Il convegno del 26 ottobre 2016 si inserisce nel Progetto Nazionale dei C.D.E Italiani dal titolo "Un Mercato Unico Digitale per l'Europa" promosso dalla Rappresentanza in Italia della Commissione Europea.

DIRITTO MERCATO TECNOLOGIA

NUMERO SPECIALE 2017

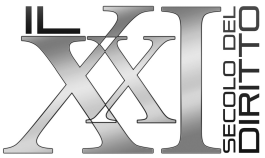
IL MERCATO UNICO DIGITALE

A CURA DI GIANLUCA CONTALDI

UNIVERSITÀ DI MACERATA — 26 OTTOBRE 2016

ATTI DEL CONVEGNO

NUOVA EDITORIALE UNIVERSITARIA



Via Colonnello Tommaso Masala, 42 - 00148 Roma
e-mail: nuovaeditriceunivers@libero.it
web: www.nuovaeditriceuniversitaria.it

Finito di stampare nel mese di dicembre 2017
dalla Infocarcere s.c.r.l.
Via C.T. Masala, 42 - 00148 Roma

ISBN: 978-88-95155-71-5

DIRITTO MERCATO TECNOLOGIA

NUMERO SPECIALE 2017

IL MERCATO UNICO DIGITALE

SOMMARIO

Marco Bolognese
Università degli Studi di Macerata

La tutela dei dati personali nel Regolamento UE 2016/679

Sommario: 1. La base giuridica – 2. Alcuni profili di illegittimità rispetto al Trattato di Lisbona – 3. La definizione dei dati – 4. I soggetti destinatari – 5. Ambito di applicazione territoriale – 6. I principi generali ed i diritti del proprietario dei dati – 7. Gli obblighi dei tenutari dei dati – 8. Le autorità di controllo – 9. Considerazioni conclusive

La tutela del trattamento dei dati personali e la loro libera circolazione verrà disciplinata, a far data dal 25 maggio 2018, dal regolamento 2016/679[1]. Il nuovo "*approccio globale alla protezione nell'Unione europea*"[2] si sostituisce alla direttiva 95/46/CE[3], divenuta oramai inidonea a causa degli incalzanti sviluppi tecnologici, che hanno accresciuto esponenzialmente la condivisone e la raccolta dei dati da parte delle imprese private e delle pubbliche autorità nello svolgimento delle loro attività. L'intento del legislatore europeo, pertanto, è quello di restaurare un clima di fiducia negli ambienti *on line*, con conseguenti benefici

[1] Regolamento (UE) 2016/79 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/45 CE (regolamento generale sulla protezione dei dati), in GUUE del 4.5.2016. L. 119/3. Tale strumento è affiancato dalla Direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati. D'ora in avanti nelle note gli articoli del regolamento verranno indicati come "art".

[2] Proposta della Commissione europea del 25.1.2012, COM(2012) 11 *final*, in *http://www.eur-lex.europa.eu*.

[3] Direttiva 95/46/CE in *Gazzetta ufficiale* n. L 281 del 23/11/1995, pag. 0031 – 0050, d'ora in avanti indicata in nota come "direttiva".

per la crescita dell'economia digitale nel mercato interno. La mancanza di fiducia, infatti, frenando i consumatori sia negli acquisti *on line* sia nell'utilizzo di nuovi servizi, rafforza il rischio di rallentare lo sviluppo di applicazioni tecnologiche innovative.

L'ambizioso progetto di una tutela globale appare in realtà tutt'altro che esaustivo. Da un lato, infatti, il Regolamento non trova applicazione nel trattamento dei dati effettuato: dagli Stati membri nell'esercizio di attività relative alla politica estera e di sicurezza comune dell'Unione; dalle istituzioni dell'U.E.[4]; in caso di repressione e di accertamento dei reati. Dall'altro lato, non si rinviene un ben definito e chiaro coordinamento con la legislazione degli Stati Membri, sia essa preesistente o futura. Invero, il tratto comune del Regolamento è la costante possibilità di deroga al trattamento dei dati per consentire l'esercizio di altri diritti fondamentali o la tutela di interessi dello Stato. A questa delicata operazione di bilanciamento si affiancano possibili profili di non conformità con i trattati istitutivi dell'Unione europea e l'esistenza a livello internazionale di una convenzione tra gli Stati membri che già disciplinava alcuni aspetti del trattamento dei dati.

Senza sottacere, poi, la complessità del testo normativo con i suoi n. 99 articoli e 173 considerando. Quest'ultimi a volte – ad esempio nel caso del trattamento dei dati sensibili[5] – oltrepassano la loro funzione di

[4] Regolamento CE n. 45/2001, in *http://www.eur-lex.europa.eu*.

[5] L'art. 9 in materia di dati sensibili pone una deroga al loro divieto di trattamento giustificata da motivi di interesse pubblico nei settori della sanità pubblica. Il considerando n. 54 aggiunge che, in tale ambito, il trattamento è lecito senza il consenso dell'interessato mentre esso non è consentito per altre finalità da parte di terzi, quali datori di lavoro, compagnie di assicurazione e istituti di credito. Analogamente l'art. 3 stabilisce in modo scarno che il regolamento si applica ai dati trattati da un titolare del trattamento non stabilito nell'Unione europea, quando l'attività di trattamento è connessa all'offerta di beni o servizi. A fronte di tale sintetica disposizione, il considerando 27 sembra aggiungere una fattispecie normativa ulteriore, riferita alla semplice intenzione di offrire: "*Per determinare se tale titolare o responsabile del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno verificare se risulta che il titolare o il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione. Mentre la semplice accessibilità del sito*

motivare "in modo conciso le norme essenziali dell'articolato", contenendo enunciati a carattere normativo, contrariamente all'accordo interistituzionale sulla qualità redazionale degli atti[6] e alla giurisprudenza interpretativa del medesimo[7].

1. La base giuridica

La protezione dei dati personali, prima del Trattato di Lisbona trovava la sua fonte in due convenzioni internazionali

L'art. 6 dell'allora TUE richiamava la CEDU come fonte da cui desumere i principi fondamentali. Non a caso l'art. 1 della direttiva 95/46/CE ricalcava a grandi linee l'art. 8 della CEDU nella interpretazione fornitane dalla Corte di Strasburgo[8], cosicché il trattamento dei dati personali veniva considerato un aspetto del diritto alla vita privata.

Lo sviluppo tecnologico degli anni '60 ha portato[9] nel 1981 alla speci-

---

web del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione".

[6] Il 22 dicembre 1998 il Parlamento europeo, il Consiglio e la Commissione hanno concluso un accordo interistituzionale sugli orientamenti comuni relativi alla qualità redazionale della legislazione comunitaria, in GU 1999, C 73, pag. 1. Gli orientamenti non sono giuridicamente vincolanti. Tra i principi ivi contenuti si annoverano i seguenti: "10. I 'considerando' motivano in modo conciso le norme essenziali dell'articolato (…). Non contengono enunciati di carattere normativo (…)".

[7] CGUE, 12 luglio 2005, cause riunite C-154/04 e C-155/04, *Alliance for Natural Health*, in *Racc. 2005*, pag. I-6451, punto 92.

