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

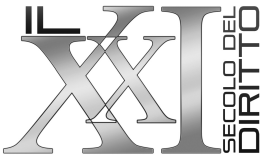
IL MERCATO UNICO DIGITALE

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

Simone Calzolaio
Università degli Studi di Macerata

Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. UE 2016/679

Abstract: Il Reg. UE 2016/679 aggiorna le regole europee in materia di protezione dei dati personali all'avvento della società digitale, introducendo un modello di protezione dei dati personali fondato sulla rischiosità del trattamento, sulla responsabilità del Titolare del trattamento e sulla protezione dei dati sin dal momento della progettazione del trattamento e per impostazione predefinita. Il contributo intende analizzare gli istituti ed i principi che caratterizzano questa riforma.

The GDPR 2016/679 updates the European data protection rules after the advent of digital society by introducing a data protection model founded on the risk-based approach, the controller's accountability and privacy by design and privacy by default. The paper investigates these main novelties introduced by GDPR.

1. Obiettivo del contributo

Obiettivo di questo contributo è delineare le principali novità introdotte dal Reg. UE 2016/679 sotto il profilo dei principi e delle dinamiche del trattamento dei dati personali[1].

È stato osservato che il nuovo Regolamento europeo non abbandona l'approccio essenzialmente riparatorio della Dir. 95/46/CE, ma tenta di completarlo affiancandovi una tutela preventiva fondata sulla strutturale e dinamica responsabilizzazione della filiera soggettiva coinvolta nel trattamento dei dati personali[2]. Accentuando questa impostazione, si discute di un vero e proprio rovesciamento di prospettiva tra Direttiva e Regolamento, la prima incentrata prevalentemente sui diritti dell'interessato, il secondo invece basato sui doveri del Titolare e del Responsabile del trattamento[3].

L'analisi che segue intende focalizzare questo approccio, concentrandosi proprio sulle parti del testo del Regolamento europeo che introducono nozioni e principi che innovano la "gestione" del trattamento dei dati personali[4].

In primo luogo, si osserveranno le ragioni che – muovendo dai considerando del Regolamento europeo – hanno indotto ad approvare il nuovo Reg. in luogo della precedente Direttiva. Quindi, si procederà a descrivere alcune delle principali novità "lessicali" introdotte dal Reg., tentando di inquadrarle nell'ambito delle problematiche che provano ad affrontare. In terzo luogo, si fornirà una descrizione dei nuovi principi

[1] Per una disamina dell'evoluzione della protezione dei dati personali nell'ordinamento italiano ed europeo cfr. L. Califano, *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale scientifica, Napoli, 2016.

[2] M. G. Stanzione, *Genesi e ambito di applicazione*, in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, Milano, 2016, p. 21.

[3] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, pp. 153 ss..

[4] Per una introduzione generale al Reg. europeo in parola cfr. G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 1 ss..

cardine della protezione dei dati personali (*privacy by design* e *by default*). Infine, si cercherà di legare questi principi alla disciplina della valutazione di impatto e alla figura del *Data protection officer*.

In questo modo si intende fornire al lettore un quadro sintetico del modello attraverso il quale il legislatore europeo intende garantire i diritti (vecchi e nuovi)[5] afferenti alla protezione ed alla sicurezza dei dati personali e, contemporaneamente, gli interessi del vecchio continente nel panorama globale.

2. Le ragioni alla base del Reg. UE 2016/679

La lettura dei considerando del Regolamento lascia intravedere, con una certa chiarezza, gli obiettivi e le finalità principali che sono alla base del faticoso processo di elaborazione, durato circa un lustro[6].

Appare evidente che il fine del Regolamento è garantire il diritto fondamentale sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea e ribadito dall'art. 16 TFUE, concernente la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale[7].

In questa prospettiva, l'esigenza primaria che ha suggerito l'adozione di un nuovo set di regole europee è strettamente legata alla

[5] Per una panoramica sui diritti tutelati dal Reg. cfr. i contributi di G. Di Genio, *Trasparenza e accesso ai dati personali*; P. Pacileo, *Profilazione e diritto di opposizione*; V. D'Antonio, *Oblio e cancellazione dei dati nel diritto europeo*; P. Pacileo, *Il diritto alla protabilità*, tutti in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, Milano, 2016, rispettivamente pp. 161 ss., pp. 177 ss., pp. 197 ss., pp. 221 ss..

[6] Cfr. S. Gutwirth-R. Leenes-P. de Hert (edited by), *Reforming European Data Protection Law*, *Law, Governance and Technology Series*, vol. 20, Springer 2015. Per i lavori preparatori del Reg. in parola, cfr. http://eur-lex.europa.eu/procedure/IT/2012_11.

[7] Cfr. F. Donati, *Art. 8. Protezione dei dati di carattere personale*, in R. Bifulco-M. Cartabia-A. Celotto, *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione europea*, Bologna, 2001, pp. 83 ss..

digitalizzazione della società e dell'economia europea (e globale). L'ambiente digitale è costituito dalla produzione, condivisione, elaborazione di un flusso incessante di dati: «*la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività*» e, contemporaneamente, «*sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano*» (cons. 6).

La circolazione di questa massa crescente di dati è un valore da custodire e promuovere, sia all'interno dell'Unione europea, sia nei rapporti con i «paesi terzi» e con le organizzazioni internazionali, ed appare tuttavia necessitare di nuove ed apposite regole europee volte alla garanzia di un elevato livello di protezione dei dati personali.

Attraverso la primaria esigenza di garantire il diritto individuale alla protezione dei dati personali segnatamente in ambiente digitale, le nuove regole europee perseguono altresì il fine di instaurare quel «*clima di fiducia*» e di certezza giuridica – fondato sulla consapevolezza delle persone fisiche di avere il controllo sui propri dati personali – necessario per lo «*sviluppo dell'economia digitale in tutto il mercato interno*» (cons. 7).

Società digitale, certezza giuridica, mercato unico[8]. Il perseguimento di questi obiettivi prioritari si lega strettamente con l'altra grande finalità (in qualche modo, strumentale ed operativa) del Reg. europeo: il superamento della frammentazione giuridica delle norme e delle prassi applicative in tema di protezione dei dati personali sul suolo

[8] Osserva puntualmente G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 1 ss. e spec. par. 3, che «in questo quadro, non si può non considerare il reg. UE n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014, "in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE". I due regolamenti, considerati in una prospettiva unitaria, indicano chiaramente l'intento del legislatore europeo di disegnare un mercato unico digitale, rimuovendo gli ostacoli giuridici costituiti dalla disomogeneità delle norme applicabili».

dell'Unione europea[9].

Si osserva infatti che «*sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche*». La coesistenza di diversi livelli di protezione a livello nazionale rappresenta un ostacolo alla libera circolazione dei dati personali all'interno dell'Unione, un freno all'esercizio delle attività economiche su scala dell'Unione, è in grado di falsare la concorrenza e di impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Si afferma con chiarezza che «*tale divario creatosi* (…) *è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE*» (cons. 9).

La conseguenza di tale osservazione è duplice e decisamente rilevante.

Non sarebbe stato sufficiente procedere ad un aggiornamento, magari radicale, delle regole europee in materia di protezione dei dati personali con una nuova direttiva. Si è reso necessario utilizzare una "nuova" fonte, il regolamento europeo, che è stato ritenuto l'unico strumento in grado di garantire «*un livello coerente di protezione delle persone fisiche*», certezza del diritto e trasparenza agli operatori economici e di «*prevenire disparità*» a livello nazionale (cons. 13), anche sotto il profilo sanzionatorio.

