IAIC MiBACT DGBIC CREDA

Diritto Mercato Tecnologia

FONDATA E DIRETTA DA
Alberto M. Gambino

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

9 Luglio 2018

Il *data breach* tra obblighi di notifica e principio di autoresponsabilità

Alessandra Spangaro

COMITATO SCIENTIFICO
Guido Alpa, Giovanni Comandè, Gianluca Contaldi, Luciana D'Acunto,
Vincenzo Di Cataldo, Giorgio Floridia, Gianpiero Gamaleri, Gustavo Ghidini,
Andrea Guaccero, Mario Libertini, Francesco Macario, Roberto Mastroianni,
Giorgio Meo, Cesare Mirabelli, Enrico Moscati, Alberto Musso,
Luca Nivarra, Gustavo Olivieri, Cristoforo Osti, Roberto Pardolesi, Giuliana Scognamiglio,
Giuseppe Sena, Andrea Stazi, Vincenzo Zeno-Zencovich, Andrea Zoppini
E
Margarita Castilla Barea, Cristophe Geiger, Reto Hilty, Ian Kerr, Jay P. Kesan,
David Lametti, Fiona MacMillan, Maximiliano Marzetti, Ana Ramalho,
Maria Pàz Garcia Rubio, Patrick Van Eecke, Hong Xue

Nuova
Editrice
Universitaria

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

Comitato dei Valutazione Scientifica

EMANUELA AREZZO (Un. Teramo), EMANUELE BILOTTI (Un. Europea di Roma), FERNANDO BOCCHINI (Un. Federico II), ROBERTO BOCCHINI (Un. Parthenope), ORESTE CALLIANO (Un. Torino), LOREDANA CARPENTIERI (Un. Parthenope), VIRGILIO D'ANTONIO (Un. Salerno), FRANCESCO DI CIOMMO (Luiss), PHILIPP FABBIO (Un. Reggio Calabria), MARILENA FILIPPELLI (Un. Tuscia), CESARE GALLI (Un. Parma), MARCO MAUGERI (Un. Europea di Roma), ENRICO MINERVINI (Seconda Un.), MARIA CECILIA PAGLIETTI (Un. Roma Tre), ANNA PAPA (Un. Parthenope), ANDREA RENDA (Un. Cattolica), ANNARITA RICCI (Un. Chieti), FRANCESCO RICCI (Un. LUM), GIOVANNI MARIA RICCIO (Un. Salerno), CRISTINA SCHEPISI (Un. Parthenope), BENEDETTA SIRGIOVANNI (Un. Tor Vergata), GIORGIO SPEDICATO (Un. Bologna), ANTONELLA TARTAGLIA POLCINI (Un. Sannio), RAFFAELE TREQUATTRINI (Un. Cassino), DANIELA VALENTINO (Un. Salerno), FILIPPO VARI (Un. Europea di Roma), ALESSIO ZACCARIA (Un. Verona).

Norme di autodisciplina

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

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

Comitato di Redazione – www.dimt.it – dimt@unier.it

PIERPAOLO ARGANELLI, MARCO BASSINI, SIMONA CASTALDO, GIORGIO GIANNONE CODIGLIONE, FRANCESCA CORRADO, CATERINA ESPOSITO, MONICA LA PIETRA, GAETANO MARINO, SILVIA MARTINELLI, DAVIDE MULA (Coordinatore), ALESSIO PERSIANI, ROSARIA PETTI, MARTINA PROVENZANO (Vice-Coordinatore), MATILDE RATTI, VALENTINA ROSSI, SILVIA SCALZINI

Sede della Redazione

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

Il *data breach* tra obblighi di notifica e principio di autoresponsabilità[1]

Alessandra Spangaro
Università "Alma Mater Studiorum" di Bologna

Sommario: 1. La direttiva europea 95/46 tra carenze originarie e disarmoniche applicazioni – 2. Il concetto di *data breach* e gli obblighi di notifica nel Regolamento 679/2016 – 3.*Segue*: Altre previsioni che impongono la notifica delle violazioni – 4. Il titolare quale soggetto passivo dell'obbligo di notifica e i soggetti che lo coadiuvano – 5. Quali responsabilità per quali soggetti?

1. La direttiva europea 95/46: carenze originarie e disarmoniche applicazioni

Come noto, la protezione dei dati personali ha trovato la sua fonte principale nella direttiva 95/46/CE[2] (c.d "direttiva madre") - promulgata anche al fine di evitare che la tutela della vita privata potesse ostacolare lo sviluppo del mercato interno[3] - attuata, nel nostro ordinamento dapprima con la L.

[1] Il presente lavoro è il frutto della partecipazione al FP7 Security Project ECOSSIAN -European COntrol System Security Incident Analysis Network, http://ecossian.eu/.

[2] Per un'analisi della direttiva cfr. Macario, *La protezione dei dati personali nel diritto privato europeo*, in *La disciplina del trattamento dei dati personali*, a cura di V. Cuffaro e V. Ricciuto, Torino, 1997, 12 ss. Tra le altre fonti del diritto alla protezione dei dati personali bisogna inoltre citare la *Carta dei diritti fondamentali dell'Unione europea*, il cui art. 8 precisa che ogni individuo ha diritto alla tutela dei dati personali che lo riguardano. Con specifico riferimento all'ordinamento italiano, occorre invece far riferimento all'art. 2 Cost., quale clausola generale a tutela dei diritti fondamentali della persona, per tutti cfr., con riferimento alla disciplina costituzionale: Barbera, sub art 2, in *Comm. Cost. Branca*, Bologna-Roma, 1975; con più preciso riguardo alla *privacy*: Finocchiaro G., Privacy *e protezione dei dati personali*, Bologna, 2012, 5.

[3] Secondo il *considerando* n. 9, infatti, *gli Stati membri non potranno più ostacolare la libera circolazione tra loro di dati personali per ragioni inerenti alla tutela dei diritti e delle libertà delle persone fisiche*; la premessa ad un tale assunto può

31 dicembre 1996, n. 675, rubricata *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, successivamente sostituita dal c.d. *Codice privacy*, L. 30 giugno 2003, n. 196.

Tale direttiva è tuttavia stata recentemente abrogata dal Regolamento UE 2016/679 (GDPR), "*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*"[4], applicabile dal 25 maggio 2018, teso a superare una serie di incongruenze alle quali aveva condotto la disarmonica applicazione della direttiva ad opera degli Stati membri.

Proprio la forma giuridica della direttiva, che, in quanto tale, richiede una norma interna di attuazione, ha infatti aperto la strada ad alcune modifiche in sede di recepimento da parte degli Stati membri e ciò ha fatto sì che siano stati almeno in parte vanificati gli auspici di uniformità che avevano mosso il legislatore europeo[5]. Con riguardo all'ordinamento italiano, per esempio, il *Codice privacy*[6] contiene una definizione di "dato anonimo"

---

rinvenirsi, tra l'altro, nel terzo *considerando*, per il quale *l'instaurazione e il funzionamento del mercato interno [...] esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona*.

[4] Il Regolamento cit. insieme alla Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, "*relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*" viene così a formare il nuovo "Pacchetto protezione dati", vale a dire l'insieme normativo che definisce un quadro comune in materia di tutela dei dati personali per tutti gli Stati membri dell'UE, cui si aggiunge la Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, "*sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi*".

[5] Finocchiaro G., *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm*., 2017, 1 ss., spec. 5 ss.

[6] Alla data del 25 maggio 2018 le norme del Codice Privacy incompatibili con il GDPR devono ritenersi abrogate; attualmente presso le Camere sono in corso i lavori delle Commissione Speciali per l'esame di atti di Governo, per l'analisi dello schema di decreto legislativo - delegato dalla L. 163/2017 – recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR. Si noti

(art. 4, lett. *n*)[7] assente nella direttiva, la quale ne riferiva solo il concetto embrionale, da individuarsi *per relationem*, in ragione del fatto che "*per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona*" (*considerando* n. 26).

Invero, il concetto di *dato anonimo* non è estraneo al legislatore europeo, che vi fa espresso riferimento non nella c.d. "direttiva madre", bensì nella direttiva 2002/58/CE[8], relativa al trattamento dei dati personali e alla tutela

---

che sul medesimo Codice si dovrà intervenire anche quando sarà approvata la Proposta di Regolamento E-provacy, 10.1.2017 COM(2017) 10 final 2017/0003 (COD), *relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche*, cfr. meglio sul punto nt. 8.

[7] Il "dato anonimo" è quello che *in origine o a seguito di trattamento non può essere associato ad un interessato identificato o identificabile* (art. 4, lett. *n*, *Cod. privacy*); in argomento cfr. Finocchiaro G., Privacy *e protezione dei dati personali*, cit., 48 ss.; Id., voce *Anonimato,* in *Dig. Disc. Priv., Sez. civ., Agg. V*, Torino, 2010, 12 ss.; Buttarelli, *Banche dati e tutela della riservatezza*, Milano, 1997; Pelino, *La nozione di dato anonimo*, in *Diritto all'anonimato. Anonimato, nome e identità personale*, a cura di G. Finocchiaro, Padova, 2008, 31 ss.; cfr. anche nt. 11.