[8] CEDU, 2 agosto 1984, ricorso n. 8691/79, *Malone c. Regno Unito;* 3 aprile 2007, ricorso n. 62617/00, *Copland c. Regno Unito*, in *www.echr.coe.int*.

[9] Committee of Ministers (1973), Resolution (73) 22 on the Protection of the Privacy of Individuals *vis-a-vis E*lectronic Data Banks in the Private Sector, 26 September 1973; Committee of Ministers (1974), Resolution (74) 29 on the Protection

fica protezione dei dati personali, attraverso la stipula dalla Convenzione n. 108[10] da parte degli Stati facenti parte del Consiglio d'Europa, ratificata poi da tutti gli Stati dell'Unione europea, ed aperta alla firma di Paesi terzi. L'esistenza di tale strumento pone qualche ragionevole dubbio sul rispetto del principio di proporzionalità da parte del Regolamento. Infatti la Convenzione contiene in larga parte elementi comuni al regolamento[11]. Senza sottacere che nel 1999[12] fu modificata per permettervi l'adesione dell'Unione europea. Infine nel 2001[13] fu adottato un protocollo addizionale riguardante i flussi transazionali di dati verso Paesi non contraenti e la creazione obbligatoria dell'Autorità di controllo per la protezione dei dati personali.

Infine, con il Trattato di Lisbona del 2009, la protezione dei dati personali divine un diritto fondamentale sancito nell'art. 8 della Carta

---

of the Privacy of Individuals *vis-a-vis* Electronic Data Banks in the Public Sector, 20 September 1974, in *www.coe.int*.

[10] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale n. 108 del 28 gennaio 1981, in *https://www.coe.int*.

[11] La Convenzione si applica a tutti i trattamenti di dati effettuati sia nel settore privato sia in quello pubblico, come ad esempio l'elaborazione dei dati da parte delle autorità di polizia e giudiziarie. La raccolta e il trattamento dei dati personali sono governati dai principi di equità e di legittimità: i dati elaborati automaticamente sono registrati per scopi legittimi specifici e non possono essere utilizzati per fini incompatibili con tali scopi; né conservati per più di quanto è necessario. Sono vietati, in assenza di adeguate garanzie giuridiche, l'elaborazione di dati sensibili quali quelli relativi alla razza, ideologie politiche, salute, religione, vita sessuale di una persona. La Convenzione sancisce anche il diritto dell'individuo di conoscere le modalità del trattamento ed il diritto alla rettifica. Le restrizioni alla tutela, stabilita dalla Convenzione, sono ammesse per garantire superiori interessi, come ad esempio la sicurezza o la difesa dello Stato contraente. La libera circolazione dei dati personali tra i Paesi aderenti subisce anche alcune limitazioni verso quegli Stati in cui la legislazione non fornisce una protezione equivalente.

[12] Amendments to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) Allowing the European Communities to Accede, Adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999, in *www.coe.int*; art. 23.2 della Convenzione n. 108.

[13] Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows, CETS No. 181, 2001, in *www.coe.int*.

di Nizza[14]; mentre l'art. 16 del TFUE (già 286 TCE), unitamente all'art. 4.1 TFUE, ne affidano la tutela alla competenza concorrente tra gli Stati membri e l'Unione europea. I due rifermenti normativi costituiscono il fondamento giuridico del Regolamento[15].

Va subito precisato che la protezione dei dati, sebbene assurga a diritto fondamentale dell'Unione, non è una prerogativa assoluta, potendo subire delle deroghe, per permettere l'esercizio di altri diritti fondamentali o proteggere particolari interessi dello Stato[16]. È pur vero che l'art. 8 della Carta di Nizza, contrariamente al "gemello" della CEDU, non contiene al suo interno alcuna limitazione. Tuttavia le restrizioni, in primo luogo, erano già state imposte dalla Corte di giustizia secondo cui la disposizione *de qua* deve essere letta tenendo presente la sua funzione nella società[17]. Secondariamente l'art. 52 della Carta prevede delle limitazioni a condizione che siano imposte dalla "dalla legge", "siano necessarie", "rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui". Tali vincoli corrispondono in buona sostanza a quelli di cui all'art. 8.2 della CEDU[18]. Pertanto

[14] Carta dei diritti fondamentali dell'Unione europea, in *http://eur-lex.europa.eu*. L. S. Rossi, *"stesso valore giuridico dei Trattati"? Rango, primato ed effetti della Carta dei diritti fondamentali dell'Unione europea*, in *Il diritto dell'Unione europea*, 2016, p. 329.

[15] Considerando 1.

[16] P. De Sena, *Proportionality and Human Rights in International Law: Some... «Utilitarian Reflection»*, in *Rivista di diritto internazionale*, 2016, p. 1009.

[17] CGUE, 9 Novembre 2010, cause riunite C-92/09 e C-93/09, *Volker e Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, in *Racc*. 2010, punto 48.

[18] Art. 8 comma 2 CEDU "Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui". Sul legittimo scopo perseguito v. CEDU, 28 gennaio 2003, ricorso n. 44647/98, *Peck c. Regno Unito,* § 85. Sulla necessità per la sicurezza sociale v. CEDU, 26 marzo1987, ricorso n. 9248/87, *Leander c. Svezia*, §§ 58-67; 18 ottobre 2011, ricorso n. 16188/07, *Khelili c. Svizzera.* Sul concetto di legge v. CEDU, 16 febbraio 2000, ricorso n. 27798/95, *Amann c. Svizzera*, § 50; 25 marzo 1988, ricorso n. 23224/94, *Kopp c. Svizzera*, § 55; 10 febbraio 2009, ricorso n. 25198/02, *Iordachi and*

atteso il contenuto quasi identico delle due disposizioni, sulla base dell'art. 52.3 della Carta, le restrizioni dovranno essere interpretate alla luce della giurisprudenza della Corte Edu. I giudici di Strasburgo, in particolare, hanno circoscritto la tutela dei dati per garantire l'esercizio di altri diritti quali la libertà di stampa, di espressione[19], la libertà di scienza e di arte[20]. Conformemente a tale giurisprudenza, il Regolamento dispone espressamente delle deroghe al diritto sul trattamento dei dati per garantire le stesse libertà[21]. Inoltre, il riferimento alla giurisprudenza della Corte di Strasburgo diverrà una operazione ermeneutica necessaria, in considerazione della possibilità degli Stati di derogare alle disposizioni del Regolamento.

La necessità di tale richiamo è testimoniata dallo stesso strumento derivato, che recepisce le restrizioni di cui all'art. 52 della Carta al fine di limitare i diritti e gli obblighi connessi al trattamento, per la salvaguardia di beni superiori come un interesse economico o finanziario dell'Unione o dello Stato membro[22].

2. Alcuni profili di illegittimità rispetto al Trattato di Lisbona

Nonostante la chiarezza della base giuridica, il continuo bilanciamento del diritto al trattamento dei dati con altri interessi, quindi la sua limitazione anche e soprattutto da parte degli Stati membri, pone un dubbio più che legittimo sul rispetto del principio di sussidiarietà da

---

Others c. Moldavia, § 50; 7 febbraio 2012, ricorso n. 39954/08, *Axel Springer AG c. Germania*, §§ 90-91; 7 febbraio 2012, ricorsi nn. 40660/08 e 60641/08, *Von Hannover c. Germania* (N. 2)*,* §§ 118 e 124, tutte in *www.echr.coe.i*nt.