È opportuno almeno accennare al fatto che è stato il cammino della competenza europea in materia di protezione dei dati personali, culmi-

[9] Cfr. D. Erdos, *European Data Protection Regulation and the New Media Internet: Mind the Implementation Gaps*, in *Legal Studies Research, Paper Series*, University of Cambridge, paper n. 30/2015, (attualmente in *Journal of Law and Society*, Dicembre 2016, pp. 534-564) il quale evidenzia la sussistenza di un divario rilevante all'interno dei singoli Stati nazionali europei nella protezione dei dati con specifico riferimento all'utilizzo delle nuove tecnologie.

nato con l'adozione dell'art. 16 del TFUE, che ha reso possibile l'adozione di un regolamento europeo in materia[10]: si tratta di un (raro, come noto, ma) evidente attestato di vitalità delle istituzioni europee, che hanno saputo decifrare il sorgere di un interesse strategico unitario europeo alla protezione dei dati personali e di disporre, conseguentemente, un peculiare titolo di competenza dell'Unione europea[11].

Pertanto, fra le ragioni che hanno condotto alla adozione delle nuove regole europee in materia di protezione dei dati personali delle persone fisiche va annoverata anche l'avvertita esigenza di sostituire la fonte regolamentare alla direttiva[12].

3. Rischio, profilazione, pseudonimizzazione. Il nuovo "dato personale"

Il Reg. contiene una disciplina molto articolata e una serie di definizioni ben più analitica rispetto alla precedente Dir. In questa sede, si vogliono trattare alcuni concetti e definizioni, che appaiono in grado di introdurre al nuovo modello di tutela europea.

Ci si vuole soffermare, pertanto, sui concetti di «*rischio*», «*profilazione*», «*pseudonimizzazione*».

---

[10] Cfr. sul tema H. Hijmans, *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU*, Springer, 2016.

[11] Cfr. B. Cortese, *La protezione dei dati di carattere personale nell'Unione europea dopo il trattato di Lisbona*, in *Dir. Un. Eur*., n. 2 del 2013, pp. 313 ss..

[12] Deve comunque sottolinearsi che, da un lato, il Regolamento europeo appare la fonte del diritto più adeguata per far tesoro dell'ormai ampia elaborazione e dei ripetuti interventi della Corte di giustizia dell'Unione europea (cfr. in particolare, CGUE, 13 maggio 2014, causa C-131/12*, Google Spain SL, Google Inc./Agencia de Protección de Datos (AEPD), Mario Costeja González*.; CGUE, 6 ottobre 2015, causa C-362/14, *Maximillian Schrems/Data Protection Commissioner*; CGUE, 8 aprile 2014, cause riunite n. C-293/12 e n. C-594/12) che avevano già interpretato in modo innovativo e perentorio il diritto dell'unione europea in materia di dati personali. D'altra parte, è opportuno segnalare che il Reg. UE 2016/679, lascia ampi margini di attuazione a livello statale (cfr., ad es., cons. 8, 10, e artt. 8, 9, 23, 80, 85, 87, 88, 90), seppure nell'ambito di stringenti meccanismi di cooperazione e coerenza (capo VII, artt. 60 ss.) volti ad uniformarne l'applicazione a livello europeo.

Si è detto che il Reg. viene adottato per aggiornare la disciplina della precedente Dir. all'avvento della società digitale. A livello scientifico, appare ormai scontato osservare che tra protezione dei dati personali e nuove tecnologie corra un difficile rapporto di compatibilità[13], in forza del quale sembra quasi ineluttabile che all'evolversi della società digitale debba corrispondere la progressiva estinzione delle istanze legate alla tutela della privacy, o in altre parole *the end of privacy*[14]. Questa osservazione sorge dalla analisi della realtà digitale: attualmente è possibile trarre informazioni strettamente personali su una o più persone fisiche semplicemente incrociando dati (né personali, né sensibili, sulla base della vigente normativa europea e italiana)[15] e, poi, altri dati personali. Ciò è agevolato dal fenomeno dei c.d. «*Big data*»[16]: una mole infinita di dati, che viene prodotta ogni giorno dalla vita digitale di persone, imprese, amministrazioni, cose[17], ed ogni giorno trattata e conservata (apparentemente) in quei non-luoghi chiamati *cloud*[18]. Un contesto c.d. *data intensive* in continua evoluzione. Questi dati, se corret-

[13] La dottrina su questo aspetto è ormai sterminata. Cfr., di recente, P. Passaglia, *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità***,** in *Consulta online*, n. 3/2016, http://www.giurcost.org/studi/passaglia7.pdf.

[14] ... così si intitolava un numero speciale della rivista *Science* (vol. n. 347 del 30 gennaio 2015, in http://science.sciencemag.org/content/347/6221/490). Cfr. A. Sarat (a cura di), *A World without Privacy. What Law Can and Should Do?*, Cambridge University Press, 2015.

[15] Cfr. A. Mantelero, *Data Protection, e-Ticketing, and Intelligent Systems for Public Transport*, in *International Data Privacy Law*, 2015, pp. 309 ss..

[16] Per introdursi alla complessità del fenomeno cfr. G. D'Acquisto - M. Naldi, *Big data e privacy by design*, Giappichelli, 2017.

[17] Cfr. U. Pagallo-M. Durante-S. Monteleone, *What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT*, in R. Leenes-R. Van Brakel-S. Gutwirth-P. DeHert (a cura di), *Data Protection and Privacy: (In)visibilities and Infrastructures*, *Law, Governance and Technology Series,* vol. 36, Springer, 2017, pp. 59 ss..

[18] Cfr. M. M. Winkler-J. Mosca, *Cloud computing e protezione dei dati personali*, in M. Fumagalli Meraviglia (a cura di), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica e scontro di civiltà?*, Editoriale Scientifica, Napoli, 2015, pp. 121 ss..

tamente interrogati, sono una fonte di conoscenza smisurata, e di una utilità ed un valore inedito nella storia dell'uomo: ne è nato un nuovo e fiorente settore di ricerca ed industriale, la «*big data analytics*». Quel che interessa in questa sede puntualizzare è che attualmente per trarre informazioni analitiche su singole persone non è più necessario trattare dati personali o sensibili. È sufficiente essere in grado di interrogare correttamente i *big data* e incrociare (*data inference* e *re-identification*) dati non personali per ottenere informazioni personali analitiche, costanti, complete, intime, riservate[19].

Le conseguenze sul piano giuridico sono molteplici[20] e ancora non del tutto intelligibili[21].

Proprio per questo, su un punto si può osservare una certa chiarezza: una volta che un dato (e, quindi, anche un dato personale) è inserito nel circuito digitale, non si può evitare che circoli, che possa essere utilizzato e riutilizzato, comunicato e diffuso, incrociato con altri dati anche di natura completamente diversa, per finalità imprevedibili rispetto alla ragione per cui il dato era stato originariamente prodotto, richiesto, trattato[22].

---

[19] Per una spiegazione del fenomeno dei Big data e della possibilità tecnica – molto contestata nel dibattito internazionale – di farlo convivere con gli strumenti a tutela della protezione dei dati cfr. G. D'Acquisto-J. Domingo-Ferrer-P. Kikiras-V. Torra-Y. A. de Montjoye-A. Bourka, *Privacy by Design in Big Data. An Overview of Privacy Enhancing Technologies in the Era of Big Data analytics*, European Union Agency for network and information security, december 2015, in *http://www.enisa.europa.eu.*

[20] Cfr. F. Di Porto (a cura di), *Big data e concorrenza*, in *Concorrenza e mercato*, numero speciale 23/16, e, in tale volume, in particolare, V. Zeno-Zencovich - G. Giannone Codiglione, *Ten Legal Perspectives on the "Big Data Revolution"*, pp. 29 ss.; per una prima indagine sul rapporto e sui risvolti fra digitalizzazione pubblica e «Big Data» sia consentito rinviare a S. Calzolaio, *Digital (and privacy) by default. L'identità costituzionale della amministrazione digitale*, in *Giornale di storia costituzionale*, n. 31/2016, pp. 185 ss..

