Privacy, tutela del consumatore e *risk based approach*

Salvatore Sica - Virgilio D'Antonio - Giorgio Giannone Codiglione - Giovanni Sciancalepore

Sommario: 1. Il trattamento dei dati personali come attività rischiosa. Profili introduttivi. – 2. Le regole sul trattamento nella nuova disciplina comunitaria. – 3. Sicurezza del trattamento. – 4. Valutazione d'impatto e consultazione preventiva. – 5. *Risk-based approach* e principio di *accountability*. – 6. Tutela dei dati personali e valutazione del rischio tra prevenzione degli «incidenti» e promozione della libertà d'impresa.

1. Una delle principali direttrici seguite dal legislatore comunitario nell'elaborazione della nuova disciplina uniforme sulla protezione dei dati personali introdotta con Regolamento n. 679 del 2016, è rappresentata dalla necessità di vagliare i rischi sottesi allo svolgimento delle attività di trattamento dei dati personali[1].

Invero, già a partire dai primi anni ottanta dello scorso secolo (su tutti, la raccomandazione OCSE del 1980 e la Convenzione di Strasburgo del 1981[2]),

[1] Tale tendenza è emersa in maniera più organica durante la discussione della proposta di Regolamento della Commissione del 25 gennaio 2012, COM (2012) 11 final, in seno al Parlamento europeo e al Consiglio, cui sono seguite l'integrazione e l'armonizzazione delle disposizioni sulla valutazione d'impatto della protezione dei dati e sulla figura del c.d. *privacy officer* (artt. 33 e 35 della proposta di Regolamento). Sul punto si v. Commissione europea, *Salvaguardare la privacy in un mondo interconnesso Un quadro europeo della protezione dei dati per il XXI secolo*, COM (2012) 9 final del 25 gennaio 2012, p. 7; Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, WP 218 del 30 maggio 2014. Sul travagliato iter normativo che ha condotto all'emanazione del nuovo Regolamento generale sulla protezione dei dati personali v. *supra*, M.G. Stanzione, *Genesi ed ambito di applicazione del regolamento*.

[2] OCSE, *Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*, C(80)58(Final) dell'1 ottobre 1980, spec. artt. 3, lett. b) (Scope of Guidelines) e 11 (Security Safeguards Principle); Consiglio d'Europa, *Convention for the protection of individuals with regard to automatic processing of personal data*, Strasburgo, 28 gennaio 1981, spec. artt. 7 (Data Security) e 9, n. 3 (Exceptions and restrictions). Per un'analisi di questi fondamentali assestamenti normativi v. M.G. Losano, *Il diritto pubblico dell'informatica*, Torino, 1986, pp. 25 e ss.

 ISSN 2704-8179

sino a giungere alla direttiva 95/46/CE[3], è emersa la chiara tendenza di investire i soggetti esercenti attività di sfruttamento dei dati di una serie di obblighi, diretti ed indiretti, per maggior parte volti a promuovere l'adozione di modelli imprenditoriali ed organizzativi incentrati sulla riduzione delle ipotesi di trattamento non conforme.

Basti a tal uopo ricordare le norme generali sul trattamento dei dati personali e quelle sugli obblighi e gli standard di sicurezza introdotti dalla direttiva 95/46 (artt. 6 e 17), queste ultime recepite dal legislatore italiano in uno schema bipartito[4].

Il quadro viene completato da una regola generale di imputazione dei danni da illecito trattamento a carattere semi-oggettivo[5], cui si accosta, in via cumulativa o sostitutiva, un regime di misure volte a sanzionare l'inadempimento degli obblighi di sicurezza sanciti dagli artt. 33 e 31, d.lgs. 196/2003[6].

[3] Si veda ad es. il considerando n. 46, dir. 95/46/CE, per cui «(…) la tutela dei diritti e delle libertà delle persone interessate relativamente al trattamento di dati personali richiede l'adozione di adeguate misure tecniche ed organizzative sia al momento della progettazione che a quello dell'esecuzione del trattamento, in particolare per garantirne la sicurezza ed impedire in tal modo qualsiasi trattamento non autorizzato; che spetta agli Stati membri accertarsi che il responsabile del trattamento osservi tali misure; che queste devono assicurare un adeguato livello di sicurezza, tenuto conto delle conoscenze tecniche e dei costi dell'esecuzione rispetto ai rischi che i trattamenti presentano e alla natura dei dati da proteggere». Cfr. anche i considerando nn. 53 e 54, dir. 95/46/CE.