[19] CEDU, ricorso n. 39954/08 *Axel Springer AG c. Germana,* cit., § 90 e 91; ricorsi 40660/08 e 60641/08, *Von Hannover c. Germany* (N. 2*),* cit., §§ 118 e 124, in *www.echr.coe.int*.

[20] CEDU, 24 maggio 1988, ricorso n. 10737/84, *Müller e altri c. Svizzera*; 25 gennaio 2007, ricorso n. 68345/01, *Vereinigung bildender Künstler c. Austria*, §§ 26 e 34, in *www.echr.coe.int*.

[21] Artt. 85 e 89.

[22] Art. 23.

parte della normativa derivata[23].

Tale violazione si individuerebbe, ad esempio, in riferimento alle ipotesi che determinano la liceità del consenso. Tra esse si annoverano il trattamento dei dati necessario o per adempiere ad un obbligo legale (cui è sottoposto il titolare del trattamento) oppure per eseguire un compito connesso all'esercizio di pubblici poteri (cui è investito il titolare del trattamento). In entrambi i casi gli Stati membri rimangono sovrani di stabilire la base giuridica da cui deriva l'obbligo del trattamento: non si richiede nemmeno l'adozione di un atto legislativo da parte del parlamento nazionale, fatte salve le prescrizioni dell'ordinamento costituzionale interessato. In aggiunta il Regolamento prevede che gli Stati membri possono mantenere (o introdurre) disposizioni specifiche sulle modalità del predetto trattamento[24].

La normativa domestica può addirittura derogare alla quasi totalità delle disposizioni del Regolamento – riguardanti i capi II (principi), III (diritti dell'interessato), IV (titolare del trattamento e responsabile del trattamento), V (trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali), VI (autorità di controllo indipendenti), VII (cooperazione e coerenza) e IX (specifiche situazioni di trattamento dei dati) – qualora sia necessario per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione. Deroghe o limitazioni sono consentite anche al diritto di acceso (art. 15) di rettifica (art. 16) di cancellazione (art. 17) per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici[25]. La normativa statale può, altresì, conservare limitazioni già disposte o introdurne di nuove riferite al trattamento di dati genetici e biometrici[26].

Appare evidente, dunque, come l'azione dell'Unione non sia affatto

[23] Art. 5.3 TUE.
[24] Considerando 41; art. 6 par. 2.
[25] Considerando 41; art. 6 par. 2. Considerando 156; art. 6 par. 3; art. 85 e art. 89.
[26] Art. 9.

necessaria, stante il mantenimento di una legislazione preesistente[27] in aggiunta alla possibilità, per i parlamenti nazionali, di derogare al regolamento. Anzi la possibilità dell'intervento statale finisce proprio per mantenere quella frammentazione della protezione dei dati, che il Regolamento si prefigge di eliminare nel territorio dell'Unione[28].

Per altro verso, il Regolamento violerebbe anche il "principio di attribuzione" delle competenze, perché più che regolare la competenza "concorrente" tra gli Stati e l'Unione[29], finisce per trasformarla in competenza "esclusiva". Infatti, una volta che l'Unione europea ha disciplinato la materia con il Regolamento in esame, il medesimo, come visto, conferisce agli Stati la possibilità di introdurre norme soprattutto di carattere derogatorio. I Paesi membri, vale a dire, possono adottare autonomamente atti giuridici vincolanti perché sono stati autorizzati dall'Unione, al pari di quanto avviene nelle competenze esclusive[30]. Mentre nella competenza concorrente, come quella in esame, gli Stati devono intervenire nella "*misura in cui l'Unione non ha esercitato la propria*"[31]; non possono, cioè, legiferare sugli elementi disciplinati nell'atto adottato[32].

Si violerebbe, poi, il precetto costituzionale europeo del divieto di discriminazione sulla base del patrimonio[33]. Infatti il Regolamento, a certe condizioni, non impone alle imprese con meno di 250 dipendenti la tenuta dei registri in cui annotare il trattamento dei dati[34]. Tuttavia tale l'obbligo, per di più soggetto a sanzione pecuniaria amministrati-

[27] Emblematico il considerando 52 che, in riferimento alla tutela dei dati sensibili, afferma che le deroga al divieto del loro trattamento dovrebbe essere consentita anche quando è prevista dal diritto degli Stati membri.
[28] Considerando 9.
[29] M. E. Bartoloni, *Competenze puramente Statali e diritto dell'Unione europea*, in *Il diritto dell'Unione europea*, 2015, p. 339.
[30] Art. 2.1 TUE.
[31] Art. 2.2 TUE.
[32] Protocollo n. 25.
[33] Art. 21 Carta dei diritti fondamentali dell'Unione europea, cit..
[34] Art. 30.5.

va[35], permane per la persona fisica professionista la cui prestazione è prevalentemente di natura personale, caratterizzata cioè dalla quasi assenza di impiego di capitali e lavoro altrui, e che per tale fatto, *a fortiori*, si avvicina all'impresa con meno di 250 dipendenti. Quindi, fermo il dato politico di individuare l'esenzione per le piccole e medie imprese, nessuna giustificazione si rinviene per mantenere tale obbligo in capo al professionista. Si trattano, così, in modo diverso situazioni patrimoniali analoghe.

Sembrerebbero violati, anche, i presupposti stabiliti dai trattati[36] per il conferimento della delega alla Commissione, per l'adozione di atti giuridici vincolanti. Infatti, in tema dei diritti dell'interessato, tra cui rientrano soprattutto le informazioni e comunicazioni che il titolare deve fornire nel rispetto del principio di trasparenza, l'art. 29 del regolamento conferisce alla Commissione il potere di adottare atti delegati "*al fine di stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate*". La parola "stabilire" va intesa come precisare e dunque è sinonimo di "integrare" l'atto legislativo di base[37]. Ciò posto si osserva che la delega sembra riguardare gli atti essenziali del regolamento, poiché la Commissione può incidere non solo sulle informazioni che costituiscono lo "zoccolo duro" dei di-

[35] Art. 83.4 lett. *a)*.
[36] Art. 290 TFUE.
[37] La Corte dopo aver tracciato la distinzione tra "*La delega di un potere di «integrare» un atto legislativo,* [che] *infatti, consiste semplicemente nell'autorizzare la Commissione ad attuare tale atto. Qualora essa eserciti un tale potere, il suo mandato è limitato allo sviluppo in dettaglio, nel rispetto dell'integralità dell'atto legislativo adottato dal legislatore, degli elementi non essenziali della specifica normativa che il legislatore non ha definito*" (41) e "*La delega di un potere di «modificare» un atto legislativo* [che]*, invece, consiste nell'autorizzare la Commissione a emendare o abrogare elementi non essenziali previsti in tale atto dal legislatore. Qualora la Commissione eserciti un tale potere, essa non è ovviamente tenuta ad agire nel rispetto degli elementi che il mandato accordatole mira a «modificare»*" (42), ritiene che il verbo specificare sia sinonimo di integrare (punto 47)*,* cfr. CGUE, 17 marzo 2016, causa C-286/14, *Parlamento europeo c. Commissione*, punto 41*,* in *ECLI: ECLI:EU:C:2016:183.*

ritti della persona fisica ma anche sulle modalità di comunicazione che sono reputate altrettanto fondamentali in quanto permeate dal principio di trasparenza.

