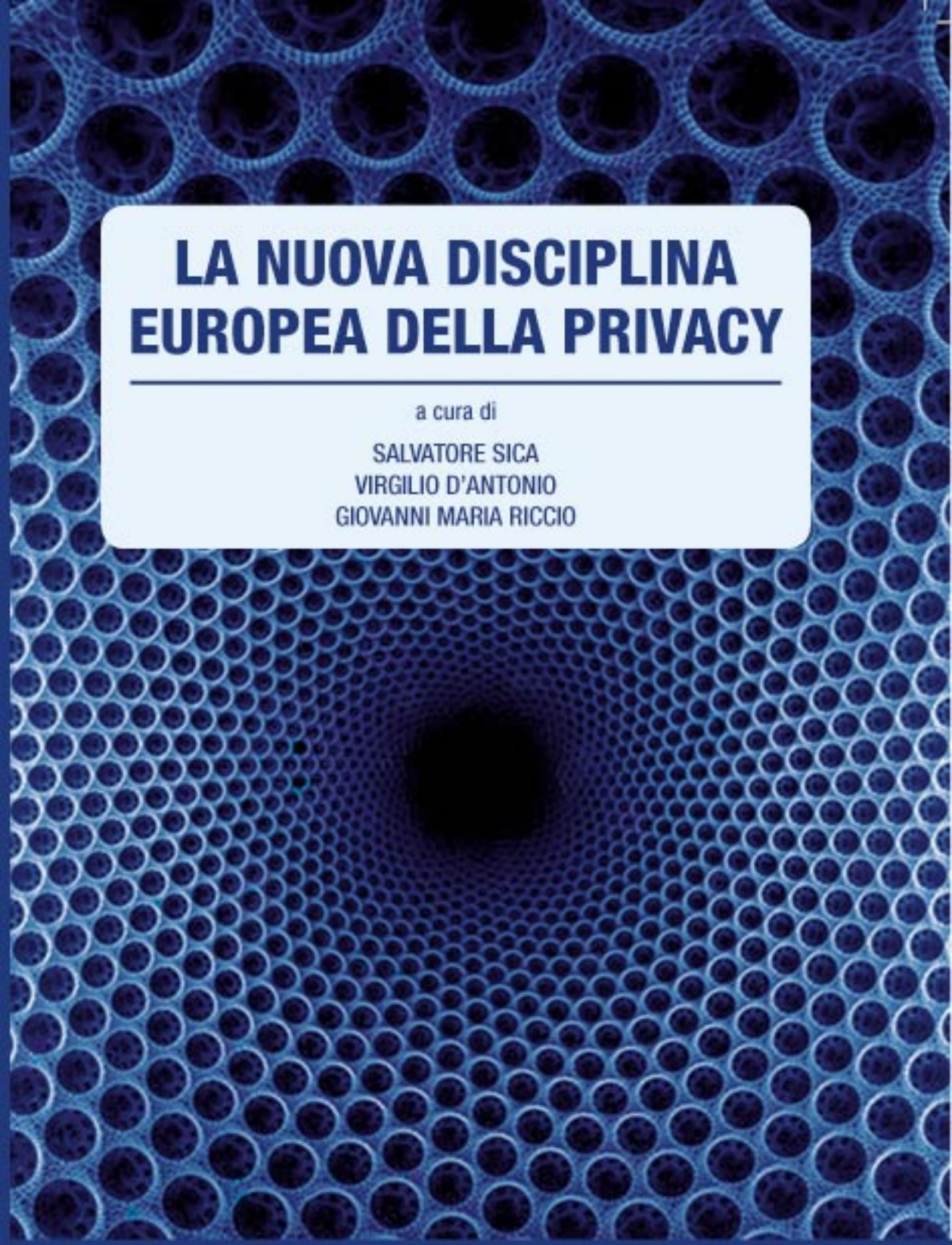
LA NUOVA DISCIPLINA EUROPEA DELLA PRIVACY

a cura di

SALVATORE SICA
VIRGILIO D'ANTONIO
GIOVANNI MARIA RICCIO



Wolters Kluwer
CEDAM

Con il Regolamento Generale del 27 aprile 2016, l'Unione europea ha riformato sostanzialmente la disciplina in materia di tutela dei dati personali. Una "rivoluzione" che impone alle imprese di adeguarsi alle prescrizioni normative e agli interpreti di confrontarsi con il mutato assetto legislativo. Il volume, ripercorrendo la genesi e lo sviluppo della privacy europea, a partire dalla direttiva 46/95/CE, passa in rassegna i principali aspetti del Regolamento (diritto all'oblio, privacy officer, privacy by design, one stop shop), offrendo una panoramica articolata delle novità introdotte e del dibattito dottrinario in corso.

Salvatore Sica, professore ordinario di Istituzioni di Diritto privato presso l'Università di Salerno. Vicepresidente della Scuola Superiore dell'Avvocatura, è componente del comitato scientifico de "Il diritto dell'informazione e dell'informatica" e direttore del Laboratorio In.Di.Co. (Informazione Diritto Comunicazione). È autore di monografie, saggi e commenti in materia di protezione dei dati personali, pubblicati in Italia e all'estero.

Virgilio D'Antonio, professore ordinario di Diritto comparato dell'informazione e della comunicazione e Presidente del Consiglio Didattico di Scienze della Comunicazione dell'Università di Salerno. È autore di monografie, saggi e commenti in materia di protezione dei dati personali, pubblicati in Italia e all'estero.

Giovanni Maria Riccio, professore associato di Diritto comparato ed europeo della comunicazione presso l'Università di Salerno. È autore di monografie, saggi e commenti in materia di protezione dei dati personali, pubblicati in Italia e all'estero.

5 000002 024986

9 788813 358327

€ 37,00 IVA INCLUSA

CEDAM

LA NUOVA DISCIPLINA EUROPEA DELLA PRIVACY

a cura di Salvatore Sica - Virgilio D'Antonio - Giovanni Maria Riccio

S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della* privacy.

