecnologia stessa e la relazione tra regole giuridiche e regole informatiche; il diritto può avvalersi della tecnica per garantire il suo rispetto. Sotto tale profilo la recente regolazione europea abbraccia un approccio preventivo e proattivo, che prende forma in due profili sinergici e strettamente connessi: l'incorporazione del diritto nella tecnica e il *risk-based approach*.

Negli atti europei degli ultimi anni emerge come paradigma capace di risolvere o quanto meno minimizzare le problematiche che affliggono il rapporto tra diritto e tecnologia, infatti, il paradigma dell'incorporazione preventiva di principi etici e giuridici, norme e rimedi nella tecnologia stessa, ossia una *legal protection by default* e *by design*, basata sull'*accountability*, presente fin dal regolamento europeo 2016/679 in materia di protezione dei dati personali[115]. Il diritto può avvalersi della tecnologia per garantire il suo rispetto, generando un modello di "diritto nella tecnica". Si tratta di un approccio proattivo, che tutela la persona fin dalla progettazione, per impostazione predefinita e per mezzo della valutazione d'impatto, capace di far leva

[114] Prima di arrivare alla proposta di regolamento sull'intelligenza artificiale, dal 2018 l'Unione europea ha dedicato una serie di atti al tema, quali comunicazioni, piani, raccomandazioni, orientamenti.

[115] Si tratta dei principi *data protection by design* e *by default*, cui si affianca il *data protection impact assessment* (artt. 25 e 35, regolamento UE 2016/679).

sulla conformazione dei sistemi tecnologici e sulla sicurezza, da una parte, e sulla responsabilizzazione e sulla consapevolezza dei soggetti, dall'altra, al fine di confinare le repressioni prevalentemente *ex post* alla tutela sanzionatoria successiva, senza reprimere eccessivamente la libera circolazione dei dati e lo sviluppo economico.

Come esaminato, l'approccio del "diritto nella tecnica" risulta capace di superare le criticità dell'applicazione delle norme in materia di *data protection* sia nel caso della *blockchain* che dell'intelligenza artificiale. Tale prospettiva è ulteriormente sviluppata nell'*Artificial Intelligence Act* (proposta di regolamento COM(2021) 206 *final* del 21 aprile 2021), che si basa su un approccio proattivo basato sul rischio, coadiuvato anche da un correlato sistema sanzionatorio, e sulla sua categorizzazione preventiva, cui si collega una regolazione differenziata. Anche il concetto del rischio, del resto, emerge fin dal regolamento in materia di *data protection* e dagli strumenti ivi previsti.

L'approccio proattivo, che prende vita nell'incorporazione preventiva del diritto nella tecnica e nell'approccio basato sul rischio, non è scevro da criticità, da affrontare al fine di assicurare un'implementazione sostenibile del modello di governo della tecnologia, quali in particolare la "rigidità" ontologica del codice informatico stesso, che si scontra con la flessibilità necessaria al bilanciamento "mobile" idoneo a una tutela efficace ed effettiva dei diritti, oltre a un'opacità linguistica, dal momento che il linguaggio è informatico e non è quello naturale delle norme giuridiche[116]. L'altra problematica di tale prospettiva sta nel fatto che in tal modo il rispetto dei principi giuridici e l'equilibrio tra diritti sono di fatto delegati a coloro che sono chiamati a sviluppare le soluzioni tecnologiche e alle categorie di operatori nel mercato con conseguenti possibili rischi.

Sinergicamente a tali aspetti, al fine di superare l'opacità e la chiusura dei processi di gestione dei dati, evitando un fideistico appalto alle tecnologie emergenti come salvifiche, è necessario garantire nella dimensione digitale una declinazione rafforzata della trasparenza, una trasparenza sostanziale algoritmica che assicuri conoscibilità, comprensibilità e sindacabilità, ren-

[116] LO SAPIO, *La trasparenza sul banco di prova dei modelli algoritmici*, in *federalismi.it*, fasc. 11, 2021, 242 ss.

dendo gli algoritmi oggetto della piena cognizione e del pieno sindacato dal parte del giudice, anche al fine di garantire quella trasparenza e apertura che connotano il volto dell'amministrazione digitale: tale principio si traduce nell'assicurare non solo informazioni e accesso ai dati, ma anche la conoscenza della logica degli algoritmi, accompagnata dalla consapevolezza in merito alle conseguenze e all'impatto sulla persona.