3. La definizione dei dati

In merito al concetto di "dati personali", la portata "globale" della tutela si percepisce non tanto nella nozione di dato personale, definita, al pari della direttiva[38], come le informazioni riguardanti una persona fisica che concorrono ad identificarla, quanto nell'aumento degli elementi che conducono all'identificazione, quali il nome, i dati relativi all'ubicazione, gli elementi genetici, e un identificativo *on line*[39]. Quest'ultimo a sottolineare l'adeguamento della normativa al progresso tecnologico.

Specifica tutela viene riservata ai dati c.d. sensibili[40] il cui novero si arricchisce rispetto alla direttiva. Ai dati relativi alla vita sessuale si affianco quelli relativi all'orientamento sessuale. Si specifica, caso mai ce

[38] Art. 83.4 lett. *a)*.

[39] Considerando 29: indirizzi IP, marcatori temporanei (*cookies*), identificativi di altro tipo, come i tag di identificazione a radiofrequenza. CGUE, 19 ottobre 2016, causa C-582/14, *Patrick Breyer c. Bundesrepublik Deutschland***,** in *ECLI:EU:C:2016:779*, secondo cui l'indirizzo IP dinamico (ossia quello, provvisorio, assegnato ad ogni connessione a Internet e sostituito in caso di successive connessioni, e non indirizzi IP «statici», che sono invariabili e consentono l'identificazione permanente del dispositivo connesso alla rete) va considerato come dato personale poiché consente l'identificabilità dell'utente (intestatario del contratto di accesso) tramite l'incrocio con i dati raccolti dal *provider*. Di conseguenza, gli operatori di un sito *web* sono ammessi a trattare i dati personali per i loro interessi legittimi, che nel caso esaminato dalla Corte erano costituiti dalla protezione della rete e del sito *web*, in particolare per ricercare i responsabili di attacchi informatici. Trattamento che per tali fini può avvenire anche senza il consenso. Mentre la raccolta degli IP non è ammessa per fini diversi, quali ad esempio il contrasto alle violazioni del *copyright*, poiché esso non rientra negli interessi legittimi dei gestori del sito.

[40] Tale qualificazione, assente nell'art. 9, si rinviene nel considerando 51.

ne fosse bisogno, che il dato «origine razziale» non implica l'accettazione da parte dell'Unione di teorie che tentano di dimostrare l'esistenza di razze umane distinte[41]. Fanno il loro ingresso i dati biometrici ottenuti cioè da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali, quali l'immagine facciale o i dati dattiloscopici. Mentre non sono più considerati sensibili e nemmeno rientranti nell'ambito di applicazione del regolamento quelli relativi alle condanne penali e ai reati, il cui trattamento e l'eventuale registro delle condanne vengono affidati all'autorità di pubblica sicurezza[42]. Essi invece sono considerati tali dalla Convenzione n. 108.

Si amplia, inoltre, l'elenco della categoria dei dati medici: i dati relativi alla salute, presenti nella direttiva senza indicazione alcuna, vengono ora definiti come quelli concernenti la salute fisica e mentale comprese le prestazioni di assistenza sanitaria che rilevino tali informazioni[43]. Essi si differenziano dai dati genetici perché quest'ultimi risultano dall'analisi di un campione biologico della persona: esempio il DNA.

I dati sensibili sono sottoposti a diversi livelli di protezione. In primo luogo viene sancito un divieto generale di trattamento, suscettibile di essere derogato per soddisfare diverse garanzie, in parte già presenti nella direttiva[44] quali la difesa in giudizio di un diritto o un interesse vitale dell'interessato; altre nuove come l'esercizio di diritti e obblighi del titolare del trattamento in materia di diritti del lavoro e della sicurezza sociale.

Viene riconfermata la tutela più stringente[45] nel momento in cui essi

[41] Considerando 51.
[42] Considerando 19; Art. 10, già art. 8.5 direttiva.
[43] Per alcune esemplificazioni v. considerando n. 35.
[44] Considerando 25, 34, 51-54; art. 9. Art. 8 direttiva.
[45] Tutela serrata già confermata dalla Corte di Strasburgo. La vicenda riguardava un cittadino inglese affetto da HIV, che aveva commesso una serie di reati sessuali. Successivamente veniva anche condannato per omicidio colposo poiché aveva deliberatamente esposto le sue vittime al rischio di infezione da HIV. Con tale sen-

siano collegati ad attività della sanità pubblica[46]. Il trattamento, in tale ambito, è ammesso per motivi di interesse pubblico (quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici), purché i dati siano trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale[47]. Allo stesso modo il trattamento è ammesso per finalità di medicina preventiva o di medicina del lavoro, di diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari, che si fondano anche su un contratto con un professionista della sanità il quale deve essere sottoposto al segreto professionale. In tali ipotesi la persona fisica non può pretendere la cancellazione dei suoi dati[48].

Preme evidenziare come la tutela dei dati relativi alla salute, approntata dal Regolamento in ambito sanitario, violerebbe il principio di attribuzione delle competenze. Il sistema sanitario, nella definizione del legislatore sovranazionale è composto anche dalle risorse destinate all'assistenza sanitaria, dalle prestazioni di assistenza sanitaria, dalle di modalità di accesso[49]. Il sistema così inteso è finalizzato alla tutela e al miglioramento della salute della persona. Quest'ultimi obiettivi tuttavia

---

tenza il giudice aveva imposto che i nominativi del condannato ed i documenti del processo dovevano rimanere riservati per 10 anni, nonostante il condannato avesse chiesto un periodo di secretazione più lungo. La Corte Edu ha ritenuto che il decennio era breve e violava l'art. 8 della CEDU, poiché la protezione dei dati medici è di fondamentale importanza per il godimento del diritto al rispetto della vita privata e familiare, in particolare quando si tratta di informazioni su infezioni da HIV, a causa della stigmatizzazione derivante da questa condizione in molte società, v. CEDU, 25 febbraio 1997, ricorso n. 22009/93, *Z. c. Finlandia*, §§ 94 e 112. Sentenze 27 agosto 1997, ricorso n. 20837/92, *M. S. c. Svezia;* 10 ottobre 2006, ricorso n. 7508/02, *L. L. c. Francia*; 17 luglio 2008, ricorso n. 20511/03, *I. c. Finlandia*; 28 aprile 2009, ricorso n. 32881/04, *K. H. E altri c. Slovacchia*; 2 giugno 2009, ricorso n. 36936/05, *Szuluk c. Regno Unito*, tutte in *www.echr.coe.int*.

[46] Per la nozione ampia di sanità pubblica v. considerando 54.

[47] CEDU, 25 novembre 2008, ricorso n. 23373/03, *Biriuk c. Lituania*, in *www.echr.coe.int*.

[48] Art. 20.