LA NUOVA DISCIPLINA EUROPEA DELLA *PRIVACY*

a cura di
SALVATORE SICA, VIRGILIO D'ANTONIO
E GIOVANNI MARIA RICCIO

Wolters Kluwer CEDAM

Stampato da GECA s.r.l. - Via Monferrato, 54 - 20098 San Giuliano Milanese (MI)

SOMMARIO

CAPITOLO QUARTO

RISK-BASED APPROACH
E TRATTAMENTO DEI DATI PERSONALI
di *Giorgio Giannone Codiglione*

CAPITOLO QUINTO

PROTEZIONE DEI DATI
BY DEFAULT E *BY DESIGN*
di *Roberto D'Orazio*

CAPITOLO SESTO

DISCIPLINA DEL CONSENSO
E TUTELA DEL MINORE
di *Giuseppe Spoto*

CAPITOLO SETTIMO

INTERNET OF THINGS
E NUOVO REGOLAMENTO PRIVACY
di *Giorgio Giannone Codiglione*

CAPITOLO OTTAVO

TRASPARENZA E ACCESSO AI DATI PERSONALI
di *Giuseppe Di Genio*

CAPITOLO NONO

PROFILAZIONE E DIRITTO DI OPPOSIZIONE
di *Piervincenzo Pacileo*

CAPITOLO DECIMO

OBLIO E CANCELLAZIONE DEI DATI NEL DIRITTO EUROPEO

di *Virgilio D'Antonio*

CAPITOLO UNDICESIMO

IL DIRITTO ALLA PORTABILITÀ

di *Piervincenzo Pacileo*

CAPITOLO DODICESIMO

DATA BREACH E SICUREZZA INFORMATICA

di *Salvatore Vigliar*

CAPITOLO TREDICESIMO

TRASFERIMENTO VERSO PAESI TERZI
di *Domenico Pittella*

CAPITOLO QUATTORDICESIMO

IL TRATTAMENTO DEI DATI NEL TERRITORIO DELL'UNIONE E IL MECCANISMO "*ONE STOP SHOP*"
di *Davide Mula*

CAPITOLO QUINDICESIMO

RESPONSABILITÀ E SANZIONI
di *Annamaria Giulia Parisi*

CAPITOLO SEDICESIMO

LA PROTEZIONE DEI DATI TRATTATI A FINI DI PREVENZIONE E ACCERTAMENTO DEI REATI

di *Paolo Troisi*

CAPITOLO XV

RESPONSABILITÀ E SANZIONI

Annamaria Giulia Parisi

SOMMARIO: 1. Il Regolamento Generale sulla tutela dei dati personali. – 2. Il principio di responsabilità nel sistema europeo di protezione dei dati: dalla Convenzione 108/1981 al Regolamento. – 3. Un mutamento di prospettiva. Le responsabilità del *data controller* e del *processor*. – 4. Il *Data Protection Officer*. – 5. L'ambito delle sanzioni.

1. Il Regolamento Generale sulla tutela dei dati personali

Nella società tecnologica globalizzata, i dati personali sono stati già definiti *global commons*, patrimonio accessibile quasi a tutti, ma fragile quanto prezioso, perché attinente all'essenza dell'individuo.

Il diritto alla protezione dei dati personali sorge come specificazione particolare del generale diritto alla *privacy*, oggi più che mai essenziale per la salvaguardia della libertà e della dignità della persona umana.

Nel mondo dematerializzato della connessione universale, a fronte di emergenze comuni da affrontare e risolvere, in qualche modo, necessariamente, il diritto vacilla, e s'impone con evidenza crescente il problema della sua globalizzazione.

Cambia la dimensione della stessa nozione di tutela dei dati, elementi, questi, preziosi e irrinunciabili delle strategie di protezione e di lotta al terrore: nella società pervasa dalla nuova 'sorveglianza', in cui ciò che prima era sottoposto a sistemi intrusivi di video e ascolto ora è investito dall'interagire continuo e automatizzato di 'sensori di calore, di luce, di suono, di movimento', le nuove tecnologie elettroniche, i droni, le analisi

biometriche e genetiche giungono a cogliere ciò che prima era inosservabile o inaccessibile[1].

In tale contesto, la disciplina della *privacy* si configura come *law in action*, che tutela un diritto che muta al mutare delle innovazioni tecnologiche e delle esigenze sociali. Flessibilità che si esplica sia in senso diacronico che sincronico, talché le norme inerenti possano adeguarsi ai mutamenti sociali che si susseguono, all'evoluzione tecnologica, alle diverse situazioni coesistenti in un momento determinato o in momenti diversi: in tale ottica nascono le Autorità Garanti per la protezione dei dati personali.

Nella corsa verso l'inarrestabile sviluppo dell'economia di mercato, nel moltiplicarsi delle iniziative di merchandising e marketing personalizzato che, grazie alla profilazione degli utenti dell'*e-commerce* riduce al minimo i rischi ed ottimizza i guadagni inducendo nei *customers* bisogni forgiati su misura, prima ancora che i destinatari ne siano consapevoli, i droni che popolano il *web* invadono la nuova dimensione dell'*infosfera*, del patrimonio di conoscenze e di connotazioni personali che caratterizzano l'individuo, ridotto ormai a persona *…disincarnata, tutta risolta nelle informazioni che la riguardano, unica e "vera" proiezione nel mondo dell'essere di ciascuno.*

E dunque il diritto alla riservatezza "decade" a diritto alla protezione dei dati, per chi, a cominciare da Zuckerberg nel 2010, ha sancito ormai 'la morte della privacy'.

Quasi in accordo con tale ipotesi, la disciplina europea innovata nel nuovo Regolamento[2] discorre di protezione dei dati personali, aggiungendo peraltro specificazione e concretezza alla nozione di *privacy* così tuttavia necessariamente limitata, all'insegna di un senso di praticità tutto latino o, se vogliamo,

---

[1] U. PAGALLO, *La tutela della* privacy *negli Stati Uniti d'America e in Europa*, Milano, 2008, p. 207.