[8] La direttiva ha trovato recepimento, nel nostro ordinamento, negli artt. 121-134 *Codice Privacy*; si riferiscono ai "dati anonimi" gli artt. 6 e 9 della direttiva cit., detta normativa, inoltre, al nono *considerando* enuncia il principio c.d. "di minimizzazione", che pone l'obiettivo "di ridurre al minimo il trattamento dei dati personali e di utilizzare i dati anonimi o pseudonimi nella misura del possibile"; in ragione di ciò, il successivo *considerando* 26 dispone che "i dati relativi al traffico utilizzati per la commercializzazione dei servizi di comunicazione o per la fornitura di servizi a valore aggiunto dovrebbero […] essere cancellati o resi anonimi dopo che il servizio è stato fornito". Anche la direttiva 2002/58/CE - così come avvenuto per la direttiva 95/46/CE – è destinata ad essere abrogata e sostituita da un regolamento europeo *relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche*; ad oggi è reperibile una Proposta di Regolamento E-provacy, 10.1.2017 COM(2017) 10 final 2017/0003 (COD), reperibile in https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A52017PC0010, ove si precisa al *considerando n. 38* che "*onde garantire la pirna coerenza con il regolamento (UE) 2016/679, l'applicazione delle disposizioni del presente regolamento dovrebbe essere affidata alle stesse autorità responsabili dell'applicazione di detto regolamen-*

della vita privata nelle comunicazioni elettroniche (c.d. "direttiva *e-privacy*"). Anche in questo caso, tuttavia, la nozione di "anonimato" non è stata recepita uniformemente nei diversi Paesi europei, basti pensare che in Germania, secondo il *Federal Data protection act,* un dato può qualificarsi come *anonimo* ove la decriptazione dello stesso richieda "una quantità *sproporzionata*[9] di tempi, costi e lavoro" [10]. In Italia, invece, valorizzando il concetto già enunciato nel *considerando* n. 26 della direttiva 95/46, si è fatto riferimento al criterio di *ragionevolezza*, per cui si considerava "anonimo" il dato che, ai fini della decriptazione, richiede sforzi, in termini di tempi e costi, che *ragionevolmente*[11] né il titolare del trattamento, né terzi possono sopportare[12]; più che di "dato anonimo" era dunque corretto parlare di "dato *ragionevolmente* anonimo", alla luce degli sforzi e dei mezzi

---

to; il presente regolamento è fondato sul meccanismo di coerenza del regolamento (UE) 2016/679".

[9] Corsivo aggiunto.

[10] Cfr. *Federal Data protection act* del 15 novembre 2006, art. 3, co. 6, reperibile in http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html, cfr. sul punto Finocchiaro G., Privacy *e protezione del dati personali*, cit., 54.

[11] Corsivo aggiunto.

[12] Sul punto, per tutti, cfr. Finocchiaro G., Privacy *e protezione dei dati personali*, cit., 48 ss., spec. 51 ss., , ove ben si mette in evidenza come l'anonimato non possa che essere un concetto relativo, valutabile in ragione degli sforzi necessari a disvelare quell'informazione; così nel parere 4/2007, adottato il 20 giugno 2007 – WP 136 - , reperibile in http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1496512, il Gruppo di lavoro *ex* articolo 29 ha definito il dato anonimo come le "*informazioni concernenti una persona fisica che non può essere identificata né dal responsabile del trattamento né da altri, prendendo in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati"* (p.21); cfr. anche Pelino, *La nozione di dato anonimo*, cit., 46; Del Federico, Popoli, *Disposizioni generali*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da G. Finocchiaro, Bologna, 2017, 63. Analogamente si è espressa la raccomandazione del Consiglio d'Europa R (97)5 sulla protezione dei dati sanitari che parla di *"irragionevole lasso di tempo e di lavoro*" ai fini dell'identificazione. Cfr. anche il parere 5/2014, adottato il 10 aprile 2014 – WP 216 – sulle tecniche di anonimizzazione, reperibile in http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3070528; cfr. in argomento esaustivamente Finocchiaro G. (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, in *Tratt. Dir. comm. e pubbl. dell'econ*., diretto da F. Galgano, Padova, 2008.

necessari per la decriptazione, concetto oggi richiamato nel Regolamento (*considerando n.* 26)[13].

Ancora, la direttiva 95/46/CE non conteneva una definizione di *dato sensibile,* pur accogliendone il concetto nell'art. 8, co. 1°, rubricato *Trattamenti riguardanti categorie particolari di dati* - che vietava agli Stati membri "il trattamento di dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale" -, previsione che è stata poi apparentemente ricalcata dal legislatore italiano nel *Codice privacy* (art. 4 lett. *d*, per il quale i *dati sensibili* sono "*dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*").

La disposizione italiana e quella europea, a tutta prima quasi sovrapponibili, manifestano tuttavia una differenza che appare lessicalmente poco significativa, ma che è invece concretamente fondamentale. Secondo la direttiva europea, infatti, i dati che in Italia sono stati definiti *sensibili*, sono quelli "*che rivelano*[14] l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose" ecc. (art. 8, co. 1°, cit.). La corrispondente previsione del

---

[13] Cfr. *considerando n. 26* del GDPR, per il quale si deve far riferimento al concetto di "*pseudonimizzazione*", per i dati "*i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni"*, persone che dunque devono considerarsi *identificabili*. Continua il *considerando n. 26* "*Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può* ragionevolmente *avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la* ragionevole *probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici"*. Sono invece "*informazioni anonime*", quelle "*che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato*". Il GDPR, conclude il *considerando n. 26,* non si applica pertanto al trattamento di tali informazioni anonime,

[14] Corsivo aggiunto.

Codice privacy identifica invece il *dato sensibile* come il "dato personale *idoneo a rivelare*[15] l'origine razziale ed etnica, le convinzioni religiose", ecc. (art. 4, lett. *d,* cit.).

Si mostra dunque, in tutta evidenza, come da una lieve variazione lessicale possano derivare effetti pratici di non poco momento, posto che l'espressione utilizzata dal legislatore italiano, rispetto a quella elaborata in sede europea, finisce per ampliare notevolmente il novero dei dati qualificabili come *sensibili* e, correlativamente, anche la discrezionalità di colui che è chiamato a valutarne le potenzialità disvelatrici[16].

Ed ancora, una discrasia di rilievo tra la disciplina della direttiva e le disposizioni del *Codice privacy* si evidenzia con riguardo al consenso al trattamento dei dati personali.

Il *Codice*, infatti, non contiene alcuna definizione di *consenso*, facendo un implicito riferimento al concetto comune riassuntivamente enucleabile nell'espressione "manifestazione di una volontà conforme"[17]. Al contrario, la direttiva 95/46 cit. conteneva una espressa e precisa definizione del concetto in esame (art. 2 lett. *h*)[18]; ma la differenza fondamentale in argomento è rinvenibile in materia di trattamento effettuato da enti pubblici non eco-

---

[15] Corsivo aggiunto.

[16] Il GDPR ridefinisce la categoria dei *dati sensibili,* facendo riferimeno a *categorie particolari di dati personali* (art. 9).

[17] Si precisa tuttavia che il consenso deve essere "espresso liberamente" e "documentato per iscritto" e deve invece essere "manifestato in forma scritta quando il trattamento riguarda dati sensibili", cfr. art. 23 Cod. privacy.

[18] Ai sensi della quale il "consenso della persona interessata" consiste in "qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento" (art. 2, lett. *h*). Nel GDPR, al *considerando n. 40* si precisa che "*Perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato o su altra base legittima prevista per legge dal presente regolamento o dal diritto dell'Unione o degli Stati membri*"; la relativa definizione è contenuta nell'art. 4, n. 11. Gli altri casi di liceità del trattamento, oltre, quindi il caso in cui l'interessato abbia prestato il proprio consenso, sono indicati nell'art. 6, tra quesi casi alla lettera *e)* è previsto quello in cui "*il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*"; ciò che rileva ai fini della liceità del trattamento è dunque la finalità e non la natura pubblica o privata del titolare.

nomici[19]: più precisamente, mentre la direttiva non distingueva a seconda che i dati venissero trattati da enti privati o enti pubblici - predisponendo una serie di *Principi relativi alla legittimazione del trattamento dei dati* (art. 7, dir. cit.), valevole per chiunque assuma il ruolo di *titolare* -, nel Codice *privacy* è invece disposto che il trattamento da parte di un ente pubblico non economico possa essere svolto anche in mancanza del consenso dell'interessato, purché ciò sia necessario per lo svolgimento delle funzioni istituzionali dell'ente medesimo (art. 18, co. 1, *cod. privacy*)[20].

[19] Non è possibile, in questa sede, analizzare la tangente questione circa la qualificabilità come "pubblico" ovvero come "privato" di un ente, basti qui richiamare i principi enucleati da Cass. S.U.,7 aprile 2010, n. 8225, in *Giorn. Dir. amm*., 2010, 620, per la quale "Ai fini della qualificazione di un ente come organismo di diritto pubblico, l'art. 3, comma 26, del d. lgs. n. 163 del 2006 deve essere interpretato, alla stregua della giurisprudenza comunitaria, nel senso che devono sussistere cumulativamente i seguenti tre requisiti: *a*) l'ente deve essere dotato di personalità giuridica; *b*) la sua attività deve essere finanziata in modo maggioritario ovvero soggetta al controllo o alla vigilanza da parte dello Stato o di altro ente pubblico territoriale o di organismo di diritto pubblico; *c*) l'ente (anche in forma societaria) deve essere istituito per soddisfare esigenze di interesse generale, aventi carattere non industriale o commerciale. In particolare, quest'ultimo requisito non sussiste quando l'attività sia svolta nel mercato concorrenziale e sia ispirata a criteri di economicità, essendo i relativi rischi economici direttamente a carico dell'ente"; Cass., S.U., 29 maggio 2012, n. 8511, reperibile nella banca dati *pluris* la quale esclude che la società Poste Italiane possa essere considerata un "organismo di diritto pubblico […], mancando il requisito del soddisfacimento di esigenze di interesse generale aventi carattere non industriale o commerciale (art. 3, comma 26, d.lgs. n. 163 del 2006) e trattandosi di un'impresa che, seppure per un settore definito, opera in regime di concorrenza ed è quindi esposta al funzionamento naturale del mercato". In dottrina si permetta per tutti il rinvio a: Ottaviano, voce *Ente pubblico*, in *Enc. dir.*, Milano, XIV, 1965, 961 ss., ove si precisa che "poiché la pubblicità è relativa ad una certa regolamentazione, la dichiarazione della natura pubblica di un ente che sia in contrasto con la disciplina in effetti disposta, da sola non sarebbe sufficiente a farlo qualificare pubblico. Normalmente, però, con il dichiarare che un ente è pubblico il legislatore intende indicare la regolamentazione pubblica che vuole applicare all'ente, sicché tale dichiarazione vale come espressione riassuntiva di siffatta normativa"; Cerulli Irelli, *Ente pubblico: problemi di identificazione e disciplina applicabile*, in *Ente pubblico ed enti pubblici*, a cura di Cerulli Irelli e Morbidelli, Torino, 1994, 89 ribadisce che "non basta una mera disposizione del legislatore per dire che un ente è pubblico".