[49] Considerando 54.

rientrano nella competenza di coordinamento[50], con la conseguenza di attirare nella loro orbita gravitazionale anche la tutela dei dati alla salute, poiché, come detto, essi sono definiti espressamente come connessi alle prestazioni di assistenza sanitaria. In sintesi: poiché i dati sulla salute, per definizione legislativa, sono connessi alle prestazioni sanitarie e le medesime a loro volta sono misure finalizzate al miglioramento della salute; miglioramento che è ricompreso nelle competenze di coordinamento, anche i dati sulla salute vi dovrebbero far parte. Si ricordi che in tale tipologia di competenza l'Unione interviene per "completare" l'azione degli Stati membri non per consentire loro, come stabilito nel Regolamento, di introdurre ulteriori condizioni, comprese le limitazioni.

4. I soggetti destinatari

Il Regolamento designa due categorie di soggetti contrapposti: i primi beneficiari del diritto alla protezione dei dati personali, i secondi destinatari degli obblighi di protezione.

I beneficiari definiti anche come gli interessati[51], sono unicamente le persone fisiche viventi[52], che si trovano nell'Unione[53], a prescindere dalla loro nazionalità o dalla loro residenza[54]. Riprova del valore "uomo"[55] della tutela viene evidenziata in riferimento modalità del consenso al trattamento dei propri dati espresso dal minore (di età compresa tra i 13 ed i 16 anni), nella ipotesi in cui egli sia parte di un contratto. In particolare quando il minore richieda ad una società un servizio erogato a pagamento[56], il consenso al trattamento dei dati è sempre necessario a

[50] Art. 6.1 TFUE.
[51] Art. 3 comma 2.
[52] Art. 1, considerando 14 e 27.
[53] Art. 3 comma 2.
[54] Considerando 2 e 14.
[55] Considerando 4.
[56] Servizio erogato a distanza (fornito senza la presenza simultanea delle parti), per

prescindere dal fatto che la minore età sia una causa di invalidità del negozio sulla base della normativa degli Stati membri[57].

Non sono annoverate, invece, le persone giuridiche. Tuttavia la loro non inclusione nei destinatari del diritto al trattamento non significa che siano sfornite di garanzia europea nella materia *de qua*. La Corte di giustizia nella causa *Volker*[58], riferendosi alla pubblicazione di dati personali relativi ai beneficiari di aiuti agricoli, ha considerato che "*le persone giuridiche possono invocare la tutela degli artt. 7 e 8 della Carta nei confronti di una simile identificazione solamente qualora la ragione sociale della persona giuridica identifichi una o più persone fisiche.* […Il] *rispetto del diritto alla vita privata con riguardo al trattamento dei dati personali, riconosciuto dagli artt. 7 e 8 della Carta,* [è] *riferito ad ogni informazione relativa ad una persona fisica identificata o identificabile […]*". In riferimento ai professionisti i giudici del Lussemburgo nella predetta vicenda hanno stabilito che «*[…] è irrilevante la circostanza che i dati pubblicati attengano ad attività professionali […]. La Corte europea dei diritti dell'uomo ha dichiarato, a tale proposito, con riguardo all'interpretazione dell'art. 8 della CEDU, che l'espressione "vita privata" non deve essere interpretata in modo restrittivo e che "nessun motivo di principio consente di escludere le attività professionali [...] dalla nozione di "vita privata"*».

La Convenzione n. 108, poi, facoltizza le Parti contraenti ad estendere la tutela prevista per le persone fisiche anche alle persone giuridiche.

Per ciò che riguarda il lato passivo, ossia i soggetti obbligati, si individuano due macro aree. Le autorità pubbliche ove vi sono sacche di parziale immunità dal Regolamento, come l'autorità giudiziaria

via elettronica (inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento e di memorizzazione di dati), e mediante trasmissione di dati su richiesta individuale.

[57] Considerando 38; art. 6 comma 1 lett. *a)*; art. 8; art. 4 n. 25.

[58] CGUE, 9 novembre 2010, cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, in *Racc.* 2010, I-11063, punti 53, 55 e 59.

nell'esercizio delle proprie funzioni giurisdizionali. L'altra categoria viene individuata nei professionisti[59] e nelle società – siano esse di persone o di capitali – anche se aggregate in gruppi societari costituiti da una controllante e da controllate.

Tutti gli obbligati dal regolamento hanno in comune tre elementi. Innanzitutto il "trattamento", definibile, in generale, come la raccolta, la conservazione e la diffusone dei dati. Esso può essere automatizzato (completamente o parzialmente) oppure manuale[60]. Si noti che rispetto alla direttiva il trattamento comprende attività ulteriori. Viene introdotto, ad esempio, il concetto di "profilazione" cioè l'utilizzo di dati per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute l'ubicazione o la salute della persona. Compare poi la "pseudonimizzazione": i dati personali non possono più essere attribuiti ad una persona specifica senza l'utilizzo di informazione aggiuntive che vengono custodite separatamente. Scompare il termine "congelazione" del dato, sintomatico di perpetuità del trattamento, surrogato dal suo opposto: il diritto alla cancellazione del dato (c.d. diritto all'oblio).

Il secondo elemento è la figura del "titolare del trattamento" ossia il soggetto che stabilisce le finalità ed i mezzi del trattamento dei dati, che nella direttiva veniva definito "responsabile del trattamento". Inoltre esso sarà individuato anche dal diritto dell'Unione o degli Stati membri qualora le finalità ed i mezzi sono stabiliti dal diritto dell'UE o degli Stati membri.

Il terzo elemento è il "responsabile del trattamento" cioè il soggetto munito di competenze tecniche, professionali e organizzative che effettua il trattamento dei dati per conto del titolare del trattamento, sulla base di un contratto, e con possibilità di delega del trattamento se autorizzato[61].

[59] Considerando 18; art. 14 in riferimento al segreto professionale; art. 23 in riferimento alla deontologia.
[60] Considerando 15 e Art. 4.
[61] Artt. 4 e 28.

Sia il titolare che il responsabile del trattamento designano il responsabile della protezione dei dati (*data protection officer*) scelto tra i loro dipendenti o su base di un contratto di servizi, che sarà coinvolto in tutte le attività di trattamento, fornendo a tal fine consulenza ed interfacciandosi con l'autorità pubblica di controllo[62].

5. Ambito di applicazione territoriale

La descrizione delle due categorie di soggetti antagoniste è utile per comprendere l'ambito di applicazione materiale del Regolamento. Occorre ricordare, a tal fine, che i dati personali sono connessi con i beni prodotti/scambiati dall'impresa, con i servizi erogati sia da professionisti sia dalle pubbliche autorità nell'ambito dei loro doveri istituzionali.

Il Regolamento quindi troverà applicazione quando almeno uno dei due protagonisti sia fisicamente presente nel territorio dell'Unione. Evenienza che si può verificare quando il titolare o il responsabile del trattamento sono stabiliti a titolo principale o secondario all'interno dell'Unione europea, indipendentemente dal fatto che il trattamento sia effettuato in territorio *extra* UE. L'altra ipotesi di applicazione si verificherà quando le persone fisiche sono nel territorio dell'UE e sono destinatari di beni o servizi, forniti dal responsabile o dal titolare non stabiliti[63]; come pure quando l'interessato tenga un comportamento monitorato da tali soggetti non presenti. Quest'ultimi designeranno per iscritto un loro rappresentante stabilito nell'UE che avrà il compito di interagire con gli interessati e le autorità nazionali preposte al controllo sul coretto trattamento dei dati[64].