[2] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), in G.U.U.E., 4 maggio 2016, n. L 119. D'ora in avanti in questo contributo sarà denominato semplicemente Regolamento.

riscontrabile anche nell'essenzialità dei dettagli del diritto strutturato tra *writs*, *remedies* e *forms of actions*[3].

Tributaria della precisione voluta dalla normativa europea *de qua*, la nozione di *protezione dei dati personali* si specifica ulteriormente nelle sue coordinate di esattezza ed affidabilità dei dati trattati e/o immessi in rete: rileva anche qui nitidamente la preoccupazione del legislatore europeo di salvaguardare il fine prioritario e l'esistenza del 'mercato unico', garantendo a c*ustomers* e *consumers*, e in genere a tutti gli interessati la tutela dei dati personali. Un'ipotesi di *failure* in tal senso sarebbe esiziale, perché timore e sfiducia allontanerebbero masse di utenti dall'utilizzo di *e-contract* e del commercio elettronico e, sostanzialmente, renderebbe meramente utopistico il concretarsi di quel *Mercato Unico Digitale* che palesemente appare l'obiettivo della nuova normativa. In un'Europa da tempo oppressa dalla crisi il *Mercato Unico Digitale* - secondo le stime della Commissione - potrebbe creare quasi quattro milioni di nuovi posti di lavoro e produrre un volume di affari annuo pari ad almeno 415 miliardi di euro.

Il Regolamento del 27 aprile 2016, oltre ad apportare novità di rilievo - come le norme in tema di diritto all'oblio[4] e di di-

---

[3] Per una singolare analogia operativa tra il diritto pretorio romano e le *forms of action*, si consenta il rinvio, anche, a A.G. PARISI, *Colpa e dolo nella responsabilità. Saggi di diritto comparato*, Torino, 2012, p. 199.

[4] Peraltro il 'diritto all'oblio' – che trova riferimento letterale nell'inciso della rubrica dell'art. 17 – era stato già sancito, evidenziando la propria funzione nomopoietica, dalla Corte di Giustizia dell'Unione Europea, nella nota decisione *Google Spain SL c. Agencia Española de Protección de Datos (AEPD)* (Corte di giustizia, Grande sezione, Sent. 13 giugno 2014, in C-131/12).

Per la ricostruzione della vicenda che ha condotto al noto *revirement* della Corte di Giustizia, cfr. A.G. PARISI, *E-contract e privacy*, Torino, 2015, pp. 213 ss., ove è agevole altresì ripercorrere il cammino della giurisprudenza costituzionale e di Cassazione in tema di diritto alla cancellazione dei propri dati e di 'diritto all'oblio' (A.G. PARISI, *ib*., pp. 203 ss.).

Regolamento (UE) 2016/679, Capo III, Sez. 3, art.17 - Diritto alla cancellazione ("diritto all'oblio"): 1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'ar-

ritto alla portabilità dei dati; come le notificazioni delle violazioni alle Autorità nazionali ed agli stessi utenti nei casi più gravi di *data breaches*[5]; le modalità di accesso ai propri dati personali più agevoli per gli interessati; il meccanismo dell'*one-stop-shop*, in virtù del quale le aziende potranno confrontarsi con un'unica autorità di vigilanza[6]; il concetto di *privacy by design,* ossia della *tutela del dato fin dalla progettazione* e di *privacy by default,* intesa quale *tutela della vita privata per impostazione predefinita* - prevede, altresì, soprattutto per le piccole e medie imprese, semplificazioni burocratiche e un connesso sgravio di costi stimato in oltre 130 milioni di euro per anno.

---

ticolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1… 3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

[5] Rileva come solo il d.lgs. n. 196 del 2003, per primo, era passato da un sistema di notificazione generalizzato ad un sistema di notificazione specifico - *i. e*. da eseguirsi solo per trattamenti che presentano rischi specifici.

[6] *The "one-stop-shop" principle, together with the consistency mechanism, is one of the central pillars of the Commission proposal. According to this principle, when the processing of personal data takes place in more than one member state, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions. The proposal states that the competent authority providing such one-stop-shop should be the supervisory authority of the member state in which the controller or processor has its main establishment…This is an important factor to enhance the costefficiency of the data protection rules for international business, thus contributing to the growth of the digital economy* (Council of European, Luxembourg, 7 October 2013, 14525/13).

Dunque appare prospettarsi un mutamento epocale in ambito economico-giuridico, perché dalla dimensione propria del precedente meccanismo fondato sull'armonizzazione e sulle norme nazionali di attuazione si passa ad un Regolamento di immediata applicazione in tutti gli Stati membri che, soprattutto, introduce regole certe atte a disciplinare non soltanto fenomeni che nella direttiva 95/46/CE[7] non erano nemmeno contemplati, ma anche quelli connessi a future problematiche, inerenti al Mercato Unico Digitale, che attualmente non ancora appaiono all'orizzonte.

2. Il principio di responsabilità nel sistema europeo di protezione dei dati: dalla Convenzione 108/1981 al Regolamento

Il principio di responsabilità è integrato nel sistema comunitario di protezione dei dati già dalla Convenzione 108/1981[8], il primo documento specificamente dedicato, in Europa, al trattamento dei dati personali. La Convenzione 108/1981, promossa dal Consiglio d'Europa ed avente il carattere e l'obbligatorietà di un accordo internazionale, conserva ancor oggi una valenza fondamentale, anche perché tra le convenzioni del Consiglio d'Europa è aperta a qualsiasi Stato, anche al di fuori dei Paesi membri, su invito del Comitato dei ministri.

Rileva, nel Preambolo, il principio secondo cui la libera circolazione delle informazioni tra i popoli non può prescindere dalla tutela dei diritti e delle libertà fondamentali di ciascuno. La sua finalità è quella di garantire la protezione degli individui senza considerazione di frontiere, a prescindere dalla loro cittadinanza o residenza.

La suddetta Convenzione non integra espressamente il principio della responsabilità di chi è coinvolto nel trattamento dei dati personali, ma discorre, rispettivamente, all'art. 5 di

---

[7] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, p. 31).

[8] La *Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale*, adottata a Strasburgo il 28 gennaio 1981, è stata ratificata in Italia dalla l. 21 febbraio 1989, n. 98.