[21] Cfr. A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 144 ss..

[22] Cfr. D. Klitou, *Privacy-Invading Tecnologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century*, *Information Technology and Law Series*, vol. 25, Asser press – Springer, 2014.

In termini sintetici, la produzione di un dato in ambiente digitale coincide di norma con l'accettazione di un rischio da parte del soggetto interessato, un rischio che abbraccia il trattamento nel cui ambito quel dato è richiesto e tutti i potenziali trattamenti c.d. secondari.

L'insieme delle disposizioni del Reg. europeo appare trovare le sue fondamenta concettuali su questa osservazione del rischio e della rischiosità della circolazione in rete di dati (e di dati personali), a partire dalla quale si può comprendere quel cambiamento di impostazione rispetto alla dir. ed, almeno in parte, alla normativa vigente in Italia[23]: è vero che il Reg. si concentra prevalentemente nell'imporre obblighi al Titolare ed al Responsabile del trattamento e con questo, in parte, muta o almeno allarga la strategia normativa della precedente Dir., che faceva di alcuni obblighi – in particolare del modello informativa-consenso – un precipitato della disciplina dei diritti dell'interessato; ma ciò avviene nell'ambito di un ardito tentativo di fornire una protezione effettiva dell'interessato, di fronte a "rischi certi" per la protezione dei dati personali in ambiente digitale.

Non a caso, il termine "rischio" (o "rischi") ricorre appena 8 volte nella Dir. e oltre 100 nel Reg., quasi a segnare il passaggio ad una prospettiva improntata al principio di precauzione nella protezione dei dati personali[24].

Ne consegue che, come è stato osservato, elemento caratteristico del Reg. consiste nella strutturale necessità di una valutazione sistematica da parte del Titolare/Responsabile del trattamento dei rischi attuali e

[23] Come osserva A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 144 ss., «è il profilo inerente la responsabilità degli autori del trattamento, in quanto collegata alla gestione del rischio, a rappresentare il nucleo centrale del nuovo quadro di tutela dei dati personali definito dall'Unione europea. In questa prospettiva, istituti centrali sono la valutazione d'impatto sulla protezione dei dati e la consultazione preventiva».

[24] Cfr. M.G. Stanzione, *Genesi ed ambito di applicazione*, in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, Milano, 2016, pp. 21 ss.; sul principio di precauzione cfr. F. De Leonardis, *Il principio di precauzione nell'amministrazione di rischio*, Giuffré, Milano, 2005.

potenziali del trattamento, sia in riferimento alla protezione dei diritti dell'interessato sia in riferimento specifico alla sicurezza dei dati. La ponderazione della rischiosità si lega strettamente con i profili inerenti la responsabilità giuridica per il trattamento e con l'operatività di altri istituti introdotti dal Reg., come la valutazione di impatto[25].

A questo riguardo, il Reg. cerca anche di qualificare il livello del rischio, distinguendo fra rischio generico e rischio elevato. Nelle pieghe del Reg. sembra anche osservarsi l'ipotesi di un rischio basso per i diritti dell'interessato [cons. 80, art. 27, c. 2, lett. *a)*].

Il parametro di valutazione del rischio prende in considerazione la probabilità e gravità di una violazione dei diritti e delle libertà degli interessati a causa o nell'ambito del trattamento[26] e non è rimesso alla mera sensibilità del Titolare del trattamento, ma trova una oggettivazione (dinamica) nella conformità della valutazione ai codici di condotta approvati e/o alle certificazioni approvate e/o linee guida fornite dal comitato europeo per la protezione dei dati e/o indicazioni fornite da un responsabile della protezione dei dati[27].

In particolare, sembrerebbe potersi ritenere che vi sia una sorta di presunzione di elevata rischiosità per i trattamenti che comportano l'utilizzo di nuove tecnologie (cfr. cons. n. 89 e art. 35, c. 1, i quali per-

[25] Cfr. G. Giannone Codiglione, *Risk-based approach e trattamento dei dati personali*, in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, Milano, 2016, pp. 55 ss..

[26] Il cons. 76 afferma che la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

Il cons. 77 afferma che per dimostrare la conformità da parte del titolare del trattamento/responsabile del trattamento è necessario attenersi ai codici di condotta approvati e/o alle certificazioni approvate e/o linee guida fornite dal comitato e/o indicazioni fornite da un responsabile della protezione dei dati.

[27] Il cons. 83 specifica che per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare/responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura.

tanto normalmente dovrebbero essere sottoposti a valutazione di impatto sulla protezione dei dati). Allo stesso modo, almeno per quanto concerne i trattamenti oggetto di valutazione preventiva, la rischiosità può variare nel corso del trattamento e spetta ancora una volta al Titolare procedere ad un riesame (quindi ad una rivalutazione) del rischio (art. 35, u.c.; più in generale, artt. 24, c. 1, e 25, c. 1).

Inoltre, viene specificamente preso in considerazione il rischio per la sicurezza del trattamento, in riferimento al quale viene individuata la "cifratura" quale tecnica idonea a limitare il rischio[28]. Sotto questo profilo, va sottolineato che le misure di garanzia di un adeguato livello di sicurezza del trattamento sono individuate «*tenuto conto dello stato*

[28] Il considerando n. 51 individua, in modo puntuale, i singoli aspetti che devono essere considerati nella valutazione del rischio: «*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o dell'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale; se sono trattati i dati genetici o biometrici per identificare in modo univoco una persona o se sono trattati i dati relativi alla salute o i dati relativi alla vita sessuale e all'orientamento sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi e la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori o se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*».

Il cons. n. 52 specifica che «*La probabilità e la gravità del rischio dovrebbero essere determinate con riferimento alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se il trattamento di dati comporta un rischio elevato. Un rischio elevato è un particolare rischio di pregiudizio dei diritti e delle libertà degli interessati*».

dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere»: si stabilisce pertanto un nesso di proporzionalità fra rischi del trattamento, evoluzione tecnologica e costi di attuazione.

Le molteplici sfumature in cui si dipana il problema del rischio ne fanno, attualmente, un oggetto di indagine ancora allo stato magmatico, sotto il profilo della sua piena operatività[29].

Tuttavia, il Reg. traccia una linea che consente, in sede interpretativa, di introdursi alla tipologia di trattamento che appare integrare pienamente gli estremi di una rilevante e persistente rischiosità nella nuova disciplina europea.

Si tratta della ormai famosa «*profilazione*», ovvero di «*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica*» (così l'art. 4, n. 4).

In linea generale, si può osservare che la profilazione è una nuova forma di conoscenza conseguente alla correlazione di dati contenuti in uno o più database volta alla definizione di un profilo di un individuo o di un gruppo. Attraverso la profilazione si conoscono aspetti, elementi, correlazioni del soggetto profilato che non sarebbe possibile trarre attraverso le modalità di analisi classiche. La profilazione pertanto non produce solo nuove o buone informazioni, ma genera un nuovo stadio di conoscenza, attraverso il quale è possibile osservare e prevedere analiticamente (cioè, profilare) comportamenti, attitudini, preferenze. La profilazione si rivela un mezzo funzionale alla assunzione di una decisione rilevante per l'individuo o per il gruppo profilato, proprio in quanto adeguato a valutare e *prevedere* analiticamente il comportamento presente e futuro del soggetto profilato[30].

---

[29] Ciò emerge anche dal contributo di A. Mantelero, *Il Consiglio d'Europa adotta le prime linee guida internazionali su Big Data e tutela dei dati personali*, in *questa Rivista*, 2017, e, più approfonditamente, ID., *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 144 ss..