[20] Sull'attuale disciplina nel GDPR, cfr. nt. 17.

Si tratta dunque di una netta bipartizione tra trattamento effettuato dall'ente privato, che richiedeva il consenso dell'interessato, e trattamento effettuato dall'ente pubblico non economico, che *non* richiedeva il consenso; bipartizione che non era prevista nella direttiva.

Invero, un punto di contatto tra le due previsioni poteva rinvenirsi laddove la direttiva precisava che il consenso non era richiesto ove il trattamento fosse "*necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento*" (art. 7, lett. *c*); tuttavia che la normativa italiana potesse essere ricondotta alla suddetta previsione non è affatto certo, sembra anzi potersi confermare la divergenza tra le due discipline laddove si ponga mente al fatto che la previsione europea si riferiva all'adempimento di un *obbligo legale*, così sembrando prendere in considerazione le *funzioni* esercitate da quell'ente[21], mentre nel Codice *privacy* la qualificazione del titolare del trattamento (quale ente pubblico o ente privato) derivava esclusivamente dalla natura giuridica del medesimo, prescindendo dunque dalle funzioni che esso in concreto esercita[22].

Infine, per arrivare al cuore del presente lavoro, anche per i casi di violazioni o incidenti al sistema atto al trattamento dei dati (c.d. *data breach*) i diversi ordinamenti si differenziavano non poco (cfr. par. 2), anche a cagione del fatto che la direttiva madre non si era occupata specificamente del tema, di modo che, nonostante gli sforzi definitori e descrittivi del Gruppo *ex* art. 29[23], ciascuno Stato membro è stato libero di optare per la disciplina ritenuta più opportuna.

---

[21] Finocchiaro G., Privacy *e protezione dei dati personali*, cit., 147; Bravo F., *Il consenso e le altre condizioni di liceità del trattamento dei dati personali*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da G. Finocchiaro, cit., 136.

[22] Finocchiaro G., Privacy *e protezione dei dati personali*, cit., 146-147 per meglio evidenziare come la bipartizione sia fondata non già sull'attività svolta dall'ente, bensì sulla natura giuridica del medesimo, precisa come, conseguentemente, anche un concessionario delle imposte debba essere considerato un privato.

[23] Come noto il Gruppo di lavoro è stato istituito dalla previsione di cui all'art. 29, dir. 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono individuati nell'art. 30 della dir 95/46/CE e nell'art. 15 dir. 2002/58/CE. Cfr. http://ec.europa.eu/justice/data-protection/index_en.htm. DEF; sul parere in argomento (n. 3 del 25 marzo 2014),

Quanto su brevemente riportato evidenzia, in sintesi, come le norme di recepimento da parte dei diversi Stati membri della direttiva 95/46 cit. si siano sovente allontanate, anche in modo sensibile, dalla disciplina comunitaria, finendo per frustrare l'originario intento uniformatore del legislatore europeo[24]. Di qui l'esigenza del Regolamento UE 2016/679, che, in quanto tale, trova applicazione immediata negli Stati membri, agevolando dunque l'affermarsi di una disciplina uniforme a livello comunitario.

2. Il concetto di *data breach* e gli obblighi di notifica nel Regolamento

Il concetto di *data breach*, come accennato nel paragrafo precedente, non era stato contemplato nella c.d. "direttiva madre"; nella pur ampia regolamentazione del trattamento dei dati personali restava dunque spoglio il profilo relativo al concetto di violazione dei dati medesimi.

Solo quasi una decina di anni dopo e con specifico riferimento al settore delle telecomunicazioni, la c.d. direttiva *e-privacy* 2002/58/CE[25] ha imposto, in capo ai soli fornitori di servizi di comunicazione elettronica, l'obbligo di adottare "appropriate misure tecniche e organizzative" per assicurare "un livello di sicurezza adeguato al rischio esistente" (art. 4, co. 1), precisando[26] doversi tenere in debito conto il fatto che un evento che coin-

---

reperibile in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213, v. meglio § 2.

[24] Anche la Corte di Giustizia, cause riunite C-468/2010 e C-469/2010, reperibile in https://curia.europa.eu/jcms/jcms/j_6/it/, aveva infatti rilevato che la c.d. direttiva madre mira a "rendere equivalenti in tutti gli Stati membri il livello di tutela dei diritti e delle libertà delle persone riguardo al trattamento dei dati personali", aggiungendo che "l'armonizzazione delle suddette legislazioni non si limita quindi ad un'armonizzazione minima, ma sfocia in un'armonizzazione che, in linea di principio, è completa". Di rilievo è inoltre il fatto che la direttiva si applica anche a Paesi che non sono parte dell'UE, ma che aderiscono al SEE (Spazio economico europeo), come la Norvegia, l'Islanda e il Lichtenstein.

[25] La direttiva è una delle cinque direttive che insieme formano il pacchetto Telecom, un quadro normativo che disciplina il settore delle comunicazioni elettroniche. Le altre direttive disciplinano il *quadro generale, l'accesso e l'interconnessione, l'autorizzazione e le licenze* e *il servizio universale, cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=URISERV%3Al24120.*

[26] Detta precisazione è invero posta dalla direttiva 2009/136/CE, che ha modificato la direttiva 2002/58/CE cit.

volge i dati personali, se non trattato in modo adeguato e tempestivo, può provocare un grave danno economico e sociale alle persone interessate[27].
La direttiva c.d. *e-privacy* (come poi modificata dalla direttiva 2009/136/CE) ha dunque introdotto il concetto di "violazione dei dati personali", da intendersi come la "*violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico nella Comunità*" (art 2 lett. h). A tale evento deve conseguire, senza indebito ritardo, la comunicazione all'autorità nazionale competente ed anche all'interessato, ma ciò solo nel caso in cui "*la violazione di dati personali rischi[a] di pregiudicare i dati personali o la vita privata*[28] *di un abbonato o di altra persona*" (art. 4, co.3).
Con il provvedimento di recepimento della direttiva 2002/58/CE[29] cit., il legislatore italiano ha conseguentemente introdotto, nell'art. 4 co. 3 del *Codice privacy,* la lett. g *bis*), la quale riferisce il concetto di violazione di dati personali sostanzialmente ricalcando la definizione fornita dal legislatore europeo[30].
Come evidente tale definizione è particolarmente ampia, atta a comprendere qualsiasi alterazione, accidentale o meno, dei dati trattati - sempre che

[27] cfr. GDPR, *considerando* n. 75. Come noto, il ruolo dei considerando deve ritenersi oggi fondamentale, in ragione dell'affermazione della Corte UE, 25 ottobre 2011, casi riuniti *eDate Advertising*, C509/09 e *Martinez*, C-161/10, par. 54 e 55, reperibile in http://curia.europa.eu, secondo la quale "il dispositivo di un atto dell'Unione è indissociabile dalla sua motivazione e deve essere pertanto interpretato, se necessario, tenendo conto dei motivi che hanno portato alla sua adozione", valutando non solo la lettera delle singole previsioni "ma anche il loro contesto e gli scopi perseguiti dalla normativa di cui esse fanno parte".
[28] La locuzione "i dati personali *o* la vita privata", con l'utilizzo della disgiuntiva *o*, costituisce un espresso indice normativo della divergenza tra i due concetti, cfr. per tutti Finocchiaro G., *Introduzione al regolamento europeo sulla protezione dei dati*, cit., 2.
[29] D. Lgs. 28 maggio 2012, n. 69.
[30] Anche nel Codice, quindi, inizialmente, non era prevista alcuna notifica in caso di *data breach*, salvo voler ricondurre tale obbligo al dovere di trattare i dati in modo lecito e corretto, di cui all'art. 11, lett. a).

questi possano essere definiti come *personali*[31] -; detta previsione, pur essendo divenuta parte integrante del *Codice privacy*, è tuttavia, come detto, relegata al solo "contesto della fornitura di un servizio di comunicazione accessibile al pubblico" (art. 4 co. 3, lett. g *bis* del *Codice privacy*) e dunque ad oggi sembra poter essere considerata ancora vigente, posto che la nuova disciplina, introdotta dal GDPR, si riferisce ad un contesto diverso.

Invero, più precisamente il GDPR ha esteso la previsione in materia di violazioni - originariamente riferita al solo mondo dei servizi di comunicazione elettronica - a qualsiasi tipo di trattamento di dati personali, in qualsiasi settore esso sia effettuato.

Ai sensi dell'art. 4, n. 12 del Regolamento UE 2016/679, oggi quindi la "violazione dei dati personali" (c.d. *data breach*) consiste in una "*violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*", a prescindere dunque dal contesto nel quale i dati vengono trattati[32].

---

[31] Il novero di ciò che può essere considerato *dato* personale è ad ogni modo molto ampio, dato che, come visto – cfr. testo – ai sensi dell'art. 2, lett. *a*) della c.d. "direttiva madre" e dell'art. 4, lett. *b*) del *Codice privacy* è "qualunque informazione relativa a persona fisica, identificata o identificabile". Restano esclusi dal novero dei "dati personali" dunque solo i dati riferibili ad un ente e i c.d. "dati anonimi", cui quali v. meglio nel testo. Con riguardo al concetto di *violazione* il Gruppo di lavoro *ex* art. 29, con il Parere 03/2014 – WP 213 – *sulla notifica delle violazioni dei dati personali, adottato il 25 marzo 2014*, reperibile in http://www.privacy.it/archivio/grupripareri201403.html, procede alla distinzione tra tre diversi casi di violazione dei dati personali: a) "violazione della disponibilità dei dati, vale a dire la distruzione accidentale o illecita o la perdita di dati personali"; b) "violazione dell'integrità dei dati", cioè l'alterazione dei medesimi; c) "violazione della riservatezza", in ragione della divulgazione o dell'accesso non autorizzato ai dati.