'qualità dei dati'; all'art. 7[9] di 'sicurezza dei dati' ed all'art. 8 di 'diritti dell'interessato'.

Come si può osservare, proprio nell'art. 5 della Convenzione 108 è racchiuso il *common core* della futura disciplina comunitaria in materia di dati personali:

> Art. 5 - Qualità dei dati. I dati a carattere personale oggetto di un'elaborazione automatizzata sono: a) ottenuti e elaborati in modo lecito e corretto; b) registrati per scopi determinati e legittimi ed impiegati in una maniera non incompatibile con detti fini; c) adeguati, pertinenti e non eccessivi riguardo ai fini per i quali vengono registrati; d) esatti e, se necessario, aggiornati; e) conservati in una forma che consenta l'identificazione delle persone interessate per una durata non superiore a quella necessaria ai fini per i quali sono registrati.

Invece all'art. 8, lett. c), è già sancito *in nuce* il 'diritto all'oblio':

> Ogni persona deve poter: …c) ottenere, se del caso, la rettifica di tali dati o la loro cancellazione qualora questi siano stati elaborati in violazione delle disposizioni di diritto interno di esecuzione dei principi fondamentali di cui agli artt. 5 o 6 della presente Convenzione…

È dunque assente nella Convenzione 108 la specifica attribuzione della responsabilità a figure o a soggetti determinati, seppure è agevolmente deducibile che essi non possano non identificarsi con i soggetti coinvolti nel trattamento dei dati.

In seguito la direttiva n. 95/46/CE (la *direttiva madre* in tema di protezione dei dati) che ha delineato i principi fondamentali in materia di *tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, segna un notevole progresso nell'individuazione e nell'attribuzione della responsabilità, soprattutto là dove, all'art. 6, § 1, detta i criteri che garantiscono la qualità dei dati trattati, e all'art. 6, § 2 stabilisce che il 'responsabile del tratta-

[9] Art. 7 - Sicurezza dei dati. Adeguate misure di sicurezza vengono adottate per la protezione di dati di carattere personale registrati nei casellari automatizzati contro la distruzione accidentale o non autorizzata, ovvero la perdita accidentale così come contro l'accesso ai dati, la modifica o la diffusione non autorizzate.

mento' è tenuto a garantire l'osservanza delle disposizioni di cui al § 1[10].

La direttiva n. 2002/58/CE[11] relativa al *trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche*, per il cui tramite il legislatore comunitario ha inteso armonizzare le disposizioni degli Stati membri in materia, pone l'accento sull'esigenza di garantire la legittimità del trattamento, la sicurezza delle comunicazioni e la tutela degli utenti.

La direttiva n. 2006/24/CE[12], entrata in vigore il 3 maggio 2006, ha modificato la direttiva n. 2002/58/CE introducendo nuovi obblighi di conservazione dei dati di traffico concernenti lo specifico ambito delle comunicazioni elettroniche: la direttiva è stata invalidata, però, dalla Corte di Giustizia (Grande Sezione) dell'8 aprile 2014, *per violazione del principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza*.

La direttiva n. 2009/136[13], che ha modificato la direttiva n. 2002/58/CE, introducendo di fatto il principio della particolare

---

[10] La direttiva del '95 disciplina il trattamento dei dati prevedendo che il relativo procedimento avvenga nel rispetto di alcuni principi e diritti dell'interessato: dal diritto di accesso al diritto di opposizione, dal diritto alla sicurezza a quello alla giustiziabilità. A questo proposito è previsto un doppio livello di tutela, giurisdizionale e amministrativo: il primo si realizza attraverso ricorsi ordinari presso le magistrature comuni - l'autorità giudiziaria ordinaria -; il secondo attraverso l'attività di un apposito organo di garanzia, l'Autorità di controllo, incaricata di *controllare* l'applicazione della normativa in materia, disponendo a tal fine di poteri investigativi, consultivi, e di promozione di azioni giudiziarie, in caso di violazione delle relative disposizioni.

[11] Direttiva del Parlamento europeo e del Consiglio n. 2002/58/CE, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), entrata in vigore il 31 luglio 2002, in G.U.C.E. 31 luglio 2002, n. L 201.

[12] Direttiva del Parlamento europeo e del Consiglio n. 2006/24/CE riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, entrata in vigore il 3 maggio 2006 (G.U.U.E. 13 aprile 2006, n. L 105).

[13] Direttiva CEE 25 novembre 2009, n. 2009/136/CE - Direttiva del Parlamento Europeo e del Consiglio recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla coopera-

responsabilità emergente in seguito al verificarsi di gravi perdite di dati personali, ha rafforzato obblighi e responsabilità dei prestatori di servizi di comunicazione elettronica, inserendo nell'art. 4 della direttiva integrata l'obbligo esplicito per i fornitori di reti e di servizi di adottare adeguate politiche di sicurezza riguardo al trattamento dei dati personali e, nel contempo, il dovere di comunicare "senza indebiti ritardi" le eventuali violazioni di dati alle Autorità nazionali di controllo ed anche all'interessato, qualora le violazioni siano tali da pregiudicare i dati personali e la sua *privacy*[14].

Rileva come i provvedimenti normativi successivi alla direttiva 95/46 sono risultati sempre aggiuntivi e mai sostitutivi rispetto alle norme della direttiva stessa, né hanno messo in di-

---

zione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, (G.U.U.E. 18 dicembre 2009, n. L 337), entrata in vigore il 19 dicembre 2009, recepita con d.lgs. 28 maggio 2012, n. 69 e con d.lgs. 28 maggio 2012, n. 70.