[30] Su questo tema è molto utile approfondire attraverso la ricerca di F. Bosco-N.

Come si può intuire, se si volesse individuare un fenomeno che plasticamente rappresenta l'endiadi fra società digitale e *big data* ci si può agevolmente riferire al rilievo assunto dalla attività di profilazione: non a caso, pertanto, il Reg. vi fa costantemente riferimento[31].

Specifica attenzione è riservata alla attività di profilazione quando è volta a «*analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*» (così, ancora, la definizione di cui all'art. 4, n. 4), in modo particolare quando si inserisce in un «*processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*». In merito, l'art. 22 afferma che, in via generale, «*l'interessato ha 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*». Correlativamente, si specifica che l'interessato, nei casi in cui i suoi dati personali sono sottoposti a trattamento automatizzato (compresa la profilazione), è titolare di un di un diritto di opposizione (art. 21, c. 1[32]) e di un "*right of explanation*" in merito alla logica utilizzata, nonché

Creemers-V. Ferraris-D. Guagnin-B.J. Koops, *Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities*, in S. Gutwirth-R. Leenes-P. de Hert (edited by), *Reforming European Data Protection Law*, Law, Governance and Technology Series, vol. 20, Springer, 2015, pp. 3 ss..

[31] Cfr., in particolare, cons. n. 24 (in merito al trattamento effettuato da Titolare/Responsabile non stabilito nell'UE, quando è riferito al monitoraggio del comportamento di un interessato); art. 47, c. 2, lett. *e)* (in merito alle norme vincolanti d'impresa stabilite dalla competente autorità di controllo); cons. nn. 60, 63, 70 e artt. 13, c. 2, lett. *f)*, 14, c. 2, lett. *g)*, 15, c. 1, lett. *h)*, 21, c. 1 e 2 (in merito ai diritti dell'interessato rispetto alla profilazione); cons. n. 71 e art. 22 (in merito al trattamento automatizzato); cons. 91 e art. 35 (in merito alla valutazione di impatto); cons. 72 e art. 70, c. 1, lett. *f)* (in merito ai poteri di orientamento del Comitato europeo per la protezione dei dati); cons. 73 e art.23 (in merito alle limitazioni).

[32] Cfr. quanto puntualmente esposto da P. Pacileo, *Profilazione e diritto di opposizione*, in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, Milano, 2016, rispettivamente pp. 194 ss..

all'importanza e alle conseguenze previste di tale trattamento[33]. Ciò significa che in qualche modo si intende riconoscere un diritto di conoscenza (e, quindi, di controllo) dell'interessato sulle «*procedure matematiche o statistiche*» utilizzate dal Titolare del trattamento «*per la profilazione*», le quali devono essere «*appropriate*» (cons. 71).

In termini sintetici, il legislatore europeo individua la profilazione ed il connesso trattamento automatizzato dei dati come un rischio specifico (e generalizzato) del trattamento dei dati personali, in base al quale l'(ignaro) interessato può trovarsi di fronte ad una decisione rilevante per la sua sfera giuridica (cfr. cons. n. 58) che è frutto di un trattamento di dati personali (e non personali) da parte di un sistema automatizzato governato da uno o più algoritmi, al fine di servire gli interessi "economico-sociali" che li ha prodotti[34], per ora, attraverso l'incidente atti-

[33] Cfr. artt. 13, 14, 15 del Reg., indicate nella nota precedente, e B. Goodman-S. Flaxman, *European Union regulations on algorithmic decision-making and a 'right to explanation'* (31 agosto 2016), in http://arxiv.org/abs/1606.08813; Wachter-B. Mittelstadt-L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation* (28 dicembre 2016), in *International Data Privacy Law*, forthcoming and now available at SSRN: https://ssrn.com/abstract=2903469.

[34] In tal senso, pur non potendo sviluppare in questa sede il tema, non appare casuale che la qualificazione più puntuale delle dinamiche della profilazione sia contenuta in un considerando che si occupa del trattamento ad opera di un titolare/responsabile non stabilito nell'Unione europea. Nel cons. 24 si afferma che «È opportuno che anche il trattamento dei dati personali degli interessati che si trovano nell'Unione ad opera di un titolare del trattamento o di un responsabile del trattamento non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al *monitoraggio del comportamento* di detti interessati, nella misura in cui tale comportamento ha luogo all'interno dell'Unione. Per stabilire se un'attività di trattamento sia assimilabile al *controllo del comportamento dell'interessato*, è opportuno verificare se le persone fisiche sono *tracciate* su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella *profilazione della persona fisica*, in particolare per *adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali*» (nostri i corsivi). Per una introduzione al problema cfr. R. Bifulco, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giur. Cost.*, n. 1/2016, pp. 289 ss..

vità di altri esseri umani[35].

Per affrontare in modo sistematico questi rischi e, comunque, per minimizzare l'impatto sulla sfera personale dei trattamenti, ivi compresi quelli automatizzati e secondari, il Reg. individua un rimedio generale, nella «pseudonimizzazione», cioè nel «*trattamento dei dati personali 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, n. 5).

È interessante osservare che, secondo la definizione appena riportata, la pseudonimizzazione si qualifica come misura tecnica (un'operazione in forza della quale i dati personali non possono essere riferiti ad un interessato senza l'utilizzo di informazioni aggiuntive), ma anche come misura organizzativa: la misura tecnica è suscettibile di generare, ai sensi del Reg., una psuedonimizzazione dei dati personali solo se le informazioni necessarie per risalire agli originari dati personali sono conservate separatamente rispetto a questi e comunque se sono soggette ad ulteriori misure di garanzia dell'irriferibilità dei dati personali pseudonimi ad una persona fisica. Misure tecniche e modelli organizzativi improntati alla sicurezza (della infrastruttura del Titolare/Responsabile) devono muoversi in sincronia: quella che si delinea con la nozione di pseudonimizzazione appare una delle chiavi di volta della nuova disciplina europea, che sembra attuare l'osservazione secondo cui «l'unico modo efficace di affrontare il problema della sicurezza dell'informazione è quello che ne comporta una visione integrata: informatica, giuridica e organizzativa»[36].

Altro profilo notevole è che la pseudonimizzazione non sottrae i dati

[35] Cfr. Information commissioner's office, *Big data, artificial intelligence, machine learning and data protection*, Version 2.0 del 1.3.2017, in *https://ico.org.uk/*.
[36] Cfr. G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 1 ss..

trattati dalla sfera di applicazione del Reg., poiché essi non sono assimilabili ai dati anonimizzati e continuano ad essere considerati come «*informazioni su una persona fisica identificabile*» (cons. 26)[37]. Tuttavia si tratta di una misura fortemente incentivata[38], poiché considerata in grado di minimizzare il rischio per gli interessati coinvolti nel trattamento (cons. 28-29) e di aumentarne sensibilmente la sicurezza [art. 32, c. 1, lett. *a)*]. Inoltre, la pseudonimizzazione, insieme alla "cifratura", appare una garanzia di protezione ritenuta rilevante in sede di trattamenti c.d. secondari [art. 6, c. 4, lett. *e)*], laddove cioè il Titolare intenda svolgere un trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti[39].