[32] L'art. 17 della *Proposta di Regolamento E-provacy, 10.1.2017 COM(2017) 10 final 2017/0003 (COD)*, rubricato "*Informazioni sui rischi relativi alla sicurezza rilevati*" prevede invece che "*Nel caso in cui esista un particolare rischio di compromettere la sicurezza delle reti e dei servizi di comunicazione elettronica, il fornitore di un servizio di comunicazione elettronica ne informa gli utenti finali e, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, comunica agli utenti finali tutti i possibili rimedi, compresi i relativi costi presumibili"*.

Secondo le *Linee guida* elaborate dal Gruppo *ex* art. 29[33] si ha una violazione nel caso in cui si verifichi un incidente inerente alla sicurezza dei dati personali, in conseguenza del quale il titolare non è più in grado di assicurare la *compliance* ai principi contenuti nell'art. 5 GDPR; questa è la differenza tra un mero incidente alle misure di sicurezza e una violazione dei dati personali (*data breach*), di modo che mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali[34].

Una volta verificatosi il *data breach*, il titolare del trattamento ha l'obbligo di *notificare* l'avvenuta violazione dei dati senza ingiustificato ritardo all'autorità di controllo (art. 33, GDPR, detta autorità, in Italia, è il *Garante per la protezione dei dati personali*) e di *comunicarla* all'interessato (art. 34, GDPR).

La diversa terminologia utilizzata (*notifica* all'autorità e *comunicazione* all'interessato) sembra voler richiamare la diversa portata delle due notizie; infatti la notizia all'autorità ha un contenuto più ricco rispetto a quella prevista per l'interessato, dovendo descrivere, tra l'altro, la natura della violazione e il numero approssimativo di interessati (art. 33, co. 3, lett. *a-d*; art. 34 co. 2 GDPR). In entrambi i casi, ad ogni modo, il titolare deve fornire al destinatario il contatto del responsabile dei dati, al quale poter chiedere informazioni.

Invero, l'obbligo di notifica della violazione non può dirsi assoluto ed anche in tal casi si rileva una disciplina differente a seconda che la notizia della violazione sia diretta all'autorità o all'interessato; con riguardo al Garante, infatti, la notifica della violazione, pur strettamente procedimentalizzata[35], è obbligatoria "a meno che sia *improbabile*[36] che la violazione dei

---

[33] *Linee guida* adottate il 3 ottobre 2017 – WP 250 – reperibili in https://www.lexology.com/library/detail.aspx?g=a7068f43-5e41-4668-8ed7-bd361bc9878c.

[34] *Linee guida* adottate il 3 ottobre 2017 – WP 250 – cit., p. 6.

[35] Il titolare deve infatti informare l'Autorità entro 72 ore dalla conoscenza del fatto; se la notifica è successiva si devono fornire le motivazioni del ritardo (art. 33, co. 1, Reg. UE 2016/679). Inoltre il Regolamento individua con precisione il contenuto della notifica, statuendo che essa deve contenere almeno: a) una descrizione della natura della violazione, compreso il numero approssimativo degli interessati;

dati personali presenti un rischio per i diritti e le libertà delle persone fisiche" (art. 33, co.1, Reg. UE 2016/679).

Con riguardo all'interessato, l'obbligo appare ancor meno stringente, in quanto sussiste solo se "la violazione dei dati personali è suscettibile di presentare un *rischio elevato*[37] per i diritti e le libertà delle persone fisiche"; anche in tale ipotesi, inoltre, la notifica non è obbligatoria se il titolare abbia posto in essere, anche *ex post*, le misure tecniche ed organizzative idonee a rendere i dati violati non intellegibili o comunque atte a scongiurare quel rischio per i diritti e le libertà delle persone, già su preso in considerazione (art. 34, co. 1 e 3, lett. *a*) e *b*), GDPR).

---

b) il nome e i dati del responsabile o del punto di contatto presso cui poter ottenere maggiori informazioni; c) una descrizione delle probabili conseguenze della violazione (art. 33, co. 3, Reg. UE 2016/679).

[36] Corsivo aggiunto. Il testo in inglese dell'art. 33 co. 1 del GDPR recita "*unless the personal data breach is* unlikely *to result in a risk to the rights and freedoms of natural persons*". Analoga terminologia è utilizzata nella direttiva 2016/680/EU, "*relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati*", all'art. 30. Le *Linee Guida* del gruppo *ex* art. 29, adottate il 3 ottobre 2017 – WP 250 – cit., pp. 15 ss., richiamando quanto già affermato nel parere in materia di *data breach*, n. 3 adottato il 25 marzo 2014 – WP 213 – reperibile in http://collections.internetmemory.org/haeu/20180102065554/http://ec.europa.eu/justice/data-protection/article29/ documentation/opinion-recommendation/files/2014/wp213_en.pdf, vale a dire che una violazione della riservatezza di
i dati personali che sono stati crittografati con un algoritmo avanzato costituisce comunque una violazione dei dati personali e, come tale deve essere notificata, precisa oggi ulteriormente che se la chiave di sicurezza è rimasta intatta, e dunque i dati sono in linea di principio non intellegibili ed esista una copia di *backup*, se ne ricava che sia *improbabile* che la violazione possa influire negativamente sulle persone e pertanto non sembra richiedere la notifica all'autorità e/o la comunicazione agli interessati.

[37] Corsivo aggiunto. Il testo inglese dell'art. 34 del GDPR recita "*a* high risk *to the rights and freedoms of natural persons*". Analoga terminologia è utilizzata nella direttiva 2016/680/EU, "*relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati*", all'art. 31.

Appare in conclusione evidente l'ampia discrezionalità valutativa, in capo al titolare del trattamento, circa la doverosità o meno della comunicazione; come detto, il margine di discrezionalità appare un po' meno ampio ove ci si riferisca all'obbligo di notifica all'Autorità garante ("rischio *improbabile*"), rispetto all'obbligo di notifica all'interessato ("rischio *elevato*")[38].

Tale ampio margine di discrezionalità non è invero nuovo alla disciplina del c.d. *data breach*; anche al fornitore di servizi di comunicazione – oggetto della dir. 2008/58/CE cit. – è infatti permesso di non procedere alla notifica all'interessato se "*ha dimostrato in modo convincente all'autorità competente di aver utilizzato le opportune misure tecnologiche di protezione*" (art. 4, co. 3, dir. cit.)[39].

Un rilevante elemento differenzia tuttavia nettamente le due ipotesi: il fornitore di servizi è comunque tenuto alla notifica all'autorità, la quale vaglierà se esentarlo o meno dalla notifica all'interessato. Nel caso disciplinato dal Regolamento UE 2016/679, invece, a tale valutazione procede direttamente il titolare, rispetto al quale, come evidente, non può certo escludersi l'ipotesi del conflitto di interessi.

Una situazione sostanzialmente analoga a quella su esposta si riscontra anche con riguardo alla direttiva 2016/680/EU, "*relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati*", che, insieme al Regolamento 2016/679, va a completare il cosiddetto "pacchetto protezione dati" che la Commissione europea presentò ufficialmente nel 2012.

In considerazione del fatto che la violazione dei dati personali può comportare, ancor più se non affrontata in modo adeguato e tempestivo, danni sia

[38] Previsione che ben sembra avvalorare quell'interpretazione secondo la quale la tutela dei dati personali, pur riconducibile all'alveo dei diritti della personalità, costituisce un diritto meramente strumentale, cfr. Finocchiaro G., Privacy *e protezione dei dati personali*, cit., 26.

[39] Precisa la norma che tali misure possono ritenersi idonee se "rendono i dati incomprensibili a chiunque non sia autorizzato ad accedervi".

materiali che immateriali[40], la direttiva pone a carico del titolare del trattamento l'obbligo di notificare la violazione, non appena ne venga a conoscenza[41], provvedendo a disciplinare anche – come già visto con riguardo al Regolamento UE 2016/679 – il contenuto della relativa comunicazione all'autorità di controllo competente e all'interessato (artt. 30, 31, dirett. 2016/680).

Rispetto alla disciplina del Regolamento UE 2016/679 si riscontra tuttavia, anche in tal caso, un rilevante elemento differenziale: secondo la direttiva 2016/680 il titolare è sempre tenuto alla notifica all'autorità, ma potrà non notificare all'interessato, laddove abbia posto in essere, anche *ex* post, le misure tecniche ed organizzative idonee a rendere i dati violati non intelle-

[40] Per esempio furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, alla riservatezza, al segreto professionale cfr. *considerando* 61 della direttiva cit.

[41] Anche in tal caso si precisa che la notifica dovrebbe avvenire entro le 72 ore dalla conoscenza del fatto, "a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo", cfr. *considerando* 61 cit. Aggiunge il *considerando* 62 che "Le persone fisiche dovrebbero essere informate senza ingiustificato ritardo in caso di violazione dei dati personali suscettibile di presentare un rischio elevato per i loro diritti e le loro libertà affinché possano prendere le precauzioni del caso. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e comprendere raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. La comunicazione agli interessati dovrebbe essere effettuata non appena ragionevolmente possibile, in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati sia tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni ripetute o analoghe dei dati potrebbe giustificare più tempo per la comunicazione. Qualora non fosse possibile evitare di compromettere indagini, inchieste o procedimenti ufficiali o giudiziari, evitare di pregiudicare la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, proteggere la sicurezza pubblica o la sicurezza nazionale o tutelare i diritti e le libertà altrui ritardando o limitando la comunicazione di una violazione dei dati personali alla persona fisica interessata, detta comunicazione potrebbe, in casi eccezionali, essere omessa".

gibili o comunque atte a scongiurare rischi per i diritti e le libertà delle persone (art. 31, co. 2).
Nel regolamento UE 2016/679, invece, come detto, il titolare valuta discrezionalmente l'opportunità di procedere alla notifica non solo all'interessato, ma anche all'Autorità.
Si palesa dunque come le esigenze che hanno spinto il legislatore ad ampliare l'obbligo di notifica dei casi di c.d. *data breach,* imponendolo a tutti coloro che effettuano un trattamento di dati personali – così quindi superando il perimetro inizialmente individuato nei soli casi di fornitura di un servizio di comunicazione accessibile al pubblico –, siano controbilanciate da altre esigenze, certamente non prive di rilievo, riconducibili genericamente alla necessità di tutelare il buon nome e l'immagine imprenditoriale del titolare del trattamento, il quale, ovviamente, finisce per perdere credibilità ad ogni notizia di violazione, con evidenti ripercussioni sulla sua reputazione economica[42]. Il fatto che l'obbligo di notifica della violazione trovi frequenti eccezioni non esclude ad ogni modo che ad esso possa riconoscersi il rango di previsione a carattere generale, in quanto posta non solo nel Regolamento cit., ma anche in diverse altre previsioni normative di origine europea, con riguardo sia all'ambito dei rapporti interprivati, sia a quelli tra gli Stati membri, a dimostrazione di una sensibilità più spiccata che in passato sul tema della sicurezza delle reti (cfr. § successivo).