Nei confronti di dati, algoritmi e intelligenza artificiale, pertanto, devono essere attribuiti e riconosciuti il diritto alla comprensibilità, capace di informare e rendere consapevole l'interessato, e il diritto alla contestabilità, idoneo a consentire all'interessato, anche per mezzo di un giudice, di valutare e di sindacare la decisione a cui perviene la tecnologia. Tali diritti si traducono più ampiamente nel diritto del singolo di mantenere la propria autonomia e autodeterminazione nei confronti della macchina: questo diritto comporta l'esigenza di comprensione dei meccanismi di funzionamento e una sorta di correlato dovere di "spiegare" in capo alla soluzione di intelligenza artificiale o, meglio, in capo a chi ne è responsabile[117]. Anche nel caso della *blockchain* emerge l'esigenza di garantire trasparenza, il diritto alla comprensione e alla spiegabilità e, di conseguenza, il diritto alla sindacabilità e alla contestabilità da parte degli interessati e del giudice, necessari per applicare pienamente le norme di riferimento e per evitare asimmetrie tra chi gestisce queste soluzioni e chi se ne serve: questi diritti possono declinarsi in tale contesto anche nell'esigenza concreta di un intermediario "interprete" delle regole informatiche, capace di superare la barriera linguistica del codice informatico.

A livello normativo europeo l'attenzione alla trasparenza algoritmica è presente fin dal regolamento 2016/679 in materia di *data protection*, dal momento che il titolare del trattamento è tenuto a fornire all'interessato, tra le informazioni necessarie per garantire un trattamento corretto e trasparente, «l'esistenza di un processo decisionale automatizzato, compresa la profilazione […] e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato»[118]; su tali informazioni esiste, altresì, un diritto di accesso, ri-

[117] Cfr. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal*, fasc. 1, 2019, 7. Al riguardo cfr. CARULLO, *op. cit.*, 445 ss.
[118] Art. 13, par. 2, lett. f) e art. 14, par. 2, lett. g), regolamento (UE) 2016/679.

conosciuto all'interessato esplicitamente dall'art. 15 del regolamento (UE) 2016/679.

L'*Artificial Intelligence Act* mostra particolare attenzione per la trasparenza, che secondo le disposizioni europee deve essere "appropriata", e dispone siano fornite informazioni chiare e adeguate all'utente sia in caso di sistemi "ad alto rischio", sia in caso di sistemi "a basso rischio". Il regolamento europeo, infatti, prevede che ogni sistema di IA ad alto rischio sia disegnato e sviluppato in modo da assicurare un appropriato livello di trasparenza (*sufficiently transparent*)[119], mostrando in tal modo consapevolezza circa la necessità di misure proporzionate, senza imporre obblighi irrealizzabili alla luce delle caratteristiche tecnologiche, come tali destinati ad una concreta inefficacia[120]. Emerge con evidenza sotto tale profilo l'esigenza di sostenibilità del diritto, più volte richiamata.

Nel quadro regolatorio europeo, alla trasparenza algoritmica si accompagna la necessaria trasparenza da parte di chi governa gli algoritmi stessi, coniugandosi pertanto l'esigenza di trasparenza delle macchine con la necessità di una correlata trasparenza da parte degli uomini che le gestiscono. La trasparenza degli algoritmi e di coloro che li governano garantisce il rispetto del diritto alla comprensione, alla spiegabilità e alle correlate sindacabilità e contestabilità, valorizzando, in tal modo, il ruolo della persona: garantire che l'uomo possa comprendere la macchina assicura che l'intelligenza artificiale rimanga strumentale rispetto a quella umana e la tecnologia mantenga la sua funzione "servente" rispetto all'uomo e alle sue decisioni, soprattutto laddove incidano su diritti.

Al riguardo, la natura degli algoritmi pone il problema se esista sempre una logica comprensibile, dato il funzionamento degli stessi e la conseguente possibile non intelligibilità secondo criteri logico-razionali[121]. L'autonomia, infatti, connota e differenzia l'intelligenza artificiale dalla logica dei soft-

[119] Art. 13, proposta di regolamento «*Artificial Intelligence Act*», COM(2021) 206 *final* del 21 aprile 2021.