[4] Che distingue tra *i*) misure minime, a loro volta poi implementate a seconda che il trattamento sia effettuato con o senza l'ausilio di strumenti elettronici (artt. 33-35); *ii*) misure idonee o preventive (art. 31), cui si aggiungono le disposizioni sugli obblighi di sicurezza relative ai fornitori di servizi di comunicazione elettronica accessibili al pubblico e i relativi obblighi di notifica, introdotti dalla direttiva 2009/136/CE (artt. 32 e 32-*bis*): sul punto, si vedano gli artt. 17 e 20, dir. 95/46/CE e l'art. 4, dir. 2002/58/CE. Per un commento, in dottrina v. G.M. Riccio, *Sub artt. 33 – 36*, in S. Sica - P. Stanzione (dir. da), *La nuova disciplina della privacy*, Bologna, 2004; P. Troiano, *Sub artt. 31-36*, in C.M. Bianca – F.D. Busnelli (a cura di), *La protezione dei dati personali*, Padova, 2007, pp. 684-731.

[5] Cfr. artt. 23, dir. 95/46/CE, recepito dall'art. 15, n. 1, d.lgs. 196/2003. Per un'organica riflessione sul regime di responsabilità civile adottato in materia di illecito trattamento dei dati personali si v. per tutti S. Sica, *Le tutele civili*, in F. Cardarelli – S. Sica – V. Zeno-Zencovich (a cura di), *Il codice dei dati personali*, Milano, 2004, p. 553 e ss.; Id., *Sub artt. 18 e 29, comma 9*, in E. Giannantonio – M.G Losano – V. Zeno Zencovich, *La tutela di dati personali.Commentario alla L. 675/96*, Padova, 1999; A. Maietta, *Sub art. 15*, in S. Sica - P. Stanzione, *La nuova disciplina della privacy*, cit.; G. Comandè, *Sub art. 15*, in C.M. Bianca – F.D. Busnelli, *La protezione dei dati personali*, cit., pp. 362 e ss.

[6] Seguendo uno schema di condotta a formazione progressiva, l'omissione delle misure di cui all'art. 33 comporta la somministrazione delle sanzioni penali di cui all'art. 169, d.lgs. cit., a causa della maggiore esposizione al rischio connessa al mancato preventivo adeguamento alle misure

 ISSN 2037-5662

In tal senso, il trattamento dei dati personali è stato *ab origine* inteso dall'ordinamento come un'attività rischiosa – ovvero un'attività di tipo organizzato che, per sua intrinseca natura, è foriera di cagionare pregiudizi maggiori rispetto a quelli scaturenti dalla c.d. attività biologica[7] – cui si ricollega la necessità di approntare regole volte in pari misura a tutelare gli interessi dei consociati sia su un piano preventivo/deterrente che successivo/riparatorio.

Il modello comunitario di tutela dei dati personali quale autonoma evoluzione del diritto alla riservatezza, si realizza attraverso la rigida imposizione di obblighi nei confronti dei soggetti che vogliono (o si trovano ad) entrare in contatto con specifiche tipologie di informazioni (titolare/responsabile del trattamento) e, dall'altra parte, riconosce una libertà positiva di controllo ed intervento (diritto all'autodeterminazione informativa o *recht auf Infor-*