3. *Segue*: Altre previsioni che impongono la notifica delle violazioni

Nonostante il fatto che – come visto nel paragrafo precedente – l'esigenza di avvertire l'interessato in caso di *data breach* non possa ancora oggi dirsi completamente tutelata, cedendo il passo a fronte di interessi ritenuti prevalenti, deve ad ogni modo rilevarsi che la sensibilità sul tema è andata nel tempo sempre più maturando. Mentre, infatti, la *direttiva madre* non con-

[42] Sul concetto di *reputazione economica* e sulle relative implicazioni, cfr. Zeno Zencovich, *Comunicazione, reputazione, sanzione*, in *Dir. Inf.,* 2007, 271; Ricci A., *La reputazione nell'era digitale*, in *Diritto dell'informatica*, a cura di Finocchiaro e Delfini, Torino, 2014, 197 ss.; Id., *La reputazione: dal concetto alle declinazioni*, Torino, 2018, 126 e spec. 144 ss.; e già Auteri, *La tutela della reputazione economica*, in *L'informazione e i diritti della persona*, a cura di Alpa, Bessone, Boneschi, Caiazza, Napoli, 1983, 94.

templava alcun preciso obbligo in caso di *data breach*, nei provvedimenti normativi successivi l'opportunità di una tale previsione è stata sempre più frequentemente avvertita, con il chiaro intento di accrescere la fiducia dell'utente nelle comunicazioni e negli scambi *on line* e, nel contempo, rendere le reti e i sistemi informativi sempre più affidabili e sicuri[43].

Un primo obbligo di notifica che sostanzialmente ricalca gli schemi definiti nel GDPR è posto dalla già richiamata direttiva 2016/680/EU, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, ove è previsto l'obbligo di notifica sia all'autorità - "a meno che *sia improbabile* che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche" (art. 30) – sia all'interessato, "quando la violazione dei dati personali è suscettibile di presentare un *rischio elevato* per i diritti e le libertà delle persone fisiche" (art. 31).

Si deve, tra l'altro, notare che l'esigenza di creare una maggior fiducia nei c.d "sistemi informativi sicuri", con conseguente obbligo di comunicazione delle eventuali violazioni, è comunemente riferita ai dati dei soggetti privati, ma è ovviamente e forse ancor più urgente laddove si tratti di informazioni di rilievo pubblicistico, relative ad interessi nazionali di un Paese; ed infatti oggi possiamo trovare obblighi di notifica delle violazioni non solo nell'ambito del trattamento dei dati delle persone fisiche, ma anche nell'ambito dei rapporti tra Stati membri e tra questi e la Commissione, rapporti dunque tradizionalmente, come detto, inquadrabili nella sfera pubblicistica se non addirittura nella sfera di sovranità propria di ciascun Paese.

[43] In questi esatti termini si esprime la direttiva 2016/1148/EU recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione, c.d. direttiva "NIS", *considerando* 1. La direttiva ed in genere le nuove normative europee che disciplinano il c.d. *data breach* e i conseguenti obblighi di informazione trovano antecedenti in alcuni studi elaborati dall'ENISA, *Data breach notification in EU*, reperibile in https://www.enisa.europa.eu/ publications/dbn; ENISA "*Recommendations for a methodology of the assessment of severity of personal data breaches*, reperibile in https://www.enisa.europa.eu/ publications/dbn-severity or att. 5.

Si tratta ovviamente di un profilo differente da quello fin'ora analizzato, strettamente inerente alla tutela dei dati personali, ma che va a confermare l'importanza affidata dal legislatore europeo alla comunicazione delle violazioni, quale strumento utile a diffondere negli utenti la fiducia nei servizi informativi, di comunicazione ed anche di identificazione elettronica.

A tale riguardo si deve dunque citare l'obbligo di notifica previsto nella direttiva sulla sicurezza delle reti e dei sistemi informativi (dir. 2016/1148/EU, c.d. *direttiva NIS*), ove - rilevando che i servizi informativi "svolgono un ruolo vitale nella società"[44] e dunque è "essenziale che essi siano affidabili e sicuri"[45] - si impone agli Stati membri di vigilare affinché i fornitori di servizi digitali adottino misure tecniche ed organizzative per la migliore sicurezza della rete[46], alla luce delle "conoscenze più aggiornate della materia" (art. 16). In caso di incidenti rilevanti[47], i fornitori dei servizi devono avvisare senza ritardo l'autorità competente, la quale, ove l'incidente abbia impatto transfrontaliero, provvederà ad informare gli altri Stati membri, preservando "la sicurezza e gli interessi commerciali dell'operatore […], nonché la riservatezza delle informazioni" (art. 16, co. 6); se utile a ridurre gli effetti negativi dell'evento, l'autorità può anche diffondere l'informazione al pubblico (art. 14, co. 5 e 6).

Ed ancora troviamo obblighi di notifica delle violazioni nel c.d. Regolamento *e-IDAS*, n. 2014/910/EU[48] in materia di identificazione elettronica, teso a realizzare l'interoperabilità giuridica e tecnica degli strumenti elettronici di identificazione, autenticazione e firma fra i Paesi dell'Unione eu-

[44] Cfr. *considerando* n. 1.

[45] *Ut Supra*.

[46] Sia per prevenire, sia per minimizzare gli impatti degli incidenti a carico della rete" (art. 16, co. 2, dir. *NIS*).

[47] La direttiva *NIS* fornisce i criteri per valutare se l'incidente possa dirsi "rilevante" all'art 16, co. 4; in proposito occorre valutare, tra l'altro, il numero di utenti interessati dall'incidente, la durata e la diffusione geografica dello stesso, l'impatto che il medesimo avrà sulle attività economiche e sociali.

[48] Sul Regolamento 2014/910/EU cfr. Delfini, Finocchiaro G. (a cura di), *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*, Torino, 2017; Finocchiaro G., *Una prima lettura del reg. UE n. 910/2014 (c.d. EIDAS): identificazione* on line*, firme elettroniche e servizi fiduciari*, in *NLCC*, 2015, 419.

ropea, per favorire il commercio elettronico all'interno dell'Unione, aumentandone i caratteri di sicurezza. A tal fine, detto regolamento dispone che ogni Stato membro possa notificare alla Commissione il sistema identificativo prescelto, che, una volta accettato e pubblicato sulla *Gazzetta Ufficiale dell'UE*, deve poi essere riconosciuto da tutti gli altri Stati membri[49].
L'interesse del Regolamento *e-IDAS*, sotto il profilo qui analizzato, è duplice ed è, innanzitutto, dato dal fatto che, trattandosi di mezzi che trasmet-

[49] In sintesi ciascuno Stato membro notifica alla Commissione il regime di identificazione elettronica che vuole che sia riconosciuto dagli altri Stati membri (c.d. "regime notificato"), ai fini della c.d. "interoperabilità transfrontaliera" (art. 9, reg. *e-IDAS*). In c.d. *regime notificato* che soddisfi alcune condizioni e specifici requisiti tecnici (art. 7 del reg. e-IDAS), assicurando determinati "livelli di garanzia" - individuati nell'art. 8, reg. *e-IDAS* - deve quindi essere riconosciuto da tutti gli altri Stati membri (di cui il riferimento alla c.d. *interoperabilità*), di modo che tutti i soggetti - persone fisiche, giuridiche ed enti - che utilizzano quel *regime notificato* potranno porre in essere, nel mondo digitale, atti giuridici rilevanti e, per esempio, accedere a un servizio prestato *on-line* da una pubblica amministrazione di uno Stato membro, essendo validamente identificabili su tutto il territorio dell'Unione. Il Regolamento di esecuzione (UE) 2015/1502 della Commissione, emanato in data 8 settembre 2015 definisce e identifica le specifiche e le procedure tecniche minime relative ai livelli di garanzia dei mezzi di identificazione elettronica; precisa, infatti, G. Finocchiaro, *Una prima lettura del reg. UE n. 910/2014 (c.d. EIDAS): identificazione* on line*, firme elettroniche e servizi fiduciari*, in *Nuove leggi civ. comm.*, 2015, 419 ss., spec. 424, che «L'obbligo di riconoscere *on line* un soggetto identificato in un altro Stato sussiste soltanto se il livello di sicurezza è almeno pari o superiore a quello richiesto dall'ente pubblico per accedere a tale servizio on line e se è almeno "sostanziale o "elevato" Il reg. cit. è reperibile in *http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/il-regolamento-ue-ndeg-9102014-eidas/atti-esecutivi-eidas.* Si noti che non è infatti obbligatorio che lo Stato notifichi alla Commissione tutti i sistemi di identificazione utilizzati, essendo libero di selezionarne solo alcuni - o eventualmente anche nessuno - ove non sia interessato al riconoscimento da parte degli altri Stati membri, cfr. *Considerando* 13: «*È opportuno che gli Stati membri non abbiano l'obbligo di notificare i loro regimi di identificazione elettronica alla Commissione. Spetta agli Stati membri decidere se notificare alla Commissione tutti, alcuni o nessuno dei regimi di identificazione elettronica utilizzati a livello nazionale per l'accesso almeno ai servizi pubblici online o a servizi specifici*». Sul regolamento e-IDAS v. per tutti: Delfini, Finocchiaro (a cura di), *Identificazione elettronica e servizi fiduciari perle transazioni elettroniche nel mercato interno. Commento al Regolamento 910/214,* Torino, 2017.

tono e ricevono dati personali, devono trovare applicazione le norme in materia di protezione dei dati personali, dunque, anche il Regolamento UE 2016/679. L'altro elemento di rilievo è da ravvisare nell'obbligo che grava su ciascuno Stato membro di informare gli altri Stati membri e la Commissione su qualsiasi violazione o parziale compromissione del *regime notificato* (art. 10, reg. *e-IDAS*). In caso di *security breach*, infatti, lo Stato membro deve *senza indugio* sospendere o revocare il regime di comunicazione (c.d. *regime notificato*), che potrà essere ripristinato solo una volta posto rimedio alla violazione[50].