[62] Artt. 37-39.
[63] Considerando 22, 23, 24; art. 3.
[64] Art. 27.

6. I principi generali ed i diritti del proprietario dei dati

Un breve accenno meritano i principi generali stabiliti dal Regolamento, in parte già previsti in parte dalla direttiva. La regola generale è caratterizzata dal fatto che il trattamento dei dati è consentito solo per finalità previste dalla legge statale o europea, e deve essere basato sul consenso espresso generalmente per ciascuna di tali finalità. Tuttavia si ammette il trattamento per una finalità diversa da quella per la quale i dati personali sono stati inizialmente raccolti e non basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri, a condizione che il responsabile del trattamento valuti l'esistenza di alcuni indici fissati dal Regolamento[65].

Merita, poi, di essere menzionata la precisazione del principio di minimizzazione dei dati: si richiede che essi siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

La liceità del trattamento poggia anch'essa sui medesimi criteri già previsti dalla direttiva[66]. Al riguardo la novità di rilievo è la definizione di "consenso inequivocabile", inteso come manifestazione dell'assenso fornita mediante dichiarazione o azione positiva inequivocabile[67]. Si prevede, inoltre, che qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato lo ha prestato. Se il consenso è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Altrimenti nessuna parte di una tale dichiarazione, in quanto resa in violazione del Regolamento, è vincolante. L'interessato, poi, ha il diritto di revocare il proprio consenso in qualsiasi momento: la revoca opera per il futuro non pregiudicando la

[65] Artt. 5 e 6; art. 6 direttiva.
[66] Art. 6; art. 7 direttiva.
[67] Considerando 32, art. 4 n. 11.

liceità del trattamento basata sul consenso conferito prima della stessa. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto[68]. Si precisa poi che il responsabile del trattamento non è obbligato ad acquisire ulteriori informazioni per identificare l'interessato al solo fine di rispettare una disposizione del presente regolamento[69].

7. Gli obblighi dei tenutari dei dati

I diritti degli interessati vanno letti anche come corrispondenti obblighi in capo al titolare e/o responsabile del trattamento, poiché questi ultimi hanno una responsabilità generale in merito al rispetto di tali prerogative (*accountability*). Agli obblighi, ricavabili da questa lettura speculare, si devono aggiungere anche quelli specificamente imposti dal Regolamento. Innanzitutto, in ossequio al principio di trasparenza, la persona fisica ha diritto alle informazioni e alle comunicazioni relative al trattamento (in particolare alle finalità e ai soggetti tenuti al trattamento). Notizie che devono essere fornite, per iscritto, dal titolare del trattamento al momento della raccolta; devono poi essere facilmente accessibili e comprensibili, redatte con un linguaggio semplice e chiaro[70]. Rispetto alla direttiva si amplia il novero delle informazioni da fornire sia quando i dati siano raccolti presso la persona fisica[71] sia quando la raccolta non avvenga presso la medesima[72]. Viene potenziato anche il contenuto del diritto

[68] Art. 7.
[69] Art. 10.
[70] Considerando 39, artt. 12, 13 e 14.
[71] Art. 13; art. 10 direttiva.
[72] Art. 14; art. 11 direttiva.

di accesso ai propri dati[73]; si rafforza il diritto di riceve su supporti anche informatici una copia dei propri dati se il trattamento si basava sul consenso; si prevede la possibilità di comandare al titolare il trasferimento di dati direttamente ad altri soggetti (c.d. portabilità)[74]. Vengono introdotti nuovi istituti come il diritto alla rettifica dei dati se inesatti o il diritto di integrarli se incompleti[75]. Si disciplina il nuovo istituto della cancellazione dei dati[76] di origine pretoria.

Per quanto riguarda le misure di protezione, specificamente previste, il Regolamento impone anche al titolare e/o responsabile del trattamento l'adozione di sistemi volti a scongiurare la violazione o i rischi di violazione del trattamento dei dati. Tali soggetti sono tenuti a dare la prova di aver posto in essere concretamente gli strumenti idonei: *onus probandi* alleggerito dall'adesione a codici di condotta o dall'ottenimento di certificazioni rilasciate da apposite autorità[77].

In particolare tra le prescrizioni imposte dal Regolamento, oltre alla tenuta di registri in cui annotare le attività di trattamento[78], si segnala la progettazione di servizi, ossia di misure tecniche e organizzative, per garantire la protezione dei dati sin dal momento del loro trattamento (c.d. *privacy by design*)[79]. L'intento è quello di prevenire una lesione dei dati come illustrata esemplificativamente nel caso *I. c. Finlandia*[80]. La vicenda riguardava una ricorrente che, nel processo interno, non era stata in grado di dimostrare che altri dipendenti dell'ospedale presso cui era impiegata, avevano avuto accesso alle sue cartelle cliniche sanitarie in modo illecito. La violazione del proprio diritto alla protezione dei dati, asserita dalla ricorrente, era stata pertanto respinta dai giudici nazionali. La

[73] Art. 15.
[74] Art. 20.
[75] Art. 16.
[76] Art. 17.
[77] Vedi Capo IV del Regolamento.
[78] Art. 30.
[79] Art. 25.
[80] CCEDU, ricorso n. 20511/03, *I. c. Finlandia*, cit..

Corte EDU, per contro, ha concluso che vi era stata una violazione dell'articolo 8 della CEDU, poiché il sistema dei registri dell'ospedale per la gestione delle cartelle cliniche non consentiva di chiarire retroattivamente quale uso fosse stato fatto dei registri dei pazienti. Infatti il sistema indicava solamente le ultime cinque consultazioni più recenti, le quali venivano cancellate subito dopo il ritorno delle cartelle negli archivi. La Corte EDU ha ritenuto decisivo il fatto che il sistema dei registri, in uso nell'ospedale, fosse stato chiaramente in contrasto con gli obblighi legali previsti dalla normativa nazionale; aspetto che non aveva ricevuto la debita considerazione da parte dei giudici nazionali.

8. Le autorità di controllo

L'osservanza dei diritti (conferiti alle persone) e degli obblighi (imposti alle imprese e pubbliche amministrazioni) si sviluppa su un duplice livello: sul piano domestico viene affidata alle singole autorità di controllo nazionali, alla cui vigilanza si sottraggono le autorità giurisdizionali. Sul territorio dell'intera Unione viene conferita alle autorità di controllo nazionali che cooperano eventualmente con la Commissione attraverso il meccanismo di coerenza.