minime di sicurezza da parte del titolare; l'adozione di misure "idonee e preventive" andrebbe invece letta nel contesto dei poteri sanzionatori o conformativi esercitati dall'Autorità garante di cui all'art. 154 o, comunque collegata all'adempimento del più ampio obbligo di porre in essere "tutte le misure idonee a evitare il danno" di cui al combinato disposto tra l'art. 15, d.lgs. cit. e l'ivi richiamato art. 2050 cod. civ. In questo senso, la sanzione civile risarcitoria, estesa nel dettato italiano a "chiunque" cagioni ad altro un pregiudizio per effetto del trattamento, andrebbe intesa come una norma di chiusura. Sul punto cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Atti previsti dal regolamento disciplinante le misure minime di sicurezza*, 29 maggio 2000, doc. web n. 40205. Per una ricostruzione in chiave graduata del sistema sanzionatorio sotteso all'applicazione delle regole di cui agli artt. 15, 31 e 33 d.lgs. 196/2003 v. A. MANTELERO, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, 2007, spec. pp. 183 e ss. e anche A. CASTALDO, *Sub artt. 167 – 172*, in S. SICA - P. STANZIONE, *La nuova disciplina della privacy*, cit.; G. CASSANO, *Diritto dell'Internet*, Milano, 2005, pp. 18 e ss.; D. LIANTONIO, *La legge sulla privacy e la sicurezza dei dati*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, pp. 751 e ss.; P. PERRI, *Sicurezza giuridica e sicurezza informatica*, in M. DURANTE – U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, 2012, spec. p. 347 s.

[7] Sull'evoluzione della nozione di attività rischiosa nel generale contesto della c.d. società industrializzata v. P. TRIMARCHI, *Rischio e responsabilità oggettiva*, Milano, 1961, spec. pp. 43 e ss.; S. RODOTÀ, *Il problema della responsabilità civile*, Milano, 1964, spec. pp. 175 e ss.; M. COMPORTI, *Esposizione al pericolo e responsabilità civile*, Napoli, 1965; ID., *Artt. 2049-2053*, in F.D. BUSNELLI (dir. da) *Il codice civile. Commentario*, Milano, 2009; P.G. MONATERI, *La responsabilità civile*, in *Tratt. dir. civ. Sacco*, Torino, 1998, pp. 1011 e ss.; M. FRANZONI, *L'Illecito*, Milano, 2010, pp. 400 e ss.; G. ALPA, *La responsabilità civile. Parte generale*, Torino, 2010, pp. 293 e ss.; G. ALESII, *Introduzione alla valutazione delle attività rischiose*, Torino, 1997 e ancora, con particolare attenzione alla permeazione del paradigma tecnologico nella sfera dell'umano in termini di opportunità e rischio V. FROSINI, *Cibernetica diritto e società*, Milano, 1968, spec. p. 124 s. S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, p. 89 s.

 ISSN 2037-5662

mationelle selbstbestimmung[8]) in favore del soggetto cui l'informazione è riferita (interessato)[9].

A ciò deve aggiungersi che il diritto alla protezione dei dati personali, in astratto equiparato agli altri diritti fondamentali riconosciuti dall'ordinamento comunitario, è stato in più occasioni collocato in una posizione gerarchica di preminenza, soprattutto rispetto ad interessi economici quali la libertà d'impresa e la proprietà intellettuale[10].

Tale marcata propensione giudiziale al rafforzamento della tutela degli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, è stata

[8] Sulla genesi del diritto all'autodeterminazione informativa, coniato dalla giurisprudenza costituzionale tedesca più di trent'anni or sono con la celebre *Volkszählungsurteil* BVferG, 15 dicembre 1983 - 1 BvR 209/83, in *NVwZ,* 1984, 167) e poi recepito dall'ordinamento tedesco con la riforma del 1990 del BDSG v. G. Sartor, *Tutela della personalità e normativa per la «protezione dei dati»*, in *Inf. e dir*., 1986, pp. 95-118 e, più recentemente ed in una prospettiva comparatistica F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict And Cooperation*, in 78 *Law & Contemp. Probs*. 231 (2015).

[9] In una letteratura a dir poco sconfinata si rimanda a S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, pp. 19 e ss.; Id., voce *Riservatezza*, in *Enc. trecc*., VII app., Roma, 2007.