Si evidenzia quindi, ancora una volta, come il sempre maggior flusso di dati personali, anche (o soprattutto) a livello transfrontaliero, abbia posto con urgenza la necessità di regolare anche la pubblicità di eventuali violazioni, non solo nel rapporto con l'interessato, ma anche - sotto una prospettiva, pur non del tutto sovrapponibile - tra Stati membri, a conferma del fatto che l'obbligo di notifica delle violazioni ha ormai assurto al rango di previsione a carattere generale.

4. Il titolare quale soggetto passivo dell'obbligo di notifica e i soggetti che lo coadiuvano

Come precedentemente evidenziato, gli artt. 33 e 34 del GDPR pongono l'obbligo di notifica e comunicazione a carico del titolare del trattamento. E' dunque il titolare che deve valutare la gravità della violazione, l'impatto della stessa sulla sicurezza dei dati, spettando al medesimo anche la decisione finale circa l'obbligatorietà o meno della comunicazione

[50] In argomento: Del Giacco, *sub* art. 10, *Violazione della sicurezza*, in Delfini, Finocchiaro G. (a cura di), *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*, cit., 129 ss. Il regime notificato che non venga ripristinato entro tre mesi dalla sospensione o revoca dello stesso viene definitivamente ritirato. Nella comunicazione di cui al testo è opportuno che lo Stato fornisca alla Commissione e all'*Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione* (ENISA), tra l'altro, le informazioni riassuntive relative all'attività del proprio organismo di vigilanza, che, per l'Italia, è da individuare nell'*Agenzia per l'Italia Digitale* (AgID), con lo scopo di « agevolare lo scambio di buone prassi fra organismi di vigilanza e consentirebbe di verificare l'applicazione coerente ed efficiente dei requisiti essenziali di vigilanza in tutti gli Stati membri», cfr. *Considerando* 39, 40 reg. *e-IDAS*.

dell'avvenuta violazione all'autorità e/o all'interessato, in considerazione dei criteri di *probabilità* (art. 33) e del grado di *rischio* (art. 34) che siano posti in pericolo i diritti e la libertà della persona.
L'imputare al titolare la responsabilità della decisione finale se procedere o meno alla notifica della violazione è d'altronde coerente con il fatto che è il solo titolare che determina le finalità e le modalità del trattamento, compreso l'aspetto relativo alle misure di sicurezza (salvo il riferimento al responsabile del trattamento, di cui all'art. 32).
Il titolare, ad ogni modo, nella attività di trattamento, può essere coadiuvato da due altri soggetti, che devono avere specifiche competenze in materia di tutela dei dati personali: il *responsabile del trattamento* (art. 28 GDPR) ed il *responsabile della protezione dei dati personali* (artt. 37 ss. GDPR).
Si tratta di due figure con compiti e responsabilità differenti, nonostante la nomenclatura sia lessicalmente forse troppo similare per evitare errate sovrapposizioni[51].
Il primo non costituisce invero una completa novità, essendo una figura in parte assimilabile a quella dell'*incaricato* di cui all'art. 2, lett. *d*) della direttiva madre, trasposta nel *Codice privacy* italiano, all'art. 4 lett. *g*) – qui nuovamente definito *responsabile* - e qui inquadrato quale soggetto "preposto" dal titolare al trattamento dei dati personali; questi, secondo il GDPR,

[51] E indirettamente anche a quella dell'art 4 lett. g) *cod. privacy*. Ed infatti anche la Relazione della Autorità Garante per la Protezione dei Dati Personali relativa all'anno 2015, rileva che la figura del DPO è "definit[a] nella traduzione italiana in maniera un po' infelice, *Responsabile della protezione dei dati",* cfr. il testo della relazione: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/ docweb/5204513. In dottrina sul punto: termini generali cfr. Bassini, *La svolta della "privacy" europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quaderni costituzionali*, 2016, 587; Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 206; Stanzione M.G., *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e dir. priv.*, 2016, 1249ss.; *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, a cura di Bolognini, Pelino, Bistolfi, Milano, 2016. Ben diversa è invece la figura del *responsabile* definito nella dir. 95/46 cit., art. 2 lett *e*), riconducibile sostanzialmente a quella del *titolare* del Codice *privacy,* cfr. sul punto anche nel testo.

è il soggetto, persona fisica o giuridica, che tratta i dati personali per conto del titolare, attenendosi alle istruzioni da questo impartite[52].

La figura del *responsabile della protezione dei dati* (di seguito DPO, acronimo di *Data Protection Officer,* artt. 37 ss.)[53] costituisce invece una delle

[52] In tal senso Greco L., *I ruoli: titolare e responsabile*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da G. Finocchiaro, cit., 251 ss., spec. 261 ss. Ai sensi dell'art. 28, co. 3 del GDPR, "*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri*", Il contenuto essenziale di tale contratto è individuato nei successivi punti della norma cit. Si noti che nel *Codice privacy* italiano è prevista anche un'altra figura, quella dell'*incaricato*, che opera "sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite" (art. 30 del Codice); al riguardo il Garante "*Pur non prevedendo espressamente la figura dell' "incaricato" del trattamento (ex art. 30 Codice), il regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*" (si veda, in particolare, art. 4, n. 10, del regolamento)", così in http://www.garanteprivacy.it/regolamentoue/titolare-responsabile-incaricato-del-trattamento.

[53] La figura era invero già nota e obbligatoria in alcuni Stati membri (per esempio, in Germania ed Austria, è invece facoltativa in Francia), ma non in Italia. Per un'analisi a più ampio raggio cfr. Finocchiaro G., Privacy *e protezione del dati personali*, cit., 89 e già la relazione al Parlamento per l'anno 2005 dell'Autorità Garante per la Protezione dei Dati personali in http://garanteprivacy.it/web/guest/docweb/-/docweb-display/docweb/303712; Avitabile, *Data protection officer*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da G. Finocchiaro, cit., 333; ; rileva Greco L., *I ruoli: titolare e responsabile*, cit., 283 che "è possibile individuare un profilo di continuità" tra il DPO e l'incaricato della protezione dei dati di cui all'art. 19, co. 2 della direttiva 95/46/CE. Il DPO deve obbligatoriamente essere nominato se il trattamento è effettuato da un organismo pubblico a carattere non giurisdizionale (art. 37, lett. *a*) o da un ente, anche privato, che proceda al "*monitoraggio regolare e sistematico degli interessati su larga scala*" ovvero la cui attività principale consista nel trattamento "*su larga scala" di particolari categorie di dati* (art. 37, lett. *b* e *c*). Sulla scarsa determinatezza del concetto di "larga scala", cfr. Avitabile, *Data protection officer*, cit., 331 ss., e le il parere del *Gruppo ex art. 29*, Adottato il 13 dicembre 2016. Versione emendata e adottata in data 5 aprile 2017, contenente le *Linee guida sui responsabili della protezione dei dati*, reperibile in http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083. Con riguardo alle "particolari categorie di dati", i l riferimento è ai dati di cui all'art. 9 del Regolamento UE 2016/679, quindi – tra l'altro – i dati genetici e biometrici e, in generale, i dati che

più rilevanti novità introdotte dal Regolamento UE 2016/679, rispetto alla direttiva 95/46. Si deve trattare di un professionista dotato di una conoscenza specialistica coerente con il tipo di trattamento di dati effettuato dal titolare (art. 37, co. 5), il quale – oltre che dover offrire consulenza al titolare, al responsabile del trattamento e ai dipendenti, e doversi occupare di formazione del personale – è inoltre preposto alla vigilanza sulla conformità delle *policy* aziendali rispetto alla normativa posta dal Regolamento, figura professionale alla quale deve quindi essere assicurata la possibilità di agire in modo indipendente, per garantirne l'autonomia di giudizio[54].

---

rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale o l'orientamento sessuale. Cfr. anche il *considerando* 97, ove si precisa che per le attività pubbliche a carattere non giurisdizionale e quelle private che richiedono il "monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie […] il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento". Si noti che la figura del DPO era comunque già prevista e disciplinata nel Regolamento n. 45/2001, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari (art. 24). Sui casi di nomina obbligatoria del DPO è intervenuto il Gruppo art. 29, con il parere *Linee guida sui Responsabili della Protezione dei Dati (RPD)*, adottato il 13 dicembre 2016, emendato il 5 aprile 2017 - WP 243 - reperibile in http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083; in argomento: Avitabile, *Data protection officer*, cit., 335.

[54] Rileva Avitabile, *Data protection officer*, cit., 353, che si tratta di una figura manageriale, con funzioni di consulenza e controllo, assimilabile, per taluni aspetti alle funzioni svolte da un organismo di vigilanza ai sensi del d.lgs. n. 231/2001. Anche in considerazione del riferimento alla "conoscenza specifica della materia", si è in prima istanza portati a ritenere che il DPO debba essere una persona fisica, pur potendo svolgere il proprio ruolo sia quale dipendente del titolare o del responsabile – pur nell'ambito dell'autonomia raccomandata dall'art. 36 Reg. 2016/679, cfr. meglio nel testo – sia quale soggetto esterno all'organizzazione del titolare o del responsabile, nell'ambito del *contratto di servizi* cui fa cenno l'art. 37, co. 6 Reg. cit.; tuttavia alcuni rilevano che, in considerazione della complessità e varietà delle attribuzioni del DPO, sia preferibile, nonostante il dato letterale, non concentrare l'attività in capo ad un unico soggetto. Cfr. Pelino, *I soggetti del trattamento*, in *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, a cura di Bolognini, Pelino, Bistolfi, Milano, 2016, 163 ss., spec. 167.