L'interrelazione fra i concetti sin qui analizzati di rischio, profilazione e

[37] Cfr. È stato recentemente puntualizzato che «la tutela introdotta con la pseudonimizzazione è volta a garantire la confidenzialità del dato, non più immediatamente intelligibile, ma anche, come avviene nel caso dell'applicazione di tecniche crittografiche, a garantirne l'integrità contro manipolazioni anche accidentali. Nel caso dell'anonimizzazione la tutela è invece volta a impedire, a meno di dover ricorrere a mezzi irragionevolmente utilizzabili, la riferibilità del dato a una persona». Per questo, si afferma che i dati anonimizzati sono una misura di tutela della privacy, mentre i dati pseudonimi sono una misura di sicurezza, così G. D'Acquisto-M. Naldi, *Big data e privacy by design*, Giappichelli, 2017, p. 39; cfr. anche Gruppo di lavoro art. 29 per la protezione dei dati personali, *Parere 05/2014 sulle tecniche di anonimizzazione* (10 aprile 2014), in *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf*, spec. pp. 21 ss. Tuttavia, anche la distinzione fra dati pseudonimizzati e dati anonimi (e poi fra dati anonimi e dati personali) si rivela di carattere giuridico-stipulativo, o comunque una distinzione fondata su una valutazione del livello del rischio di disvelazione di dati personali, poiché «*anonymized data can always become personal data again depending upon the evolution of the data environment*», cfr. S. Stalla-Bourdillon-A. Knight, *Anonymous Data v. Personal Data – A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data* (6 Marzo 2017), in *Wisconsin International Law Journal*, 2017, disponibile presso *https://ssrn.com/abstract=2927945*.

[38] Cfr. oltre alle disposizioni citate di seguito nel testo, i cons. 75, 78, 85, 156 (quest'ultimo, insieme all'art. 89, c. 1, riferito al trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici) e gli artt. 25, c. 1; 40, c. 2, lett. *d)* (in riferimento alla elaborazione di codici di condotta).

[39] Cfr. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, p. 253.

pseudonimizzazione appare in grado di giustificare la innovazione introdotta dal Reg. nella basilare definizione di «*dato personale*» (art. 4, n. 1), la quale, come è stato rilevato, si estende ormai «all'insieme di informazioni relative ad una persona fisica, avendo riguardo per gli identificativi prodotti da dispositivi on line (indirizzo IP, cookies, ecc.) o di quei dati che, nonostante la pseudonimizzazione, possono essere oggetto di combinazione con ulteriori informazioni in modo da rendere possibile, direttamente o indirettamente, l'identificazione dell'interessato»[40].

Si tratta, per l'appunto, della qualificazione del concetto di «*dato personale*» al tempo del "rischio digitale".

4. La nozione di *privacy by design* (e di *privacy by default*) nel Reg. europeo

Il Reg. fa una scelta di campo netta in merito al soggetto cui addebitare l'intera responsabilità (intesa nel duplice senso di responsabilità giuridica e di connesso vincolo alla cura "amministrativa" e organizzativa) della gestione della composita filiera del trattamento dei dati personali. Il protagonista ed anche il *pivot* della nuova architettura giuridica europea è il Titolare del trattamento.

Ai sensi dell'art. 24, spetta al Titolare tenere conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento. Ciò significa, in primo luogo, essere in grado di determinare e delineare puntualmente i caratteri del trattamento, aspetto che può dimostrarsi di difficile realizzazione pratica nella società digitale[41].

---

[40] Cfr. G. Giannone Codiglione, *Risk-based approach e trattamento dei dati personali*, cit. p. 64.

[41] Come osserva A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 144 ss., spec. par. 5, nel contesto dei Big Data «le finalità "specifiche" del trattamento dati possono essere assai difficilmente descritte al momento della raccolta delle informazioni, stante la natura mutevole dell'utilizzo dei dati posto in essere dai titolari del trattamento che im-

Sulla base di questa iniziale valutazione, spetta al Titolare procedere a ponderare i rischi del trattamento sia sul versante della *probabilità* del verificarsi dei medesimi, sia sul versante della *gravità* della lesione dei diritti e delle libertà delle persone fisiche in caso di realizzazione delle ipotesi di rischio contemplate[42].

In ragione di questi due livelli di valutazione, il titolare del trattamento decide quali misure tecniche e organizzative sono adeguate per garantire che il trattamento sia effettuato conformemente alle disposizioni del Reg. e le mette in atto.

Si deve precisare che queste tre distinte attività non si esauriscono nella fase prodromica al trattamento, ma si estendono per tutta la sua durata: il Titolare deve monitorare i caratteri del trattamento (natura, ambito, contesto, finalità) ed i rischi connessi (probabilità e gravità) per l'intera durata del trattamento e su tale base, se necessario, è tenuto a procedere al riesame ed all'aggiornamento delle misure adottate.

Il Titolare, infine, deve essere in grado di dimostrare – in sostanza –

---

piegano soluzioni di Big Data analytics».

[42] Il cons. 75 elenca una molteplicità di ipotesi rischiose: «*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*».

lo svolgimento di tutte le attività appena descritte[43].

Sorge spontaneo il quesito sulle modalità concrete con cui il Titolare debba adempiere ad un così articolato schema normativo.

Su questo versante, si ritiene che il Reg. abbia adottato, allo stato, un indirizzo generico sul piano normativo, ma realistico sul versante applicativo.

In primo luogo, l'art. 24, c. 2, specifica che le misure tecniche ed organizzative «*includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento*», se ciò è proporzionato rispetto ai caratteri del trattamento. È forse opportuno segnalare che, in realtà, tutta l'attività di valutazione preventiva del trattamento, testé delineata, rappresenta già una politica di trattamento dei dati personali che prelude alla individuazione e messa in atto delle misure tecniche (e non viceversa). In questa prospettiva, quel che forse più rileva è il riferimento al principio di proporzionalità, col quale si vuole evidentemente sottolineare che non tutti i trattamenti presentano profili di rischiosità tali da necessitare di una particolare strategia (o politica) di prevenzione.

L'ultima parte dell'art. 24 indirizza il titolare verso una modalità di comprensione analitica di cosa effettivamente sia tenuto a fare, per rispettare i dettami normativi europei. Non si individuano direttamente condotte, ma si prelude ad un intenso lavorio di concreta specificazione di pratiche e modelli attuativi delle disposizioni regolamentari: «*l'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento*».

Si potrebbe sintetizzare che c'è molta *privacy by design* – o, se si preferisce, protezione dei dati fin dalla progettazione – nel principio di *accountabilty*[44] delineato dall'art. 24: una volta posta in capo al Titolare

[43] Si ricorda che il cons. 81, cui si rinvia, specifica una articolata serie di doveri e cautele del Titolare nel caso in cui designi un Responsabile del trattamento.

[44] Sul rilievo e sul significato del principio di *accountability* cfr. G. Finocchiaro,

– ovviamente, peraltro – la responsabilità del trattamento, si delinea una procedura costante di valutazione dei caratteri e dei rischi del trattamento, che va svolta "agganciando" l'organizzazione e la struttura aziendale alle condotte ritenute idonee sulla base degli appositi codici o delle buone pratiche connesse con i meccanismi di certificazione. All'esito di questa procedura il Titolare è credibilmente in grado di valutare, determinare e, se del caso, aggiornare in corso d'opera le misure tecniche e organizzative adeguate al trattamento.

In questa prospettiva, l'art. 25, c. 1, del Reg. si rivela utile perché arricchisce e specifica – sempre in modo sostanzialmente generale – i caratteri della progettazione del trattamento.

In primo luogo, si precisa che quanto richiesto al Titolare deve essere ragionevole e proporzionato, poiché nel determinare le «*adeguate*» misure tecniche e organizzative si tiene conto dello «*stato dell'arte*» e dei «*costi di attuazione*» delle medesime, in comparazione con i caratteri strutturali del trattamento e con la valutazione dei rischi.

In secondo luogo, si offrono precisazioni sulle misure tecniche e organizzative ritenute – di *default* – adeguate, come la pseudonimizzazione, e sui principi di architettura del modello europeo di protezione dei dati, quale il principio generale di minimizzazione dei dati [art. 5, c. 1, lett. *c)*], in forza del quale «*i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*».