[10] Si vedano ad esempio CGE Grande sez., 13 maggio 2014, causa C-131/12, *Google Spain, Google Inc. c. AEPD, Costeja González*, in questa *Rivista*, 4/5, 2014, pp. 535 – 562, ora anche in G. Resta – V. Zeno-Zencovich, *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015, disp. all'URL http://ojs.romatrepress.uniroma3.it/index.php/oblio/, con commenti di T.E. Frosini, O. Pollicino, G. Finocchiaro, G. Caggiano, P. Piroddi, G. Sartor – M. Viola De Azevedo Cunha, A. Mantelero, S. Sica – V. D'antonio, C. Comella, G.M. Riccio, R. Flor, F. Pizzetti e ancora in *Foro it*., 2014, IV, 295, n. A. Palmieri – R. Pardolesi e volendo in *Nuova giur. civ. comm*., 11, 2014, pp. 1054 – 1072, n. G. Giannone Codiglione, par. 97, in cui si afferma che gli artt. 7 e 8 della Carta «prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona (…)»; CGE, sent. 29 gennaio 2008, caso C-275/06, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, in *Dir. inf*., 2008, pp. 182 e ss., par. 70, per cui «(…) le direttive 2000/31, 2001/29, 2004/48 e 2002/58 non impongono agli Stati membri (…) di istituire un obbligo di comunicare dati personali per garantire l'effettiva tutela del diritto d'autore nel contesto di un procedimento civile. Tuttavia, il diritto comunitario richiede che i detti Stati, in occasione della trasposizione di queste direttive, abbiano cura di fondarsi su un'interpretazione delle medesime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario. Poi, in sede di attuazione delle misure di trasposizione delle dette direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme a tali direttive, ma anche evitare di fondarsi su un'interpretazione di esse che entri in conflitto con i detti diritti fondamentali o con gli altri principi generali del diritto comunitario, come il principio di proporzionalità». Per una riflessione sistematica sulla portata di tali assestamenti giurisprudenziali si rimanda a S. Rodotà, *Solidarietà*, Bari-Roma, 2014, p. 92 s.

 ISSN 2037-5662

recepita dal legislatore comunitario attraverso la rilettura e l'estensione dei principi-cardine su cui poggia la direttiva del 1995, al contempo integrandone la struttura con disposizioni tecnico-programmatiche volte a non incidere oltremodo sulle aspettative e gli interessi dei prestatori di servizi della società dell'informazione, nell'ottica del perseguimento degli obiettivi di progresso economico e sociale[11].

2. Sotto un profilo oggettivo, il nuovo Regolamento generale abbraccia una più articolata nozione di trattamento dei dati personali: alla descrizione base fornita dall'art. 4, n. 2), sostanzialmente identica all'art. 2, lett. b), dir. 95/46[12], si accostano i riferimenti alla c.d. profilazione [art. 4, n. 4)] e ai c.d. trattamenti transfrontalieri [art. 4, n. 24)[13]].

Seguendo una prospettiva maggiormente sensibile alle più moderne strategie di sfruttamento economico dei dati personali nell'ambito delle comunicazioni elettroniche, la profilazione viene definita come autonoma tipologia di trattamento automatizzato di dati personali, attuata allo scopo di analizzare o valutare ai fini predittivi un particolare aspetto relativo a una persona fisica quali il rendimento professionale, la situazione economica, la salute, le

[11] Si veda a tal proposito il considerando n. 2 del Regolamento, il quale rimarca come la tutela dei dati personali debba essere intesa anche come strumento per il perseguimento del rafforzamento e della convergenza delle economie del mercato interno, nonché del benessere delle persone fisiche. In argomento si leggano anche i considerando n. 4, 6, 7 e 13, i quali a loro volta affermano come il diritto alla protezione dei dati personali non sia intangibile e debba essere contemperato con altri diritti fondamentali, garantendo in pari misura la libera circolazione dei dati personali ed il controllo degli stessi da parte degli interessati. In generale sul tema della regolazione del rischio in relazione alla tutela dei dati personali si vedano i contributi di A. Antikainen, *Risk-Based Approach as a Solution to Secondary Use of Personal Data*, Helsinki, 2014; R. Gellert, *Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative*, in 5 *International Data Privacy Law* 3 (2015); D. Kloza - N van Dijk – P. De Hert, *Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologies*, in F. Skopik – P. Smith, *Smart Grid Security*, Amsterdam, 2015, pp. 37 e ss.

[12] Rispetto alla precedente versione normativa, l'art. 4 del Regolamento introduce, in via meramente esemplificativa (e in un caso sostitutiva) le attività di strutturazione, adattamento e limitazione dei dati personali.