Il DPO gode quindi di un profilo di autonomia maggiore rispetto al responsabile del trattamento, non potendo ricevere alcuna istruzione nell'esecuzione dei propri compiti né da quest'ultimo, né dal titolare (art. 37, co. 3 GDPR).

La figura del DPO, pur "di nuovo conio", compare anche nell'art. 32 della direttiva 2016/680/EU[55], relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità a fini di prevenzione, indagine, accertamento e perseguimento di reati. In tale normativa, invero, non si fa espresso cenno ad alcuna autonomia rispetto al titolare o al responsabile del trattamento – come invece indicato nel GDPR art. 38, co. 3 – tuttavia la consimilarità con la posizione del DPO, come disegnato nel GDPR, può ricavarsi della previsione di cui all'art. 34, lett. *b*) della direttiva cit., ove si precisa che il responsabile della protezione dei dati è tenuto, tra l'altro a "*sorvegliare l'osservanza della presente direttiva […], nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali*".

Il DPO funge, inoltre, da punto di contatto[56] con l'autorità di controllo per questioni connesse al trattamento; ciò significa che egli deve collaborare con

[55] Ruolo definito esattamente come nel GDPR, vale a dire *Data protection officer* nella versione inglese e *Responsabile della protezione dei dati* nella versione italiana della dir. 2016/680/EU, art. 32. Si noti che invero il DPO è contemplato anche nel Reg. 45/200, concernente la tutela delle persone fisiche in relazione ai dati personali da parte delle istituzioni e degli organismi comunitari, il cui art. 24 dispone che ciascuna istituzione comunitaria deve nominare almeno un Responsabile della protezione dei dati, il quale, tra l'altro deve "*garantire in maniera indipendente che le disposizioni del presente regolamento vengano applicate all'interno dell'istituzione o organismo di cui fa parte*" (art. 24, lett. c), senza che questi possa ricevere alcuna istruzione per quanto riguarda l'esercizio delle sue funzioni (art. 24, co. 7).

[56] Sia nel GDPR (art. 39, lett. *e*) sia nella dir. 2016/680/EU (art. 34, lett. *e*). La figura del c.d. *punto di contatto* è oggi ricorrente in molte normative europee, con lo scopo di individuare *ex ante* un referente, con idonee competenze, che possa dare una risposta immediata all'Autorità sulla tipologia e consistenza di un imminente pericolo ovvero un primo intervento in caso di violazione dei dati, della rete informativa ecc. cfr. per es. anche dir. 2008/114/CE relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, art. 6. Lo sviluppo, la sicurezza e la qualità della vita nei Paesi industrializzati dipendono dal funzionamento continuo e coordinato di un insieme di infrastrutture sempre più

il garante sia nell'ambito della consultazione preventiva prevista dall'art. 36 GDPR, sia per qualsiasi altra questione possa dirsi rilevante ai fini del trattamento[57] e, in particolare, in caso di *data breach,* posto che i dati di contatto del DPO devono essere obbligatoriamente comunicati all'Autorità e

---

connesse alla rete, le quali in ragione della loro rilevanza strategica sono definite – appunto – "critiche" Si tratta, invia generale, di aziende pubbliche o private il danneggiamento delle quali finirebbe per comportare un significativo impatto sulla popolazione che usufruisce del servizio offerto dalle medesime, impatto da valutarsi in termini di conseguenze sulla fiducia dei cittadini, perdita di servizi essenziali e rilevanza delle conseguenze economiche (per es. deterioramento dei prodotti o servizi, conseguenze ambientali ecc.), senza tuttavia potersi escludere nemmeno un certo numero di potenziali vittime[56]. In tale ambito rientrano quindi, per esempio, le aziende che operano nelle reti di trasporto (aereo, navale, ferroviario e stradale), di comunicazione, i fornitori di energia elettrica e gas, ma anche il sistema sanitario, i circuiti finanziari e, in generale, le reti a supporto del governo, quali quelle per la gestione delle emergenze (si pensi, in Italia, al sistema di Protezione civile). Tali infrastrutture sono oggi diventate sempre più complesse ed interdipendenti, migliorando, da un lato la qualità dei servizi erogati e permettendone il contenimento dei costi, sotto altro profilo, tuttavia, ciò ha esposto dette infrastrutture a nuove vulnerabilità; pur non esistendo, ad oggi, un quadro completo si annoverano infatti ormai diversi casi in cui il danno materiale alla infrastruttura appare direttamente riconducibile ad una azione che ha avuto corso attraverso la rete. Per esempio: Agosto 1998 – Località non rivelata – Settore idrico Un malfunzionamento software ha causato lo spegnimento del sistema di clorinazione di un acquedotto, rendendo l'acqua non potabile (circa 40000 utenti coinvolti); Giugno 1999 – Bellingham, Washington State – Oleodotto Un incidente all'infrastruttura di una condotta è stato aggravato dal fallimento dei sistemi di controllo SCADA); Agosto 2003 – Costa Orientale – Settore elettrico Durante il grande blackout un difetto di un sistema SCADA per la gestione dell'energia ha contribuito ad aggravare le conseguenze dell'incidente; Agosto 2003 – Jacksonville, Florida – Settore ferroviario Il virus "Sobig" ha causato lo spegnimento del sistema di segnalamento ferroviario in molti stati della costa orientale; Dicembre 2005 – Lesterville, Missouri – Settore idroelettrico Un bacino artificiale è tracimato a causa della routine software che controllava le operazioni di ripompaggio notturna. Il software non ha spento le pompe quando il bacino si è riempito, causando il problema; Ottobre 2006 – Harrisburg, Pennsylvania – Settore idrico Un cracker ha penetrato i sistemi IT di un impianto di filtraggio dell'acqua ed è riuscito a installare almeno un software malevolo (malware), con la capacità di influenzare le operazioni e i parametri di funzionamento dell'impianto; Marzo 2008 – Baxley, Georgia – Centrale nucleare Un update scorretto del software (riguardante sembra un solo computer) ha causato lo spegnimento di emergenza della centrale per 48 ore; http://www.isaca.org/chapters5/venice/benefits/documents/isaca_venice_quaderni_05_infra_critiche.pdf.

[57] Sul punto cfr. Avitabile, *Data protection officer*, cit., 363 ss.

all'interessato (art. 33, lett. *b* e art. 34 co. 2, GDPR), nei casi nei quali il titolare possa ritenersi obbligato a notificare la violazione (cfr. § 2).
La previsione appare coerente con uno dei compiti generali affidati al DPO, vale a dire il costituire il riferimento degli interessati "*per tutte le questioni relative al trattamento […] e all'esercizio dei loro diritti*" (art. 38, co. 4 GDPR).
Da quanto su esposto emerge dunque come sia il responsabile del trattamento sia il DPO non solo interagiscano continuamente con il titolare, ma abbiano anche precisi compiti, che il GDPR riserva loro direttamente, i più rilevanti dei quali, per i profili che qui interessano, sono in ambito di misure di sicurezza (art. 32) e di valutazione preventiva di impatto (art. 35), in quanto, in tali casi, la loro attività ben può riflettersi sulla gestione dell'eventuale *data breach* e, se non vi sono dubbi sul fatto che l'opportunità di procedere alle comunicazioni di cui agli artt. 33 e 34 GDPR costituisca una valutazione cui può procedere e di cui risponde il solo titolare, non sempre altrettanto chiaro è il confine delle responsabilità di ciascuno dei tre soggetti indicati (titolare, responsabile del trattamento, responsabile della protezione dei dati[58]).

5. Quali responsabilità per quali soggetti?

Alla luce di quanto esposto nei procedenti paragrafi, è emerso come i soggetti che attivamente partecipano al trattamento dei dati personali siano oggi almeno tre – titolare, responsabile del trattamento, responsabile della protezione dei dati – e come non sia semplice riuscire a distinguere le varie sfere di responsabilità. Occorre dunque di seguito indagare chi sia chiamato a rispondere in caso di *data breach* e verso quali soggetti.
Il rischio di violazioni dei dati è infatti ovviamente ineliminabile, pur essendo il GDPR teso proprio ad indurre specificamente alla predisposizione

[58] Senza contare il c.d. *incaricato* di cui all'art. 4, lett. *h*) del Cod. privacy italiano, sul quale v. Finocchiaro G., Privacy *e protezione dei dati personali*, Bologna, 2012, 100. Tale figura è stata spesso oggetto di critiche, anche in considerazione della non sempre facile distinzione, in concreto, con la figura del responsabile del trattamento, cfr. in argomento Pizzetti, *Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 206.

di misure tecniche ed organizzative che, secondo una valutazione *ex ante*[59], siano idonee a ridurre il più possibile il pericolo che si verifichino *danni materiali o immateriali*[60], in particolare nei casi nei quali il trattamento possa comportare discriminazioni, furti di identità, pregiudizi alla reputazione, alla riservatezza, anche dei dati protetti da segreto professionale ovvero anche perdite finanziarie[61].

Nell'attuale regolamento l'analisi preventiva dei profili di rischio (*risk assessment*) si inserisce dunque nel più ampio ambito della gestione del processo di trattamento dei dati, che, rispetto alla direttiva madre, risulta incentrata non più solo sull'individuazione dei parametri di legittimità di trattamento, ma anche sul principio della *accountability*[62], vale a dire la responsabilizzazione del titolare del trattamento, tenuto a garantire il rispetto dei principi di cui all'art. 5, tra i quali, per quanto qui rileva, quello della idoneità delle misure di sicurezza, sotto il profilo sia tecnico che organizza-

---

[59] In tal senso si esprimono anche le *Linee guida* del Gruppo Ex art. 29 in materia di notifica del *data breach,* adottate il 3 ottobre 2017 – WP 250 – cit. ed in tal senso depone il principio di *accountability*, cfr. sul punto: Finocchiaro G., *Introduzione al regolamento europeo sulla protezione dei dati*, cit., 10ss.