[14] Direttiva 2002/58/CE, art. 4. Sicurezza del trattamento. 1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve prendere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della rete. Tenuto conto delle attuali conoscenze in materia e dei loro costi di realizzazione, dette misure assicurano un livello di sicurezza adeguato al rischio esistente. 1 bis: Fatta salva la direttiva 95/46/CE, le misure di cui al paragrafo 1 quanto meno: - garantiscono che i dati personali siano accessibili soltanto al personale autorizzato per fini legalmente autorizzati; - tutelano i dati personali archiviati o trasmessi dalla distruzione accidentale o illecita, da perdita o alterazione accidentale e da archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti, e garantiscono l'attuazione di una politica di sicurezza in ordine al trattamento dei dati personali. Le autorità nazionali competenti sono legittimate a verificare le misure adottate dai fornitori di servizi di comunicazione elettronica accessibili al pubblico e a emanare raccomandazioni sulle migliori prassi in materia di sicurezza che tali misure dovrebbero conseguire. 2. Nel caso in cui esista un particolare rischio di violazione della sicurezza della rete, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di informarne gli abbonati indicando, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, tutti i possibili rimedi, compresi i relativi costi presumibili. 3. In caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza indebiti ritardi detta violazione all'autorità nazionale competente. Quando la violazione di dati personali rischia di pregiudicare i dati personali o la vita privata di un abbonato o di altra persona, il fornitore comunica l'avvenuta violazione anche all'abbonato o ad altra persona interessata.

scussione l'esistenza delle Autorità di controllo o del Gruppo di Lavoro Articolo 29.

Il ruolo fondamentale svolto dal principio di responsabilità nel diritto europeo si concretizza, con riguardo al ruolo e alla responsabilità del titolare e del responsabile del trattamento, nel Parere 1/2010 (WP n. 169) espresso dal Gruppo di Lavoro Articolo 29 e nel successivo Parere 3/2010 (WP n. 173) esplicitamente dedicato al 'Principio di responsabilità'.

Il Regolamento amplia la disciplina stabilita dalle direttive 2002/58/CE e 2009/136, estendendo il principio di responsabilità da *data breach* a tutti i tipi di trattamento.

Nel Regolamento la notificazione è analogamente connessa, come si vedrà, al tipo di rischio, e in particolare al *risk for the rights and freedoms of individuals.*

La notifica, invece, non è d'obbligo se non emerge un rischio per i diritti e le libertà fondamentali delle persone.

3. Un mutamento di prospettiva. Le responsabilità del *data-controller* e del *processor*

La citata direttiva 95/46/CE, che sarà di fatto abrogata con l'entrata in vigore del Regolamento, è oggettivamente strutturata in modo da far risultare *common core* del provvedimento e delle tutele predisposte l'interessato e i suoi diritti: la disciplina innovata segue una prospettiva opposta, incentrata su oggettive esigenze di correttezza e conformità alle norme, avvertite dalle imprese e dal contesto.

Il principio di responsabilità, infatti, segna in modo marcato la differenza di approccio e di prospettiva tra la disciplina attualmente vigente e quella delineata dal Regolamento[15], e dato che la responsabilità è strettamente connessa sotto ogni profilo

[15] Ciò rileva con evidenza maggiore se si fa conto che la direttiva 95/46/CE dedica solo gli artt. 16 e 17 alla *security*, mentre ben quattro sezioni del Capo IV, nel definire gli obblighi e le responsabilità del *controller* e del *processor*, salvaguardano l'elevata sicurezza dei dati. Non è richiesta la notifica di una violazione dei dati personali a un abbonato o a una persona interessata se il fornitore ha dimostrato in modo convincente all'autorità competente di aver utilizzato le opportune misure tecnologiche di protezione e che tali misure erano state applicate ai dati interessati dalla violazione della sicurezza. Tali misure di protezione rendono di fatto i dati incomprensibili a chiunque non sia autorizzato ad accedervi.

al trattamento dei dati, essa è incardinata su chi pone in essere tale trattamento: talché, quella che viene da molti considerata la parte più ampia ed innovativa, costituita dalle cinque sezioni del Capo IV, concerne proprio le figure e i ruoli del *controller* e del *processor,* la cui centralità è speculare al rilievo del trattamento dei dati.

Il principio di responsabilità è ovviamente connesso sia al rispetto delle regole giuridiche e tecniche, cui vanno improntati le modalità e gli scopi del trattamento, sia al rispetto dei diritti del *data subject*.

Il quadro delle responsabilità che incombono sul titolare del trattamento ex art. 24 si specifica nella responsabilità connessa alla conformità o meno del trattamento alle norme; nella responsabilità derivante dall'obbligo di adozione delle misure idonee a garantire la protezione e la sicurezza dei dati; nell'obbligo di dimostrare in qualunque momento tale conformità agli interessati, alle Autorità di controllo e a soggetti pubblici o privati legittimati a farne richiesta.

Dunque, mentre il responsabile del trattamento di cui all'art. 6 della direttiva 95/46 - figura che ora corrisponde al titolare del trattamento! - è tenuto al rispetto delle norme concernenti la liceità del *data processing*, ex art. 24 del Regolamento il *controller* deve, invece, porre in atto tutte le misure di natura tecnica e/o organizzativa atte a dimostrare che il trattamento dei dati sia conforme alle norme.

Il ruolo del *controller* pertanto è caratterizzato da un duplice obiettivo: il rispetto delle regole e l'obbligo di comprovarne la *compliance*.

Nello specifico, ex art. 24 il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che esso è effettuato conformemente al Regolamento, e ciò tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento stesso, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone. Tali misure devono essere riesaminate e aggiornate, qualora necessario, dal *controller* che deve essere in grado di dimostrare il rispetto dei suoi obblighi. Il che può avvenire anche tramite l'adesione ai codici di condotta di cui all'articolo 40 o al meccanismo di certificazione di cui all'articolo 42 che, in particolare, al § 1 specifica come l'istituzione di procedimenti di certificazione possa *dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e*

dai responsabili del trattamento. Tuttavia, il medesimo art. 42 al § 4 precisa testualmente che: *la certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti a norma degli articoli 55 o 56*.