[13] Su tale ultimo profilo, oggetto di un importante assestamento della Corte di giustizia e di un serrato dibattito politico, si rimanda all'organica esposizione effettuata *infra* da D. Pittella, *Trasferimento verso paesi terzi*, nonché a CGE Grande sez., 6 ottobre 2015, causa C-362/14, *Maximillian Schrems* c. *Data Protection Commissioner*, in *Dir. inf*., 475, 2015, pp.603-635, con commenti di V. Zeno-Zencovich, G. Resta, C. Comella, O. Pollicino – M. Bassini, G. Finocchiaro, S. Sica – V. D'antonio, P. Piroddi, G.M. Riccio, A. Mantelero, G. Giannone Codiglione.

 ISSN 2037-5662

preferenze, gli interessi, l'affidabilità, il comportamento o gli spostamenti[14]. Il Regolamento prevede alcune regole generali applicabili ad ogni forma di trattamento[15], implementate e/o specificamente declinate con riguardo alla particolare tipologia dei dati (ad es. i c.d. dati sensibili) o, ancora, a particolari sotto-categorie di trattamento (per l'appunto, il c.d. *profiling* e il trasferimento transnazionale di dati personali).

Le nuove regole uniformi, inoltre, si applicano ai soli trattamenti riconducibili, direttamente o indirettamente, all'esercizio di un'attività commerciale o professionale, restando escluse le attività di sfruttamento di tipo domestico[16].

Secondo i principi generali di cui all'art. 5, i dati personali devono essere: *a*) trattati in modo lecito, corretto e trasparente; *b*) raccolti per finalità determinate, esplicite e legittime e trattati in maniera compatibile con queste ultime; *c*) adeguati ed esatti; *d*) conservati in modo tale da rendere identificabile l'interessato solo per il lasso di tempo necessario ai fini del perseguimento delle finalità, eccetto nelle ipotesi di conservazione per interesse pubblico, scientifico, storico o statistico; *e*) trattati in maniera sicura. Compete al titolare del trattamento l'osservanza di tali prescrizioni e, conseguentemente, risulta essere indicato come il soggetto in grado di darne prova (principio di responsabilizzazione o *accountability*).

[14] Già l'art. 14, d.lgs. 196/2003 contempla una nozione «base» di profilazione in relazione alla validità di quegli atti e provvedimenti giudiziario o amministrativo aventi per oggetto la valutazione del comportamento umano che fossero basati «su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato», riconoscendo altresì all'interessato il diritto di opporsi ad ogni tipo di valutazione fondata su tale tipologia di trattamento. Per un approfondimento v. *infra* P. Pacileo, *Profilazione e diritto di opposizione*, ma anche A. Maietta, *Sub art. 14*, in S. Sica - P. Stanzione, *La nuova disciplina della privacy*, cit.; A. Mantelero, *Attività di impresa in Internet e tutela della persona*, Padova, 2004, pp. 146 e ss. ; I.S. Rubinstein - R.D. Lee - P.M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, in 75 *U. Chi. L. Rev*. 261 (2008).

[15] Si veda ad es., con riguardo alla profilazione, il considerando n. 72.

[16] Cfr. il considerando n. 18, per cui andrebbero escluse dalla portata di applicazione del Regolamento attività quali la corrispondenza, gli indirizzari, o l'uso dei social network fatta salva l'applicazione «(…) ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico». Il Regolamento non si applica altresì ai dati riguardanti le persone decedute (considerando n. 27), alle questioni attinenti la sicurezza nazionale e la politica estera, nonché 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, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica, materie queste disciplinate dalla direttiva 2016/680/UE.

 ISSN 2037-5662

La liceità del trattamento può discendere, oltre che *a1*) dall'integrità e validità del consenso prestato dall'interessato[17], anche da altri fattori, quali: *a2*) il collegamento tra attività di sfruttamento ed esecuzione di un contratto in cui una delle parti coincide con l'interessato; *a3*) l'adempimento di un obbligo legale da parte del titolare o il perseguimento di un legittimo interesse del titolare o di un terzo, a patto che esso non prevalga sulle prerogative dell'interessato; *a4*) l'esecuzione di un compito di interesse pubblico o, ancora (in maniera parzialmente difforme da quanto affermato dall'art. 7, lett. d), dir. 95/46) la salvaguardia degli interessi vitali dell'interessato o dei consociati[18].