[60] Si esprimono in termini di danni *materiali o immateriali* i considerando nn. 75 e 85, così facendo da immediato referente a quanto previsto dall'art. 82, si rileva in dottrina che ciò corrisponde alla nozione italiana danno *patrimonial*e e *non patrimoniale*, cfr. Ratti, *La responsabilità da illecito trattamento dei dati personali nel nuovo regolamento*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da G. Finocchiaro, Bologna, 2017, 616; *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, a cura di Bolognini, Pelino, Bistolfi, cit., 596.

[61] Esplicativo in tal senso il considerando n. 75; in argomento Mantelero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati, valutazione d'impatto e consultazione preventiva (artt. 32-39),* in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da G. Finocchiaro, Bologna, 2017, 287 ss., il quale rileva come il concetto di rischio sia insito e all'origine della *data protection* e come la digitalizzazione delle informazioni abbia portato al fenomeno della *datification*, che ha fatto emergere una nuova forma di potere, qualificabile come *informativo*, basato sulla logica del controllo.

[62] Rileva Mantelero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati, valutazione d'impatto e consultazione preventiva (artt. 32-39),* cit., 301 ss., che ciò avviene al di fuori dell'ambito giuridico; ma, in considerazione dell'acuta attenzione della *data protection* ai profili procedimentali può dirsi oggi che questo avvenga anche in ambito eminentemente giuridico.

tivo (art. 5, lett. *f,* GDPR), il che comporta anche il conseguente onere di riuscire ad offrire la duplice prova della messa in atto e della idoneità delle medesime[63]. Tale idoneità – elemento pregnante della c.d. *risck assessment* – deve essere valutata alla luce della probabilità che si verifichi la violazione e della gravità degli effetti che eventualmente ne derivino per i diritti e le libertà dell'interessato, con riguardo alla natura, al contesto e alle finalità del trattamento (cfr. considerando n. 76).

Significativo è in argomento il considerando n. 74 per il quale "*è opportuno stabilire la* responsabilità generale *del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato*"[64]. Detta *responsabilità generale* del titolare del trattamento trova conferma nell'art. 82, co. 2 del Regolamento, per il quale questi risponde per tutti i danni cagionati da un trattamento posto in essere in violazione del Regolamento medesimo, mentre il responsabile del trattamento è chiamato a rispondere dei danni cagionati solo se non ha adempiuto agli obblighi specificamente a questi indirizzati ovvero nel caso in cui egli abbia agito difformemente rispetto alle istruzioni impartite dal titolare. Si noti che, in siffatte ipotesi, si configura per il responsabile del trattamento una responsabilità diretta; il danneggiato in tal caso può perciò rivolgere direttamente a

[63] Al riguardo il considerando n. 77 precisa che "Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati. Il comitato può inoltre pubblicare linee guida sui trattamenti che si ritiene improbabile possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e indicare quali misure possono essere sufficienti in tali casi per far fronte a tale rischio"; in argomento cfr. Pizzetti, *Dalla direttiva 95/46 al nuovo Regolamento europeo*, cit., 279 ss.

[64] Il considerando n. 74 precisa infatti ulteriormente che "In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche".

quest'ultimo la propria domanda risarcitoria, non trovando qui dunque applicazione il tipico schema della preposizione di cui all'art. 2049 c.c., per il quale il titolare è tenuto a rispondere in prima istanza, salvo il successivo regresso.

Non è tuttavia chiaro il titolo di responsabilità a cui sono chiamati il titolare e il responsabile. Il terzo comma dell'art. 82 cit. precisa che questi sono esonerati ove l'evento dannoso non sia loro "*in alcun modo imputabile*"; tale formulazione si presta invero a plurime interpretazioni[65].

In primo luogo può sostenersi che con essa si voglia far riferimento esclusivamente al nesso di causalità, di modo che, ove questo non sussista e dunque l'evento non sia causalmente riconducibile a quella specifica condotta, l'agente non possa essere chiamato a rispondere di alcunchè. Ne deriverebbe il configurarsi di una responsabilità oggettiva in capo alle figure suddette, che, per gli interpreti italiani, non costituirebbe una novità, in considerazione del rinvio effettuato dall'art. 15 del Cod. privacy all'art. 2050 c.c.

Ma, come anticipato, la formulazione dell'art. 82, co. 3 GDPR, riferendosi al concetto di *imputabilità*, potrebbe ricondursi anche alla regola generale della responsabilità colposa, più precisamente al requisito (o meglio all'assenza del medesimo) della diligenza qualificata, trattandosi di soggetti che svolgono professionalmente l'attività di trattamento.

La scelta per l'una o l'altra opzione comporta, come evidente, conseguenze concrete di non poco momento; nel primo caso, infatti, la responsabilità del titolare e del responsabile sarebbe più stringente, dovendo il danneggiato limitarsi a provare il fatto, il danno e il nesso di causalità, mentre i due potenziali danneggianti sarebbero chiamati alla prova del caso fortuito o di aver adottato tutte le misure idonee, in considerazione dello stato della tecnica, previsione, quest'ultima, che appare più coerente della prima rispetto

[65] Ratti, *La responsabilità da illecito trattamento dei dati personali nel nuovo regolamento*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da G. Finocchiaro, Bologna, 2017, 616; *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, a cura di Bolognini, Pelino, Bistolfi, cit., 596.

a quanto oggi posto dall'art. 32 GDPR ed al già richiamato principio di *accontability*[66].

Ove, invece, si optasse per il regime soggettivo della responsabilità, l'onere della prova diverrebbe evidentemente ben più gravoso per il danneggiato. Oltre alla già citata significativa coerenza sistematica della prima delle soluzioni prospettate, non appare in questa sede il caso di azzardare possibili soluzioni elettive, in considerazione del fatto che a breve il legislatore sarà chiamato ad intervenire specificamente sul punto[67].

Occorre tuttavia soffermarsi anche sulla figura del DPO e sulla possibile concorrenza delle responsabilità di quest'ultimo con quelle del titolare e del responsabile del trattamento, rispetto ai quali il primo gode di una sfera di autonomia che il legislatore europeo ha ritenuto opportuno enunciare espressamente ed inequivocabilmente (cfr. § precedente). In proposito si deve richiamare alla memoria, in primo luogo, il fatto che il regolamento delinea una responsabilità *generale* del titolare e del responsabile (art. 82), soggetti ai quali è dunque affidata la *compliance* delle scelte organizzative e tecniche aziendali rispetto al Regolamento[68]; ciò tuttavia non può escludere *a priori* che anche per il DPO si profilino ipotesi di responsabilità e ciò anche in considerazione delle competenze tecniche che devono caratterizzare la figura, in ragione del ruolo svolto.

Come meglio evidenziato nel precedente paragrafo, i compiti del DPO consistono nel fornire consulenza al titolare, al responsabile e ai dipendenti in merito agli obblighi derivanti dal Regolamento, assicurando l'osservanza dei precetti in esso contenuti e nel collaborare con l'Autorità di controllo (art. 39 GDPR). Inoltre, ove il trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche, in considerazione dell'uso di nuove tecnologie, della natura, dell'oggetto, del contesto e delle finalità

[66] Con riferimento all'art. 15 del *Cod. privacy*, rileva Finocchiaro G., Privacy *e protezione dei dati personali,* cit., 107 che, pur non rilevando i profili della colpa, in coerenza con la fattispecie del richiamato art. 2050 c.c., assumono "estremo rilievo le conoscenze tecniche del settore sulla base delle quali l'autorità giudiziaria, di volta in volta, valuterà se erano state adottate tutte le misure idonee ad evitare il danno".

[67] Cfr. nt. 6.

[68] Sul punto cfr. Avitabile, *Data protection officer*, cit. 361.

del trattamento, egli, se richiesto, deve fornire un parere in merito alla valutazione d'impatto sulla protezione dei dati cui, ai sensi dell'art. 35, è tenuto il titolare del trattamento. Emerge dunque come il DPO sia certamente in grado di influire sulle scelte finali del titolare, il quale dovrà tenere in debito conto i pareri espressi da un soggetto così tecnicamente qualificato; ciò che tuttavia ha rilievo decisivo è che nessuna decisione finale, nella sua dimensione operativa concreta, risulta affidata al DPO. Se ne può dunque inferire che questi non possa essere chiamato a concorrere con il titolare o con il responsabile del trattamento, nemmeno a livello concorsuale, non potendosi invece certamente escludere quella responsabilità che connota in via residuale l'attività di tutti i soggetti che prestano attività lavorativa da individuarsi nel dolo o nella negligenza professionale. A differenza di quanto previsto in capo al responsabile, tuttavia, anche in questi casi, deve ritenersi che per il DPO non possa configurarsi alcuna responsabilità diretta nei confronti del danneggiato.

Dall'analisi sin qui condotta emerge quindi, in conclusione, come il GDPR abbia arricchito il novero dei soggetti attivi del trattamento, allargando anche la sfera delle rispettive responsabilità, ma piuttosto che concentrarsi sull'ottica riparatoria, *ex post*, abbia privilegiato una logica di prevenzione, coinvolgendo tutti i soggetti su individuati, pur con funzioni e attività diversificate, nella messa in atto di misure (quali, per esempio, protocolli operativi, codici di condotta, misure tecniche quali la pseudonimizzazione) che *ex ante* siano in grado di ridurre al minimo la probabilità di *data breach;* mentre la gestione successiva della violazione dei dati è largamente affidata al principio di autoresponsabilità, per cui si attribuisce allo stesso titolare la valutazione delle possibili conseguenze di tale violazione in capo agli interessati e, quindi, la decisione se procedere o meno alla comunicazione di tale violazione (notificazione e comunicazione al Garante e all'interessato), secondo una impostazione forse più libera di quanto ci si potrebbe aspettare ove ci si avvicinasse al GDPR con una prospettiva di osservazione più tradizionale, portata generalmente a concentrarsi sulle conseguenze dell'evento dannoso, piuttosto che sulle attività utili ad evitarle.

Diritto Mercato Tecnologia

Numeri Speciali

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

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