Per quanto riguarda la vigilanza in ambito nazionale, le autorità (designate e rette dal diritto interno) godono di indipendenza da ogni potere. In caso in cui il titolare del trattamento operi in più Stati membri l'autorità di controllo sarà quella in cui il titolare ha l'amministrazione centrale, cioè lo stabilimento principale (c.d. autorità capofila). Tale autorità collaborerà e coopererà con quelle istituite nei diversi Stati, in cui il titolare ha altri stabilimenti (c.d. autorità interessate), ma sarà l'unica ad emettere una decisione nei confronti del soggetto vigilato e l'unica a cui la persona fisica può presentare un reclamo. Qualora invece la trattazione dei dati è circoscritta in un solo degli Stati membri, l'autorità interessata può emettere la relativa decisione, previa informazione

all'autorità capofila ed a condizione che quest'ultima non decida di avocare a sé la questione (c.d. Meccanismo dello sportello unico). Possibili conflitti tra tali autorità, riguardanti l'adozione di una decisione nei confronti del soggetto vigilato, verranno composti all'interno del "meccanismo di coerenza", ferma *medio tempore* la possibilità dell'autorità interessata di adottare misure d'urgenza, circoscritte al proprio ambito nazionale per la tutela delle persone fisiche[81].

I compiti delle autorità possono essere classificati in informativi, con cui favorisce la consapevolezza in capo agli interessati e ai titolari circa i rispettivi diritti e obblighi; propositivi con cui si agevola l'adozione di codici di condotta ed i meccanismi di certificazione; normativi in senso ampio fornendo consulenza agli Stati per l'adozione di misure legislative in tema di trattamento, adottando le norme vincolanti d'impresa e clausole contrattuali (cioè gli strumenti per trasferire i dati verso organizzazioni internazionali o Paesi terzi), e decidendo sui reclami presentati dall'interessato[82].

Le suddette prerogative vengono realizzate tramite tre tipologie di poteri. In primo luogo con i poteri di indagine che si spingono fino all'accesso nei luoghi del titolare del trattamento ivi inclusi i sistemi di tenuta dei dati. Poteri correttivi che partono dalla diffida all'afflizione di sanzioni amministrative, oltre la possibilità di agire in giudizio per far rispettare il Regolamento. Infine poteri autorizzativi e consultivi come l'accreditamento degli organismi di certificazione e l'approvazione dei codici di condotta. Gli Stati possono ampliare il novero dei poteri delle autorità. Poteri il cui corretto esercizio è sempre garantito dal ricorso giurisdizionale[83].

Le autorità di vigilanza, inoltre, cooperano tra loro scambiandosi informazioni ed esercitando congiuntamente i poteri di cui sono munite, con possibilità di delegare le operazioni all'autorità di vigilanza interessata. Lo Stato membro è tenuto a risarcire i danni causati, nel proprio

[81] Art. 60.
[82] Art. 57.
[83] Art. 58.

territorio, sia dalla sua autorità di vigilanza sia dal personale dell'autorità di controllo ospitato, salvo in quest'ultimo caso il rimborso da parte dello Stato di riferimento.

Al fine di applicare in modo coerente il Regolamento in tutto il territorio dell'Unione è istituito in meccanismo di coerenza per la cooperazione tra le autorità di controllo.

Il meccanismo, tendenzialmente, opera quando il trattamento dei dati riguarda un numero significativo di interessati in vari Stati membri. Infatti tra i suoi compiti rientrano quelli di emettere parerei[84] e comporre le controversie[85]. In un caso il parere viene reso se richiesto della Commissione o da qualsiasi autorità di controllo, quando sia dubbio che una autorità di vigilanza non abbia rispettato gli obblighi relativi all'assistenza reciproca o alle operazioni congiunte. Nell'altro caso il parere, di natura preventiva obbligatoria, viene fornito qualora l'autorità di controllo adotti una misura intesa a produrre effetti giuridici, come nel caso di adozione del codice di condotta indirizzato ad attività in vari Stati membri. In entrambe le evenienze se l'autorità comunica di non uniformarsi al parere si apre la fase di composizione in cui il "meccanismo" deve rendere una decisione vincolante, entro un termine. La decisione vincolante viene resa, come detto, anche in caso di conflitti tra l'autorità capofila e quella interessata.

Il meccanismo opera in concreto tramite il Comitato europeo per la protezione dei dati[86]. Si tratta di un organismo dell'Unione, qualificato come indipendente[87], munito di autonomia statutaria[88], e dotato di personalità giuridica. Per quanto riguardo la sua struttura è composto da un presidente che lo rappresenta. Ne fanno parte anche il Garante europeo della protezione dei dati e la figura di vertice dell'autorità di controllo

[84] Art. 64.
[85] Art. 65.
[86] Sostituisce il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito con direttiva.
[87] Art. 69.
[88] Art. 72.

di ciascuno Stato membro. La Commissione partecipa alle attività del Comitato senza diritto di voto. Il Comitato è assistito da un segretariato messo a disposizione dal Garante europeo della protezione dei dati. Il personale del Garante europeo, impegnato nell'assolvimento dei compiti attribuiti al Comitato, è sottoposto esclusivamente alle istruzioni del presidente del Comitato e deve riferire solo a quest'ultimo.

Il meccanismo di coerenza lungi dall'essere un sistema di regolamentazione di competenze sul controllo, sembra quasi assurgere ad una sorta di nuova istituzione dell'Unione, dotata di ampia discrezionalità valutativa e di azione in riferimento a compiti dai confini piuttosto estesi. Sebbene esso non sia previsto nei Trattati, possiede caratteristiche che lo accomunano con le istituzioni europee. La Corte di giustizia ha avuto modo di precisare[89] che il termine istituzione comprende anche quegli organismi che sebbene non elencati nei Trattati hanno il compito di contribuire alla realizzazione degli scopi dell'Unione con conseguente loro responsabilità extracontrattuale. Il meccanismo soddisfa le statuizioni della Corte, in quanto avendo il compito di applicare in modo coerente il Regolamento in tutto il territorio dell'Unione, ne persegue i fini, vale a dire contribuire alla realizzazione di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche. Inoltre la personalità giuridica di cui è munito lo rende tenuto a risarcire i danni che ha causato nell'adempimento delle competenze eserciate.

La connotazione di istituzione emerge anche dai poteri normativi "in senso lato" in grado di incidere in modo diretto sulla sfera giuridica dei soggetti vigilati. L'assunto trova conforto nella definizione di istituzione che può trarsi dal caso *Van Gend an Loos*[90]. Si è poc'anzi osservato

[89] CGUE, 3 marzo 1988, causa C-85/86, *Commissione c. BEI*, in *Racc.* 1998, p. 01281; 2 dicembre 1992, causa C-370/89, *SGEEM e Etroy c. BEI*, in *Racc*. 1992, p. I-006211.

[90] CGUE, 5 febbraio 1963, causa C- 26/62, *Van Gend en Loos / Administratie der Belastingen* in *Racc*. 1963, p. 0003 "... organi investiti istituzionalmente di poteri

che nel caso di adozione, da parte di una autorità di vigilanza, del codice di condotta che si riferisca ad attività in vari Stati membri, l'autorità deve preventivamente richiedere un parere al Comitato. Questi se ritine il progetto del codice conforme al regolamento trasmette tale parere alla Commissione la quale con atti di esecuzione (procedura d'esame) può conferire al codice validità generale all'interno dell'Unione[91]. Al di là del dato formale dell'atto di esecuzione della Commissione, la valenza normativa del codice risiede a monte nel parere, senza il quale la Commissione non potrebbe attivarsi.