In maniera analoga rispetto all'art. 8, dir. 95/46, l'art. 9 del Regolamento impone un divieto generale di trattamento senza l'esplicito consenso dell'interessato per quanto attiene i c.d. dati sensibili, ovvero quelle informazioni che disvelano un particolare ed intimo aspetto della persona interessata o della propria vita. La regola è poi temperata da un insieme di eccezioni[19].

[17] Il Regolamento prende atto delle molteplici modalità di raccolta del consenso in ambito telematico, confermando la centralità dell'istituto quale strumento di garanzia di un'informazione trasparente e consapevole dell'interessato, propedeutica alla successiva manifestazione di volontà. Sul punto si veda quanto affermato dal considerando n. 32, per cui «il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. (...)». Per un approfondimento di tali profili evolutivi, specialmente in relazione al ruolo dei minori, v. *infra* G. Spoto, *Disciplina del consenso e tutela del minore*.

[18] La direttiva faceva infatti riferimento alla salvaguardia degli interessi vitali del solo interessato.

[19] L'art. 9 vieta il trattamento di categorie particolari di dati personali, ampliando poi il novero di eccezioni tassativamente previste (da 5 della direttiva 95/46 a 10). Tale ipotesi, in sintesi, riguardano: a) il consenso esplicito dell'interessato, fatta salva la revoca; b) il trattamento necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale; c) il trattamento necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali; f) il trattamento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria; g) il trattamento per motivi di interesse pubblico rilevante; h)

 ISSN 2037-5662

Norme specifiche sono ancora dettate in materia di dati giudiziari e nell'ambito i quei trattamenti che per le proprie finalità non richiedono l'identificazione dell'interessato (artt. 10 e 11, reg. cit.)[20].

Come è noto, i principi di correttezza e trasparenza trovano compiuta espressione nel rapporto sussistente tra il consenso dell'interessato e l'obbligo d'informazione posto in capo al titolare, avente come oggetto in primo luogo le finalità del trattamento[21].

In questo comparto, il nuovo Regolamento si concentra maggiormente sull'evoluzione dei servizi offerti nell'ambito del c.d. web 2.0, prendendo in considerazione il problema del trattamento svolto per finalità diverse da quelle per cui i dati sono stati raccolti (c.d. trattamento secondario).

In tali ipotesi, nell'assenza di consenso dell'interessato o di altro atto legislativo che sancisca la liceità dell'attività, il titolare è tenuto a valutare se il trattamento sia astrattamente conforme ai principi di necessità e proporzionalità di cui all'art. 23 del Regolamento[22], con particolare riguardo agli scopi perseguiti dal trattamento principale.

trattamento necessario per finalità di medicina preventiva o di medicina del lavoro; i) trattamento necessario per motivi di interesse pubblico nel settore della sanità pubblica; j) trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

[20] Secondo l'art. 10 del Regolamento, «il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica». Quanto al trattamento che non richiede l'identificazione (art. 11), il Regolamento prevede che il titolare non debba più conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato, previa informativa dell'interessato. In tali casi, gli articoli da 15 a 20 non saranno applicati tranne nel caso in cui l'interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisce ulteriori informazioni che ne consentano l'identificazione.

[21] Sul punto v. il considerando n. 39, per cui «(…) Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. (…)». Sull'applicazione dei principi di trasparenza ed informazione si vedano altresì i considerando nn. 60-64.

[22] L'art. 23 (e il considerando n. 73) dispone infatti che il diritto dell'Unione o degli Stati membri può imporre limitazioni a specifici principi e ai diritti di informazione, accesso, rettifica e cancellazione di dati, al diritto alla portabilità dei dati, al diritto di opporsi, alle decisioni basate sulla profilazione, nonché alla comunicazione di una violazione di dati personali all'interessato e ad alcuni obblighi connessi in capo ai titolari del trattamento, ove ciò sia necessario e proporzionato in

 ISSN 2037-5662

Come specificato dall'art. 6, n. 4, tale vaglio preventivo di compatibilità dovrà, in via meramente esemplificativa, tenere in considerazione ogni possibile nesso sussistente tra le diverse finalità, il contesto in cui i dati personali sono stati raccolti, la loro natura, le possibili conseguenze dell'ulteriore trattamento e l'esistenza di garanzie adeguate volte a minimizzare i rischi ad esso sottesi, quali la cifratura o la pseudonimizzazione[23].