Va osservato come il Regolamento renda più severe e cogenti le norme che disegnano il ruolo e la responsabilità del *controller*, che si connota agli occhi del giurista italiano di pressoché tutte le caratteristiche della responsabilità che incombe su chi svolge un'attività pericolosa. Non a caso, mentre la direttiva 95/46/CE all'art. 23 si limita a stabilire che il soggetto che subisce un danno a causa del trattamento illecito dei suoi dati personali o a causa di un atto incompatibile con le disposizioni nazionali di attuazione della direttiva stessa ha diritto al risarcimento del danno da parte del titolare del trattamento dei dati personali, il legislatore italiano recepiva il medesimo provvedimento in modo singolare, andando oltre la direttiva stessa: infatti stabiliva l'applicabilità dell'articolo 2050 c.c. al titolare del trattamento dei dati, che veniva, così, equiparato al soggetto che esercita un'attività pericolosa[16].

Il legislatore italiano ha altresì stabilito che colui che è stato danneggiato dal trattamento illecito dei suoi dati personali, in base all'articolo 2059 c.c. può richiedere il risarcimento dei danni morali da tale trattamento derivati.

Per la dottrina italiana il riferimento del legislatore alle attività pericolose è corretto e coerente, dato che - come è anche previsto dalla vigente norma comunitaria - il titolare del trattamento può essere esonerato da tale risarcimento se prova che il danno non è a lui imputabile, così come, in base all'art. 82, § 3 del Regolamento, il titolare del trattamento illecito può provare la propria non imputabilità, dimostrando di aver adottato tutte le misure idonee per evitare il danno.

---

[16] La direttiva n. 95/46/CE è stata recepita nel nostro ordinamento con la l. 5 febbraio 1999, n. 25 - *Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee - legge comunitaria 1998.* (in G.U., 12 febbraio 1999, n. 25, S.O.).

Dunque il Legislatore della rinnovata disciplina ha in certo modo, a sua volta, *recepito* la severità della norma italiana ritenendola, nella specie, più adeguata.

Nel Regolamento è dunque più ampio l'ambito della responsabilità del titolare del trattamento, come è più ampio lo spettro delle Autorità cui potenzialmente egli è obbligato a dimostrare di aver fatto tutto ciò cui era tenuto, nello specifico.

Inoltre, mentre nella direttiva 95/46 ancora vigente non compaiono particolari disposizioni nel caso in cui più titolari o più soggetti concorrano a stabilire le modalità del trattamento, tranne che per l'inciso dell'art. 2, lett. d), in cui nel definire la nozione di titolare del trattamento - lì definito 'responsabile' - lo identifica nella *persona fisica o giuridica, autorità pubblica…o qualsiasi altro organismo - da solo o assieme ad altri - determina finalità e strumenti del trattamento dei dati personali*, l'art. 26, § 1 del Regolamento precisa che, nel caso di *joint controllers*, questi possono dettagliatamente ed in maniera trasparente specificare le rispettive responsabilità in ordine alla *compliance* tra norme e *data processing*, con particolare riguardo, qui, ai diritti del *data subject* - che, peraltro, può azionarli, ai sensi del Regolamento, nei confronti di e contro ciascun titolare del trattamento - :

> Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

Si ribadisce dunque che il Regolamento innalza notevolmente il livello di obblighi e responsabilità, nelle quali ultime al titolare è unito il responsabile del trattamento: infatti, ex art. 32, § 1:

> il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio…..

e ancora, ex § 4:

Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento…

e ancora, di concerto, alla Sezione 2, art. 32 (Sicurezza del trattamento) ex § 1:

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio…

È evidente il nesso tra figure, responsabilità e ruolo del *controller* e del *processor*. Come pure è evidente che si tratta di una responsabilità di tipo pubblicistico, laddove l'art. 33 (rubricato: *Notifica di una violazione dei dati personali all'autorità di controllo*), § 1, prescrive che, in caso di *data breaches*,

… il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Ed al § 2, con riferimento al responsabile del trattamento:

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

È infatti palese che sia appunto di natura pubblicistica la responsabilità connessa all'obbligo della notifica alle Autorità, mentre la notifica all'interessato è solo eventuale, in quanto non è necessaria quando, (ex § 3):

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

o quando:

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1.

Rileva come nella vigente direttiva 95/49, invece, l'obbligo di informazione in caso di *data breach* è previsto solo nei confronti dell'interessato.

Rappresentano una novità, nell'impostazione del Regolamento, anche le previsioni di cui agli artt. 35 e 36 della Sezione 3 (*Valutazione d'impatto sulla protezione dei dati e consultazione preventiva*). In particolare, ex art. 35, il titolare del trattamento è tenuto ad effettuare, prima di procedere, *una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali* quando l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, *può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.*

È prevista anche una valutazione d'insieme, in quanto: *una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*.

In particolare, in base al § 3, il *controller* è tenuto al *data protection impact assessment*, qualora esso riguardi:

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.

È evidente che la disciplina innovata tiene conto sia dell'esperienza in materia, accumulata nei tre lustri successivi

all'emanazione della citata direttiva n. 46, sia delle indicazioni e dei pareri del Gruppo Articolo 29. Rileva, in proposito, il già citato Parere n. 3/2010 (WP n. 173) sul principio di responsabilità, ove si sottolinea che la valutazione del rischio e della connessa scelta delle misure da adottare deve essere continua, anzi immanente al trattamento stesso, cosicché le misure, appena risultino inadeguate a fronte di ulteriori rischi o di nuovi sviluppi nel campo delle tecnologie, possano essere opportunamente incrementate.

Vi è chi ritiene di natura pragmatica la responsabilità connessa all'obbligo di valutare costantemente l'impatto con le modalità di trattamento e le finalità da perseguire, in quanto *essa è già insita ed integrata nel dovere di rispettare le norme*; e inoltre le si riconosce anche una natura dinamica, perché è associata alla valutazione dell'impatto, che va costantemente aggiornata, *in parallelo con gli ulteriori sviluppi e diversificazioni* delle suddette modalità.

Il *data protection impact assessment* appare del resto assolutamente necessario, ove si consideri il livello d'automazione raggiunto dal trattamento, che è tale da consentire l'utilizzo *in puncto temporis* di milioni di dati.