La potestà normativa emerge più chiaramente ponendo mente ai compiti attribuiti al Comitato. Infatti deve emettere un parere – obbligatorio nella richiesta e vincolante nel risultato – sulle norme giuridiche, adottate dall'autorità di controllo nazionale, che disciplinano in modo standardizzato il vincolo tra il titolare ed il responsabile del trattamento[92]. Il potere normativo sembrerebbe conferito anche nel compito di pubblicare le linee guida, le raccomandazioni e le migliori prassi per promuovere l'applicazione coerente del Regolamento[93]: il contenuto di tali strumenti costituirà ragionevolmente l'oggetto della consulenza fornita alla Commissione per le eventuali proposte di modifica del Regolamento[94].

Su un piano più generale, il meccanismo di coerenza, conferma la tendenza del legislatore europeo di avocare a se la regolamentazione di alcune competenze che, in quanto affidate agli Stati membri, generano una tutela frammentata che inficia il corretto funzionamento del mercato. L'intervento legislativo dell'Unione però non esautora completamente i Paesi membri, poiché a causa della complessità della materia, l'Unione non riuscirebbe a verificarne la completa osservanza. A tal fi-

---

sovrani da esercitarsi nei confronti sia degli Stati membri sia dei loro cittadini".
[91] Art. 40.
[92] Art. 28.
[93] Art. 70.1 lett. *e)*.
[94] Art. 70.1 lett. *b)*.

ne il legislatore sovranazionale crea meccanismi caratterizzati non solo da un controllo ripartito tra una autorità centrale europea e le autorità nazionali, ma anche muniti di poteri normativi e di composizione di conflitti insorti tra le stesse[95].

9. Considerazioni conclusive

Dall'analisi delle disposizioni, l'interrogativo se i dati personali risultino maggiormente tutelati, rispetto alla direttiva, non riceve una risposta agevole. Non c'è dubbio che vi sia un aumento delle garanzie, le quali però nel concreto devono essere fornite dall'impresa o dalla pubblica amministrazione. È plausibile, pertanto, che gli obbligati alla protezione dovranno supportare costi per adempiere al Regolamento: la realizzazione di strutture e sistemi interni, l'ottenimento di certificazioni, come pure prestazioni rese da soggetti esterni (es. *data protection officer*). È inoltre ragionevole supporre che le imprese si accolleranno oneri assicurativi per garantirsi da eventuali inadempimenti della normativa europea, forieri di danni. Costi che inevitabilmente verranno scaricati sulla stessa persona fisica in termini di aumento: *i)* dei prezzi dei beni/servizi acquistati (in caso di imprese); *ii)* della tassazione in generale per gli oneri delle pubbliche amministrazioni.

[95] Il riferimento è al Meccanismo unico di vigilanza bancaria. L'Unione europea, infatti, ha trasferito in capo alla BCE, i compiti esclusivi di vigilanza sulla solvibilità e sulla solidità delle banche ed imprese d'investimento significative, ubicate negli Stati della zona euro. L'istituzione europea, a far data dal 4 novembre 2014, esercita tale supervisione, assistita dalle autorità di controllo nazionali (costituite generalmente dalle banche centrali nazionali). La sinergia si svolge all'interno del Meccanismo unico di vigilanza, istituito dal Regolamento UE 1024/2013, e completato dal Regolamento della BCE 468/2014. La supervisione degli enti meno significativi rimane affidata, invece, alla vigilanza delle Autorità nazionali le quali però subiscono diversi gradi interferenza da parte della BCE: dal costante e reciproco scambio di informazioni fino all'assunzione in capo alla stessa della vigilanza, esautorando le Autorità nazionali.

Ad opacizzare il quadro concorre, poi, la possibilità per gli Stati non solo di derogare la disposizione europea, ma anche di fissare l'obbligo giuridico del trattamento.

Il dubbio sul reale effetto utile della normativa e quindi sul rispetto del principio di sussidiarietà, si aggrava, altresì, ponendo mente alla regolamentazione dei trasferimenti dei dati in Paesi *extra* UE, attraverso lo strumento della decisione di adeguatezza[96], in cui l'azione della Commissione rivela, ad oggi, tutta la sua inefficacia. Il riferimento è alle recenti vicende sul trasferimento dei dati negli Stati Uniti. La Corte di giustizia nel 2015[97] aveva annullato il c.d. "*Safe Harbor*", cioè la decisione della Commissione, adottata sulla base della direttiva 95/46, che aveva consentito il trasferimento dei dati negli Stati Uniti, poiché ritenuti capaci di offrire un livello di protezione adeguato, cioè conforme alla normativa europea. Per la Corte, invece, la legislazione americana autorizzava in maniera generale ed indiscriminata la conservazione di tutti i dati personali, trasferiti dall'Unione verso gli Stati Uniti, senza alcuna distinzione, limitazione o eccezione basate sull'obiettivo perseguito, e senza che fosse previsto alcun criterio oggettivo che permettesse di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore per fini precisi, rigorosamente ristretti ed idonei a giustificare tale ingerenza. Né le normative americane prevedevano alcuna possibilità per il cittadino europeo di avvalersi di rimedi giuridici per accedere ai propri dati personali, oppure per ottenerne la rettifica o la soppressione. Le perplessità di conformità agli standard europei permangono, seppur ridotte, nonostante la sostituzione dell'atto annullato, con la de-

[96] Art. 45.

[97] CGUE, 6 ottobre 2015, causa C- 362/14, *Maximillian Schrems* c. *Data Protection Commissioner*, in *ECLI:EU:C:2015:650*. L. Azoulai-M. van der Sluis, *Institutionalizing Personal Data Protection in Time of Global Institutional Distrust: Schrems*, in *Common Market Law Review*, 2016, p. 1343; M. Nino, *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della Corte di giustizia U.E.*, in *Il diritto dell'Unione europea*, 2016, p. 754.

cisione sullo "scudo UE-USA sulla privacy"[98]. Il Parlamento europeo[99] al riguardo rileva come sia rimasta, sebbene circoscritta, una raccolta di massa di dati e di comunicazioni personali di cittadini non statunitensi. Il carattere generalizzato della raccolta non risulta quindi conforme ai più rigorosi criteri di necessità e proporzionalità stabiliti nella Carta di Nizza. Si evidenzia, poi, come gli strumenti di ricorso per la tutela dei cittadini europei sono ancora complessi, necessitando di soluzioni adeguate per rendere la procedura efficace e di semplice utilizzo.

[98] Decisione di esecuzione (UE) 1250/2016 della Commissione, in *GUUE* 1 agosto 2016, L 207/1. F. Rossi Dal Pozzo, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali (dal Safe Harbour al Privacy Shield)*, in *Rivista di diritto internazionale*, 2016, p. 617; K. Kowalik-Banczyk. *Les aspects transfrontaliers des infractions à la privée par surveillance de masse de part des agences étatiques*, in *Revue générele de droit international public*, 2016, p. 383.

[99] Risoluzione del Parlamento europeo del 26 maggio 2016 sui flussi di dati transatlantici (2016/2727 RSP), P8_TA(2016)0223, in *http://www.europarl.europa.eu*.