[120] Cfr. CASONATO, MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal*, fasc. 3, 2021, 426 ss.

[121] Cfr. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, fasc. 1, 2019, 77 ss.; SIMONCINI, SUWEIS, *op. cit.*, 97 ss.

ware tradizionali[122]; il modello solitamente non è direttamente intelligibile da parte dell'essere umano (*black box*). L'approccio dell'intelligenza artificiale non è fondato su spiegazioni causali e logico-deduttive, tipiche del ragionamento umano, basato su ipotesi predeterminate e nessi di causalità, ma si affida a connessioni e inferenze tra dati e poggia sull'approccio statistico e sulla probabilità, determinando talvolta difficoltà di comprensione circa le motivazioni (il "perché") delle risposte fornite[123].

Pertanto garantire la trasparenza algoritmica può essere particolarmente complesso a fronte di una congenita opacità che caratterizza gli algoritmi, che si declina in un'opacità strutturale, derivante dal funzionamento degli stessi e dal fatto che resta non comprensibile persino ai programmatori l'iter logico seguito dalla macchina per giungere al risultato partendo dai dati a disposizione, cui si somma l'opacità linguistica già precedentemente richiamata, dovuta al linguaggio informatico e non a quello naturale[124].

Tale aspetto può risultare particolarmente problematico in caso di utilizzo dell'IA in ambiti giuridici quali l'amministrazione pubblica, dal momento che i provvedimenti amministrativi (art. 3, legge 241/1990) devono essere necessariamente accompagnati da una motivazione; l'opacità delle motivazioni di un provvedimento amministrativo impedisce qualsiasi controllo sull'esercizio della funzione, potendo portare all'annullamento delle decisioni impugnate sotto tale profilo[125].

La sfida dell'ordinamento e del diritto è operare un ragionevole bilanciamento tra diritti ed interessi diversi. In tale quadro di riferimento, è necessario un rafforzamento dello spazio giuridico pubblico a protezione dei diritti

[122] L'apprendimento automatico da parte della macchina può essere o meno supervisionato dall'uomo, ossia può o meno ricevere indicazioni dall'esterno; l'analisi dei dati consiste in un processo di approssimazione, che genera il rischio di trarre conclusioni imprecise e discriminatorie, laddove i dati non siano corretti o non siano debitamente annotati, in modo da poter essere correttamente utilizzati e interpretati dalla macchina.

[123] In tal senso AMATO MANGIAMELI, *Intelligenza artificiale, big data e nuovi diritti*, in *Informatica e diritto*, fasc. 1, 2022, 9 ss.; CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, numero speciale, 2019, 101-130; MORO, *Algoritmi e pensiero giuridico. Antinomie e interazioni*, in *Rivista di diritto dei media*, fasc. 3, 2019, 19.

[124] LO SAPIO, *op. cit.*, 242 ss.

[125] Cfr. CASONATO, *op. cit.*, 119 ss.

e delle libertà della persona, che passa necessariamente dal ruolo delle autorità indipendenti coinvolte, le uniche capaci ontologicamente di trovare quell'equilibrio tra certezza e flessibilità e creare di conseguenza un diritto sostenibile. Di conseguenza la riflessione in materia deve concentrarsi anche sull'opportunità di creare nuovi modelli di *governance* e una ridefinizione delle competenze delle autorità e degli enti coinvolti (come il Garante per la protezione dei dati personali, AgID etc.), dando vita a un'applicazione normativa congiunta e a una forte collaborazione tra autorità. Questo approccio è necessario anche per i nuovi comitati e organismi creati dai regolamenti europei, che dovranno valersi di una stretta collaborazione e cooperazione. Ciò va nella direzione di un approccio orizzontale che scardina i sistemi regolatori verticali, meno adatti da sempre al volto orizzontale della rete, ed evita il rischio di autorità che possono far pendere la bilancia verso l'uno o l'altro diritto o tecnologia per cui sono istituite, abbracciando invece il necessario approccio olistico sicuramente conforme alla complessità digitale e all'intreccio tra diritti diversi.