I due aspetti appaiono legati ancora una volta alle dinamiche della società digitale: tanto più il trattamento appare suscettibile di comportare il rischio di una circolazione di dati personali in ambiente digitale, quanto più si fanno stringenti le esigenze strutturali di minimizzazione e di pseudonimizzazione dei dati trattati fin dalla progettazione del trattamento. Diversamente, sulla base dei principi di ragionevolezza e proporzionalità, potranno apparire prevalenti, allo stato dell'arte, misure diverse e meno costose a livello organizzativo ed economico. In en-

---

Introduzione al regolamento europeo sulla protezione dei dati, in *Le Nuove Leggi Civili Commentate*, 1/2017, pp. 1 ss., spec. par. 5.1.

trambi i casi è comunque necessaria una valutazione di questi aspetti in sede di progettazione del trattamento ed il Titolare deve essere in grado di giustificare le misure adottate (e quelle non adottate), sulla base di una «istruttoria» interna che si snoda dalla progettazione sino alla conclusione – fase, come noto, delicatissima – del trattamento.

In questa prospettiva, il successivo principio della protezione dei dati personali per impostazione predefinita (o *privacy by default*, cfr. art. 25, c. 2) appare principalmente una (opportuna) specificazione del principio generale di minimizzazione dei dati[45].

Il Titolare deve garantire, in primo luogo, che la infrastruttura tecnica di cui si avvale consenta di svolgere il trattamento utilizzando «*solo i dati personali necessari per ogni specifica finalità del trattamento*». Si instaura, in tal modo, una stretta correlazione fra «*ogni specifica finalità del trattamento*», così come emerge attraverso le informazioni che normalmente il Titolare rende all'interessato, acquisendone il consenso, e «*quantità dei dati personali raccolti*», «*portata del trattamento*», «*periodo di conservazione*» e, soprattutto, «*accessibilità*» dei dati personali trattati. Come più volte emerso in precedenza, quel che veramente si vuole evitare, attraverso i *default settings*, è che «*siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*» (art. 25, c. 2; l'u.c. dell'art. 25 specifica, ancora una volta, che un "elemento" che può essere utilizzato dal Titolare per dimostrare la conformità ai requisiti della *privacy by design* e *by default* è costituito da un meccanismo di certificazione riconosciuto ai sensi dell'art. 42).

Come anticipato, il Reg. affida interamente la protezione dei dati fin dalla progettazione e per impostazione predefinita al Titolare del trattamento. È superfluo osservarlo, ma ciò significa che – nella prospettiva del legislatore europeo – la *privacy by design* è riferita alla progettazione del trattamento.

---

[45] Cfr. G. D'Orazio, *Protezione dei dati by default e by design*, in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, Milano, 2016, pp. 79 ss..

Ci si deve domandare se ciò corrisponda pienamente alla natura ed alla logica del principio in parola.

La domanda sorge leggendo il cons. n. 78, ove – in riferimento alle misure tecniche e organizzative – l'attenzione non è rivolta esclusivamente al Titolare del trattamento, ma prende in specifica considerazione «*i produttori dei prodotti, dei servizi e delle applicazioni*», i quali «*in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni (...) dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati*».

Come è evidente, lo stesso Reg. riconosce che non v'è perfetta analogia fra la protezione dei dati fin dalla progettazione del trattamento, da parte del Titolare, e la protezione dei dati fin dalla progettazione da parte del produttore di prodotti, servizi e applicazioni. Più precisamente – seppure in modo implicito – è lo stesso Reg. che lascia giustamente intendere che, in assenza della *privacy by design* dei – si passi la sintesi – sistemi *hardware* e *software*, il Titolare potrebbe non essere in grado di adempiere agli obblighi di protezione «*fin dalla progettazione*» (del trattamento) su di lui gravanti.

In effetti, è stato rilevato che la protezione dei dati fin dalla progettazione è un principio che ha come primario termine di riferimento la progettazione di applicazioni, servizi, prodotti[46], poiché è funzionale

[46] Cfr. D. Klitou, *Privacy-Invading Tecnologies and Privacy by design. Safeguarding Privacy, Liberty and Security in the 21st Century*, *Informtaion Technology and Law Series*, vol. 25, Asser press – Springer, 2014: «PBD simply seeks to ensure that privacy is taken into consideration or built-in at the earliest stage of the device or system's lifecycle, i.e. when the device or system is being designed and manufactured, as opposed to "glued on" or "bolted on" after the device or system has already been developed. In essence, PBD is meant to serve not as a barrier to technology, but rather as a guided and prudent driver of technological development».

all'integrazione all'interno di un prodotto o sistema o applicazione di un modello adeguato di protezione dei dati personali, secondo i 7 famosi principi della *privacy by design*[47]. Il principio pertanto appare rivolgersi innanzitutto ai produttori ed agli ideatori di *information and communications technology* (ICT)[48] e potrebbe in tale prospettiva declinarsi, per chiarezza, in termini di *privacy by research*.

Nella prospettiva disciplinata dal Reg., invece, il principio è tutto declinato – almeno in prima battuta – sul Titolare, e solo indirettamente, per suo tramite, nei confronti di chi architetta e gestisce i sistemi informatici[49].

Il nodo fattuale è che il Titolare può trovarsi ad operare con prodotti e sistemi già predefiniti (*ex ante*) in assenza di un orientamento di *privacy by design*. A quel punto, in sostanza, la protezione dei dati fin dalla progettazione del trattamento finirebbe per risolversi con l'applicazione "ortopedica" (*ex post*) di *privacy enhancing technologies* (ovvero tecnologie di protezione della privacy) su prodotti e sistemi non pensati, all'origine, per integrare strutturalmente la protezione dei dati personali.

D'altra parte, almeno in prospettiva, tale esigenza del Titolare – di tutti i Titolari – non potrà che scaricarsi come istanza ai fornitori ed ai consulenti (a loro volta, in ipotesi, Titolari di trattamenti) e, quindi, progressivamente la *privacy by design* dovrebbe disseminarsi fra «*i*

[47] A. Cavoukian, *7 Foundational Principles of Privacy by Design*, Office of the Information & Privacy Commissioner of Ontario, 2010.

[48] Cfr. A. Principato, *Verso nuovi approcci alla tutela della* privacy*: privacy by design e privacy by default settings*, in *Contratto e impresa. Europa*, 1/2015, pp. 199 ss..

[49] Cfr. The European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Data Protection Reform Package*, 7 marzo 2012, ove si afferma che «182. The principles of data protection by design and by default are not presently addressed to advisers, developers and producers of hardware or software. However, they will be relevant for them from the start, as controllers are bound by them and accountable for compliance. In other words, obligations for controllers (and for processors, as mentioned above) are likely to create some incentives for the market of relevant goods and services».

produttori di applicazioni, servizi, prodotti» in riferimento al loro ambito di attività[50].

Una spinta analoga alla disseminazione delle pratiche della *privacy by design* dovrebbe arrivare dai meccanismi di certificazione di cui i Titolari possono dotarsi, i quali plausibilmente li orienteranno a richiedere l'adozione di sistemi e prodotti orientati alla protezione dei dati personali fin dalla progettazione e per impostazione predefinita.

Appare tuttavia evidente che il legislatore europeo non ha voluto spingersi al di là del mero incoraggiamento dei produttori a tener conto della protezione dei dati personali in sede di sviluppo e progetto dei prodotti (cons. 78), poiché ciò avrebbe comportato una marcata differenziazione normativa di questa categoria di soggetti che, allo stato, deve essere apparsa prematura, non proporzionata e forse un disincentivo all'innovazione ed agli investimenti in ICT[51].

5. Un cenno ad alcuni istituti e figure della *privacy by design*

È opportuno volgere un rapido sguardo ad alcuni istituti che completano il quadro sistematico del trattamento dei dati personali nel nuovo Reg.