E se indubbiamente la norma di cui all'art. 35 aggrava l'onere delle responsabilità connesse al ruolo del titolare, è altrettanto certo che accresce notevolmente il livello di protezione del *data processing* e, indirettamente, la credibilità degli *officer* nei confronti degli utenti, nonché lo spazio riservato all'autotutela, sia con riferimento alle Autorità di controllo, sia in previsione di ricorsi promossi per via giurisdizionale.

Ex articolo 36 (*Prior consultation*), il titolare del trattamento, nell'ipotesi in cui la valutazione d'impatto sulla protezione dei dati, a norma dell'articolo 35, indichi che il trattamento effettivamente presenterebbe un rischio elevato in assenza di misure adottate al fine di attenuarlo è tenuto a consultare, in proposito, l'Autorità di controllo, cui comunicherà altresì *le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale*, come pure le finalità e i mezzi del trattamento previsto; le misure predisposte a tutela dei diritti e delle libertà degli interessati; la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35; eventualmente i dati di contatto del *data protection officer*, ove esistente.

L'Autorità di controllo è tenuta a rispondere nei termini indicati dalla norma[17].

Rileva dunque come l'intero complesso delle disposizioni contenute nella Sezione III sia così dettagliato da comprovare l'influenza proveniente dall'esperienza di quasi tre lustri di applicazione della disciplina in materia, e tale gravoso insieme di regole e di responsabilità si inserisce nel novero dei doveri del titolare e, il più delle volte, del responsabile.

4. Il *Data Protection Officer*

La Sezione IV dunque introduce la figura - e le responsabilità - del *Data Protection Officer*, che viene designato dal titolare e dal responsabile ogni volta che il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico[18]; quando i trattamenti *per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala*, o quando *riguardino dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattino dati genetici*[19]*, 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. 8), o *dati concernenti condanne penali e reati* (art. 9).

---

[17] Art. 36, § 2: "Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione".

[18] Eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali [art. 37, comma 1, lett. a)].

[19] Si consenta il rinvio, in materia, a A. PARISI, *Sub artt. 85-90*, in *La nuova disciplina della* privacy, *Commentario diretto da* S. SICA - P. STANZIONE, Bologna, 2004, pp. 384 ss.

Tale designazione viene effettuata in base alle qualità professionali e, in particolare, in base alla *conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati*, o alla *capacità di assolvere i compiti di cui all'articolo 39*[20]; nell'eseguire i propri compiti il responsabile della protezione dei dati *considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.*

Il *Data Protection Officer* in realtà è una figura tipica del *common law* nordamericano e anglosassone in genere[21] e comune alle *holding* multinazionali: tramite il Regolamento essa viene introitata nella disciplina europea del trattamento dati assieme alle sue ben enumerate e dettagliate caratteristiche.

Infatti la previsione di cui all'art. 37 stabilisce l'obbligatorietà del *Data Protection Officer* per *autorità, uffici ed enti pubblici,* ma - in talune ipotesi - anche per i privati.

Ex art. 38, il responsabile della protezione dei dati è tempestivamente e adeguatamente coinvolto dal titolare e dal respon-

---

[20] Art. 39. *Compiti del responsabile della protezione dei dati*.1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo

[21] Il ruolo del responsabile della protezione dei dati appare nell'ordinamento tedesco (*Datenschutzbeauftragter*) nel 1970. Negli U.S.A. tale figura fu istituita per la prima volta nel 1999 dalla società *AllAdvantage*, produttrice di servizi pubblicitari *byInternet*, come risposta alle preoccupazioni dei consumatori sull'utilizzo dei propri dati personali, onde far fronte e gestire esigenze emergenti. Il Data Protection Officer dal 2013 fa parte del personale presidenziale della Casa Bianca.

sabile del trattamento in tutte le questioni riguardanti la protezione dei dati personali; riceve dagli stessi le risorse necessarie per assolvere ai suoi compiti, ma non riceve da loro istruzione alcuna per quanto riguarda l'assolvimento della sua funzione.

Infatti, il responsabile della protezione dei dati non risponde ("*non è rimosso o penalizzato*") al titolare o al responsabile del trattamento per l'adempimento dei propri compiti, ma, ex art. 38, § 3, *riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento*, ed è tenuto al segreto o alla riservatezza in merito all'adempimento, in conformità del diritto dell'Unione o degli Stati membri.

L'art. 39 definisce il ruolo del responsabile della protezione dati: oltre al compito di informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento in merito ai loro obblighi; di sorvegliare l'osservanza del Regolamento; di fornire, ove richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati, quel che maggiormente rileva è il suo ruolo di contatto per l'autorità di controllo per questioni connesse al trattamento, compresa la consultazione preventiva di cui all'art. 36.

5. L'ambito delle sanzioni

Per essere competitive e per fruire appieno delle opportunità offerte dalle nuove prospettive di mercato, aziende e imprese dovranno necessariamente avvalersi delle competenze di *privacy officers* opportunamente preparati per consentire il dialogo giuridico-economico attraverso le frontiere dei Paesi europei nel prossimo futuro unificati, non più 'armonizzati', nella conforme disciplina del nuovo mercato: e ciò, anche al fine di evitare le severe sanzioni da quella previste.

Il sistema delle sanzioni è disciplinato al Capo VIII, rubricato: *Mezzi di ricorso, responsabilità e sanzioni,* strutturato in otto articoli, dal 77 all'84.

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il Regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure nel luogo ove si è verificata la presunta violazione.

L'articolo 82, infatti, prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

In base alla lettera della norma (art. 82, § 2), mentre il titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi il Regolamento, il responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi specificatamente diretti dal Regolamento ai responsabili del trattamento o se ha agito in modo difforme o contrario rispetto alle istruzioni impartite dal titolare del trattamento.

La clausola di esonero di cui all'art. 82, § 3 prevede che il titolare del trattamento o il responsabile del trattamento sono esonerati dalla responsabilità di cui al § 2 se, rispettivamente, dimostrano che l'evento dannoso non è in alcun modo a loro imputabile.

Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, § 2, che recita:

Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.