Si collega alla *governance* di autorità indipendenti e all'esigenza di flessibilità l'opportunità di avvalersi di linee guida di interpretazione, codici di condotta e sistemi di certificazione, strumenti previsti dalla disciplina in materia di *data protection* e far leva sulla ricerca interdisciplinare, sia per l'intelligenza artificiale che per la *blockchain* come suggerito a livello sovranazionale.

Il cambiamento pervasivo determinato dalla centralità assunta dai dati investe i complessi equilibri consolidati tra diritti e libertà, il bilanciamento tra interessi contrapposti, il rapporto tra poteri e la tenuta dei principi democratici fondamentali, influenzando le direttrici culturali ed etiche del futuro. In questo scenario si pone una chiara responsabilità pubblica nel garantire effettiva tutela ai diritti e alla persona, affrontando complessi, saggi e necessari bilanciamenti tra diritti e interessi che nella dimensione digitale si intrecciano e confliggono, mossi da tensioni diverse.

Le criticità, che riguardano i profili esaminati e che rischiano di frenare questa evoluzione del volto della sanità digitale e il correlato uso delle tecnologie emergenti, possono essere superate solo con un approccio sostanziale (e non formale), realmente attento alla sicurezza e alla conformazione dei

sistemi tecnologici, basato su una valutazione di impatto preventiva ai rischi, atta a confinare le repressioni prevalentemente *ex post*. Tale approccio per realizzarsi ha bisogno di un'opera ampia, pervasiva e profonda di cultura digitale non solo per la collettività, al fine di garantirne la consapevolezza e quindi anche la libertà, ma altresì all'interno delle amministrazioni, al fine di far comprendere che la sinergia tra digitalizzazione, trasparenza, apertura e protezione dei dati personali è necessaria per un'amministrazione che voglia raggiungere con successo l'obiettivo del "buon andamento" a vantaggio della collettività, reale beneficiaria di tutta la normativa di riferimento. A ciò si unisce l'esigenza di risorse umane e finanziarie.

Garantire i diritti e le libertà nella dimensione digitale involge la *governance* della tecnologia ed è quanto mai necessario provare a cercare quello che il Maestro Frosini chiamava «l'orizzonte giuridico di Internet», individuando l'"ordinamento giuridico digitale" e il modello di governo della tecnologia cui siamo e dovremmo essere indirizzati, capace di tutelare in modo efficace la persona e la società rispetto alla tecnologia: un diritto sostenibile, capace di bilanciare protezione e circolazione, certezza e flessibilità senza impattare negativamente sulla persona grazie a un saggio equilibrio tra diritti e interessi, facendo leva su un approccio olistico, al cui centro situare la persona stessa per far sì come vuole il regolamento europeo che il trattamento dei dati personali sia al servizio dell'uomo[126].

[126] Considerando 4, reg. (UE) 2016/679.

Diritto Mercato Tecnologia

Numeri Speciali

2016 Lo Statuto Etico Giuridico dei Campioni Biologici Umani
a cura di Dario Farace

2017 Il Mercato Unico Digitale
a cura di Gianluca Contaldi

2018 La Ricerca su Materiali Biologici di Origine Umana:
Giuristi e Scienziati a confronto
a cura di Alberto M. Gambino, Carlo Petrini e Giorgio Resta

2019 La Tassazione dell'Economia Digitale tra Sviluppi Recenti
e Prospettive Future
a cura di Alessio Persiani

La rivista "Diritto Mercato Tecnologia" intende fornire un costante supporto di aggiornamento agli studiosi e agli operatori professionali nel nuovo scenario socio-economico originato dall'interrelazione tra diritto, mercato e tecnologia, in prospettiva interdisciplinare e comparatistica. A tal fine approfondisce, attraverso studi nei settori privatistici e comparatistici, tematiche afferenti in particolare alla proprietà intellettuale, al diritto antitrust e della concorrenza, alle pratiche commerciali e alla tutela dei consumatori, al biodiritto e alle biotecnologie, al diritto delle comunicazioni elettroniche, ai diritti della persona e alle responsabilità in rete.

ISSN (Online Edition): 2239 -7442