Si è già accennato (*supra*, par. 3) alla valutazione di impatto sulla protezione dei dati (art. 35), riferita all'ipotesi di trattamento che possa presentare un rischio elevato.

Il Reg. individua – in modo abbastanza generico – tre tipologie di

[50] Nella prospettiva di un efficace coordinamento fra protezione dei dati personali e *big data*, attraverso l'implementazione della *privacy by design* cfr. A. Cavoukian, *Evolving FIPPs: Proactive Approaches to Privacy, Not Privacy Paternalism*, in S. Gutwirth-R. Leenes-P. de Hert (edited by), *Reforming European Data Protection Law*, *Law,Governance and Technology Series*, vol. 20, Springer, 2015, pp. 293 ss..

[51] Sull'impatto economico della regolazione europea in materia di protezione dei dati personali, cfr. H. Lee-Makiyama, *The Political Economy of Data: EU Privacy Regulation and the International Redistribution of Its Costs*, in L. Floridi (a cura di), *Protection of Information and the Right to Privacy - A New Equilibrium?*, *Law, Governance and Technology Series*, vol. 17, Springer, 2014, pp. 85 ss..

trattamento che richiedono una valutazione preventiva di impatto[52]. Il novero dei trattamenti necessariamente soggetti a valutazione si completa con un elenco redatto dalla autorità nazionale di controllo, la quale può anche predisporre un elenco di trattamenti per cui non è richiesta la valutazione (art. 35, c. 3, 4, 5).

Il Titolare è tenuto a consultare preventivamente l'autorità di controllo se dalla valutazione di impatto emerge l'esistenza di un rischio elevato in assenza di misure di attenuazione del rischio (art. 36, c. 1).

Quel che interessa sottolineare[53] è che l'inserimento dei principi della *privacy by design* e *by default* ha reso ragionevole superare la previsione della Dir. dell'obbligo generale, in riferimento ad alcuni trattamenti, di notifica alla autorità di controllo (cons. 89), rendendo – almeno astrattamente – residuali le ipotesi in cui è obbligatorio ricorrere alla comunicazione preventiva, la quale – in ogni caso – è successiva ad una "fase istruttoria" sviluppata autonomamente dal Titolare del trattamento (la valutazione di impatto)[54].

Il Reg. prevede che, nel momento in cui svolge la valutazione di impatto il Titolare del trattamento consulta il responsabile della protezione dei dati «*qualora ne sia designato uno*» [art. 35, c. 2 e correlativamente art. 39, c. 1, lett. *c)*].

Ciò ci consente di osservare una delle principali novità del Reg.: il

[52] L'art. 35, c. 3, dispone che: «*3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: 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; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*».

[53] Per un approfondimento della valutazione di impatto sulla protezione dei dati e della comunicazione preventiva si rinvia a G. Giannone Codiglione, *Risk-based approach e trattamento dei dati personali*, in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, cit. pp. 68 ss..

[54] Cfr. art. 18 (e 20), Dir. e artt. 17 e 37, D.Lgs. 196/03.

c.d. *data protection officer* (DPO).

In questa sede non interessa analizzare nello specifico le funzioni ed i caratteri del responsabile della protezione dei dati[55], mentre rileva invece inquadrarlo nella prospettiva di un trattamento che fin dalla progettazione incorpora l'esigenza della protezione dei dati personali. Forse non a caso, pertanto, si tratta di una figura che è già disciplinata in diversi Stati membri e che oggi il Reg. vuole introdurre in via generale a livello europeo[56].

La designazione di un DPO da parte del Titolare (art. 37, c. 1) è obbligatoria solo in casi specifici: in generale, i soggetti pubblici («*autorità pubblica*», «*organismo pubblico*») devono sistematicamente nominare un DPO, ad eccezione delle autorità giurisdizionali quando esercitano la funzione giurisdizionale; per tutti gli altri soggetti, la designazione è obbligatoria quando le «*attività principali del Titolare*», considerati i caratteri del trattamento, «*richiedono il monitoraggio regolare e sistematico degli interessati su larga scala*» oppure quando consistono nel trattamento, su larga scala, di categorie particolari di dati, di cui all'art. 9[57], o di dati relativi a condanne penali e reati di cui all'art. 10.

---

[55] Cfr. comunque cons. n. 77 (in merito agli orientamenti per la individuazione del rischio da parte del Titolare) e artt. 13, c. 1, lett. *b)*; 14, c. 1, lett. *b)* (in merito ai diritti dell'interessato di conoscere i dati di contatto del DPO); 30, c. 1, lett. *a)* e c. 2, lett. *a)* (in merito alla indicazione nei registri da parte del Titolare/Responsabile del nome e dati di contatto del DPO); 33, c. 3, lett. *b)* (in merito al contenuto del nome e dati di contatto del DPO nella notifica in caso di violazione dei dati personali); 35, c. 2; il capo IV , sez. 4, artt. 37-39 (dedicati proprio alla figura del DPO); gli artt. 47, c. 2, lett. *h)*; 57, c. 3. Per chiari dettagli sulla nomina, la posizione e i compiti del DPO, cfr. Gruppo di lavoro Articolo 29, *Linee-guida sul responsabile della protezione dei dati (RPD)*, (versione emendata del 5 aprile 2017), in *http://www.garanteprivacy.it/*.

[56] Cfr., per più specifiche indicazioni, G. M. Riccio, *Data protection officer e altre figure*, in Sica-D'Antonio-Riccio, *La nuova disciplina europea della privacy*, cit., pp. 33 ss., spec. PP. 49 ss..

[57] … quali i «*dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale», ovvero i «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*» (art. 9, c. 1).

Il DPO è designato in funzione delle qualità professionali ed è tenuto ad una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati; può essere un dipendente del Titolare o del Responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi; i dati di contatto del DPO devono essere comunicati al Garante dal Titolare/Responsabile del trattamento (art. 37, c. 5-7).

I compiti del DPO si dipanano essenzialmente su due fronti: nei confronti del Titolare/Responsabile del trattamento, poiché spetta al DPO fornire consulenza e sorvegliare la corretta applicazione della normativa in materia di protezione dei dati, contribuire ad informare e formare il personale, oltre che, se richiesto, fornire un parere e sorvegliare lo svolgimento della valutazione di impatto; nei confronti dell'Autorità di controllo, con cui il DPO è chiamato a collaborare e a fungere da «*punto di contatto*» (in particolare in caso di comunicazione preventiva). Ovviamente, non si può escludere che il DPO possa avere una funzione anche nei confronti degli interessati al trattamento, i quali hanno diritto di ottenerne i dati di contatto da parte del Titolare (cfr. artt. 13 e 14).

Il compito principale del DPO si rinviene incrociando la qualificazione professionale che lo caratterizza, con il ruolo di collegamento operativo fra Titolare/Responsabile del trattamento ed il livello istituzionale della protezione dei dati personali. In altri termini, il vero ruolo che il DPO assume è quello di importare, nell'organizzazione del Titolare del trattamento, l'esperienza maturata ed aggiornata in merito alle migliori pratiche attuative ed alle politiche della *privacy by design* e *by default*[58].

Se è giusto sottolineare che – nella normativa europea – il principio della *privacy by design* significa integrare la protezione dei dati fin dalla progettazione del trattamento, è bene osservare che questa strategia – per buona parte dei trattamenti su larga scala (e per i trattamenti dei

[58] Come osserva F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati. Il Regolamento europeo 2016/679*, Torino, 2017, p. 109, «il DPO opera a livello per così dire "micro". Esso, infatti, costituisce una figura di raccordo tra gli interessi e le finalità dei titolari dei trattamenti, la tutela proattiva degli interessati, l'attuazione coerente della nuova normativa e l'attività di consulenza e controllo delle Autorità».

soggetti pubblici) – trova compimento attraverso l'inserimento, nella organizzazione aziendale, di una figura specializzata, che ha esattamente questa vocazione professionale e questo compito.