L'articolo 83 invece stabilisce le *Condizioni generali per infliggere sanzioni amministrative pecuniarie.*

Tali sanzioni sono inflitte *in aggiunta o in sostituzione* delle misure che, ex art. 58, § 2, lett. da a) ad h), e j) rientrano nei *poteri correttivi* attribuiti alle Autorità di controllo[22].

---

[22] Rientrano in tali poteri, ex art. 58, § 2, le seguenti misure correttive: a)…**avvertimenti** al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento; b)…**ammonimenti** al titolare del trattamento

Rileva l'ampia discrezionalità conferita alle Autorità di controllo cui è rimessa la facoltà di 1. *decidere se infliggere una sanzione amministrativa pecuniaria*; 2. *fissare l'ammontare della stessa*; nonché l'onere di valutare le singole ipotesi di *data breaches* e di operare la scelta della sanzione adeguata.

Ogni Autorità provvederà ad irrogare le sanzioni amministrative pecuniarie in relazione alle disposizioni di cui ai §§ 4, 5 e 6.

In base al contenuto dell'art. 83, sono previste due tipologie di sanzioni, in rapporto a due precise categorie di violazioni. Tale duplice complesso di sanzioni è connotato da identiche modalità di erogazione, mentre è differente l'ammontare delle sanzioni stesse: ciò perché esse siano adeguate e proporzionate alla gravità del *data breach*, e - nel contempo - tali da integrare una giusta valenza dissuasiva.

Le due tipologie sono connesse a due categorie di violazioni, nella prima delle quali, ex art. 83, § 4 sono raggruppate le infrazioni 'meno gravi', che riguardano:

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43; b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

---

o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento; l'**ingiunzione** c)… al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti derivanti dal presente regolamento; l'**ingiunzione** d)...al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine; l'**ingiunzione** e)…al titolare del trattamento di comunicare all'interessato una violazione dei dati personali; la facoltà di f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento; la facoltà di g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19; la facoltà di h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti; la facoltà di j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale. Il medesimo art. 58, § 2, alla lett. i) conferisce alle Autorità di controllo il potere di: *infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso.*

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4.

Per queste violazioni l'autorità di controllo può comminare una sanzione amministrativa pecuniaria fino a 10.000.000 di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Le sanzioni più severe, invece, sono comminate, ex § 5 del medesimo art. 83, per violazione delle seguenti disposizioni:

> a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9; b) i diritti degli interessati a norma degli articoli da 12 a 22; c) i trasferimenti di dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale a norma degli articoli da 44 a 49; d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX; e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

In entrambi i casi, ex art. 83 § 2, ultimo comma, le Autorità di controllo fisseranno l'ammontare della sanzione, nei rispettivi limiti prefissati, tenendo conto dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito; b) il carattere doloso o colposo della violazione; c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati; d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32; e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento; f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; g) le categorie di dati personali interessate dalla violazione; h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione; i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti; j) l'adesione ai codici

di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42 e k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Nel caso in cui in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del Regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

L'art. 83, al § 7 dispone che, fatti salvi i poteri correttivi delle Autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possano essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro; e, al § 9, qualora l'ordinamento giuridico nazionale non preveda sanzioni amministrative pecuniarie dispone che l'azione sanzionatoria sia solo avviata dall'autorità di controllo competente e che la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali.

Gli Stati membri provvederanno a notificare alla Commissione le disposizioni di legge adottate a norma del presente paragrafo entro il 25 maggio 2018, comunicando senza ritardo ogni successiva modifica.

Dal quadro sanzionatorio appena delineato emerge ancora una volta la prospettiva diversa della disciplina regolamentare al paragone di quella predisposta dalla direttiva 95/46: quest'ultima è diretta a tutelare, di volta in volta, il singolo nei confronti del titolare del trattamento; il Regolamento mira invece a sanzionare severamente i trattamenti illeciti, in una prospettiva ben più ampia della visione centrata sulla tutela dell'interessato, in quanto rivolta alla salvaguardia dell'intera collettività dai trattamenti illeciti, soprattutto qualora il numero rilevante o la particolare tipologia integrino rischi collettivi che travalicano il limite del singolo.

Ne è riprova la possibilità offerta non solo al *data subject* ma anche ad organizzazioni e associazioni: se a quello può tornare utile essere affiancato nella propria azione di rivalsa, sembra invece prevaricare il diritto del singolo la facoltà concessa a tali associazioni ed organizzazioni di promuovere il ricorso alle

Autorità di controllo, anche senza il mandato dell'interessato e, quindi, anche contro la sua volontà ed intenzione.

La nuova normativa dunque, pur di preservare l'interesse generale della collettività dal rischio di trattamenti illeciti va oltre l'interesse del soggetto anzi lo priva della libertà di scegliere se far valere oppur no il proprio diritto.

Peraltro, tanto, in nome del superiore diritto alla tutela dei propri dati: né va dimenticato che nel percorso che ha visto evolversi il sistema di protezioni e di tutele considerato, tra la direttiva madre n. 95/46/CE ed il Regolamento va a posizionarsi la Carta dei diritti dell'Unione Europea siglata a Nizza il 7 dicembre 2000, che all'art. 8 riconosce come diritto fondamentale il diritto alla protezione dei dati[23]:

> Articolo 8. Protezione dei dati di carattere personale. 1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Talché dalla tutela di un 'diritto nuovo', utilizzato come strumento di armonizzazione nel mercato interno, si trascorre alla salvaguardia rafforzata da un rigido complesso di norme, in cui la protezione dei dati personali è inscindibilmente integrata nella tutela collettiva dei diritti e delle libertà fondamentali.

---

[23]Rileva che nel 2008 la Corte Costituzionale tedesca ha creato il nuovo diritto della personalità alla «garanzia della segretezza e integrità dei sistemi informatici» o *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, al fine di porre un argine alle indagini particolarmente invasive che si avvalgono delle tecnologie elettroniche ed informatiche. (Cfr. *BverfG* 27 febbraio 2008 (1 *BvR* 370/07; 1 *BvR* 595/07). In tema, cfr. R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* Online Durchsuchung, in *Riv. trim. dir. pen. econ*., 2009, 695).