In tal modo, il legislatore europeo tenta – per i trattamenti più rischiosi – di colmare l'inesorabile *gap* fra norme vigenti e relativa applicazione, inserendo – se si passa la sintesi – perizia e «prassi» applicativa all'interno del tessuto organizzativo del Titolare del trattamento. Con ogni evidenza, grazie all'introduzione sistematica del DPO nell'organizzazione dei soggetti pubblici Titolari del trattamento, il Reg. ha ritenuto di far leva sul vasto e ramificato settore pubblico europeo per raggiungere questo fine.

Va osservato, infine, che attraverso la figura professionale del DPO, si ottiene anche un legame – non solo, come talvolta si osserva, formale e burocratico – fra meccanismi di certificazione o processi di formazione nel settore della protezione dei dati personali e figure professionali interne o al servizio dell'organizzazione del Titolare del trattamento.

In conclusione, pertanto, è possibile osservare che l'istituto della valutazione di impatto induce il Titolare alla formalizzazione della visione e delle politiche del trattamento che presenti elevati rischi, mentre la figura del DPO è volta ad integrare nell'organizzazione del Titolare quell'insieme di competenze e di collegamenti necessari per strutturare quella visione e quelle politiche di protezione dei dati: entrambi gli aspetti vanno colti ed osservati come istituti che completano la strategia europea per una organica protezione dei dati, anticipata rispetto all'insieme dei trattamenti, sistematica e costante per tutta la loro durata.

6. Già e non ancora: il Reg. europeo fra rilievo globale ed esigenze di attuazione

Si vuole concludere il presente contributo con tre osservazioni finali.

Si sono passate in rassegna diverse disposizioni della pur vastissima e complessa trama del Reg. europeo (173 cons. e 99 artt.). Non si può

evitare di rilevare che il Reg. introduce molteplici novità, ma con una chiara coscienza della necessità di una attuazione progressiva dei nuovi principi e dei nuovi istituti. Ne sono un segno evidente non solo i diversi rinvii alla integrazione da parte degli Stati membri (cons. 8) contenuti nell'articolato, ma anche il ruolo riconosciuto alla c.d. *soft law* (codici di condotta, linee guida, elenchi, ecc.), agli atti delegati della Commissione europea (art. 92), ai meccanismi per garantire una applicazione uniforme delle regole introdotte dal Reg. e di quelle che grazie al Reg. prenderanno forma (ci si riferisce, in particolare, alle disposizioni contenute nel capo VII «*Cooperazione e coerenza*» del Reg., e in particolare al meccanismo di coerenza). Non meno rilevanti le innovazioni sul piano istituzionale e delle relazioni e competenze delle istituzioni nazionali ed europee.

È facile pertanto osservare che il Reg. ha mosso un passo importante verso la *privacy by design*, ma che questo passo è il primo di un cammino che si prospetta lungo e volto ad affrontare non solo un'epoca di cambiamenti, ma un cambiamento d'epoca[59], indotto – per quanto qui interessa – dalla evoluzione digitale.

Ciò consente di introdursi ad una seconda osservazione. La società digitale è un fenomeno globale in grado di comportare – di *default* – l'avvento di una sorveglianza di massa, che non ha riguardo a confini e limiti, che può arrivare a prevedere i comportamenti e prima ancora le aspirazioni ed i desideri e, prevedendoli, può influenzarne il divenire ed il libero progredire. Il tutto attraverso processi automatici, progressivamente gestiti (guidati?) da forme di intelligenza artificiale al servizio di intelligenze umane e dei loro interessi. Si tratta di un contesto c.d. virale, che si diffonde attraverso l'espandersi e la fruizione dei servizi e delle utilità digitali da parte delle persone e delle collettività.

[59] Cfr. quanto acutamente osservato da Papa Francesco, *Discorso del Santo Padre*, V Convegno nazionale della Chiesa italiana, Firenze, 10 novembre 2015, in *http://w2.vatican.va/content/francesco/it/speeches/2015/november/documents/papa-francesco_20151110_firenze-convegno-chiesa-italiana.html*.

In questo contesto, l'Unione europea non è una realtà neutrale nel panorama mondiale. Infatti, se in altre parti del mondo si concentra la produzione di *devices* e l'ideazione e produzione di ICT, non è difficile osservare che il vecchio continente (cioè l'Unione europea) è principalmente un grande consumatore di ICT e produttore di dati (anche personali).

L'esigenza di tutelare i propri «prodotti» è alla base della familiarità dell'ordinamento europeo con la protezione dei dati personali, sia in una visione di tutela della persona, sia nella prospettiva di tutela di un vero e proprio interesse pubblico europeo (cfr., *supra*, par. 2). Per questo, pur non essendo nata su suolo europeo[60], la *privacy by design* si è fatta strada proprio nell'Unione europea. Si tratta di un principio olistico, che attraverso la tutela della autodeterminazione informativa della persona si presta a garantire anche la protezione di gruppi, territori, Stati: esigenza particolarmente avvertita, nel continente europeo, al tempo dei *big data*, della profilazione e della sorveglianza di massa[61].

A ben vedere si tratta di una esigenza che inizia ad essere avvertita anche al di là dei confini dell'Unione europea, su cui vale la pena spendere l'ultima considerazione. Non ci si può nascondere che il Reg. e prima ancora le istituzioni europee hanno l'ambizione di fare della disciplina europea un punto di riferimento nel panorama internazionale. Sotto questo profilo, il fine del Reg. è di rappresentare uno «standard globale» di tutela[62], capace di diffondersi viralmente grazie alla ragionevolezza ed utilità dell'approccio di tutela in esso contenuto, così co-

[60] Cfr. A. Cavoukian, *Privacy by Design: Leadership, Methods, and Results*, in S. Gutwirth-R. Leenes-P. de Hert-Y. Poullet (a cura di), *European Data Protection: Coming of Age*, Springer, 2013, p. 175.

[61] Cfr. quanto segnalato da R. Bifulco, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giur. Cost.*, n. 1/2016, pp. 289 ss..

[62] Cfr. L. Califano, *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale scientifica, Napoli, 2016, p. 70, la quale puntualmente ricorda che con il motto "*one continent, one law*", che ha accompagnato nelle istituzioni europee l'iter formativo del Regolamento, la allora Vicepresidente della Commissione Viviane Reding dichiarava chiaramente di ambire a creare proprio un "global standard".

me si diffondono grazie alla loro semplicità ed utilità le tecnologie digitali[63]. *Vaste programme*, potrebbe chiosare qualcuno[64]. Tuttavia, il Reg. vigente ha la naturale vocazione a estendere la propria influenza al di là dei confini dell'Unione europea, se non altro nei confronti di chi ha interesse a trattare dati (e non solo dati) europei e di chi ritiene che la *privacy by design*, magari declinata in modo autonomo ed originale, non sia un'idea da scartare. Forse, infatti, è proprio la *privacy by design*, più che la sua versione europea, ad essere suscettibile di divenire uno standard globale. Già, e non ancora.

[63] Cfr. G. Buttarelli, *The EU GDPR as a clarion call for a new global digital gold standard*, in *International Data Privacy Law* 2/2016, pp. 77-78.

[64] Cfr. B.J. KROOPS, *The Trouble with European data protection law*, in *International Data Privacy Law*, 2014, Vol. 4, no. 4, p. 250: "The trouble with the law, as with Hitchcock's Harry, is that is dead. What the statues describe and how the courts interpret this has usually only a marginal effect on data-processing practices. Data protection law is a dead letter; current ideas what to do with the body are not leading anywhere except that they offer entertainment to spectators. With the current reform, the letter of data protection law will remain stone-dead".