Tale disposizione deve essere poi letta unitamente alla nuova nozione di dato personale apprestata dal Regolamento, la cui portata è estesa non solo a «qualsiasi informazione concernente una persona fisica identificata o identificabile» (art. 2, lett. a, dir. 95/46[24]), ma all'insieme delle informazioni relative ad una persona fisica, avendo riguardo per gli identificativi prodotti da dispositivi on line (Indirizzo IP, cookies, ecc.) o di quei dati che, nonostante la pseudonimizzazione, possano essere oggetto di combinazione con ulteriori informazioni in modo da rendere possibile, direttamente o indirettamente, l'identificazione dell'interessato[25].

Leggendo l'art. 4, n. 1), si può osservare come vengano coperte per via normativa tutte le forme di trattamento multiplo di dati che conducono, anche astrattamente, all'identificazione di una persona fisica, con l'esclusione

una società democratica per salvaguardare la sicurezza nazionale e pubblica; la difesa; la prevenzione e il perseguimento di reati o l'esecuzione di sanzioni penali; altri importanti obiettivi di interesse pubblico; la salvaguardia dell'indipendenza della magistratura; la prevenzione della violazione della deontologia professionale; la tutela dell'interessato; l'esecuzione delle azioni civili.

23 Si veda anche il considerando n. 50, per cui «il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali. (…)».

24 La direttiva 95/46 fa riferimento ad una qualità intrinseca della singola informazione (numero identificativo, caratteristiche specifiche dell'identità personale), tralasciando ad esempio l'attività di combinazione e sovrapposizione tra una o più informazioni.

25 Secondo il parere dell'Article 29 Data Protection Working Party, *Parere 05/2014 sulle tecniche di anonimizzazione*, WP216, 10 aprile 2014, p. 21, la pseudonimizzazione consiste nel sostituire un attributo (solitamente un attributo univoco) di un dato con un altro. L'art. 4, 5) del Regolamento aggiunge come essa consista nel «(…) trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile». Il Gruppo di lavoro sottolinea altresì (p. 11) che i dati pseudonimi andrebbero ritenuti protetti dalla normativa sulla protezione della privacy, come confermato dallo stesso considerando n. 26 del Regolamento.

 ISSN 2037-5662

dei dati anonimi (ovvero le informazioni che non si riferiscono a una persona fisica identificata o identificabile) e dei dati personali trattati in maniera tale da impedire o da non consentire l'identificazione dell'interessato[26].

Quanto alla durata del trattamento e alla relativa conservazione dei dati da parte del titolare (principi di adeguatezza e limitazione del trattamento), il Regolamento specifica come essa debba essere limitata al tempo necessario al perseguimento delle finalità del trattamento, anche previa fissazione di un termine per la definitiva eliminazione delle informazioni o, ancora, per effettuare una verifica periodica e l'eventuale rettifica[27].

Il problema della moltiplicazione delle attività di trattamento dei dati personali è stato pertanto affrontato in maniera maggiormente dinamica attraverso un tentativo di ricostruzione delle singole tipologie e riconduzione entro obiettivi diversificati di tutela.

Come si è avuto modo di verificare, tale scopo protettivo è perseguito non solo attraverso l'imposizione di precisi obblighi in capo al titolare: già dal combinato disposto degli artt. 4 e 7 del Regolamento, appare difatti chiara l'intenzione del legislatore di incentivare modelli imprenditoriali volti a limitare dall'origine l'uso di dati che siano riferiti o riferibili, anche attraverso una loro combinazione, ad una persona fisica.

[26] Si cfr. i considerando nn. 26 e 30. In questo ambito di interesse appare ancora di interesse il parere emesso dall'Article 29 Data Protection Working Party, *Parere 05/2014 sulle tecniche di anonimizzazione*, WP216, 10 aprile 2014, p. 10 e ss., che in relazione alle procedure di anonimizzazione discerne tra randomizzazione e generalizzazione dei dati: nel primo caso si tratta di tecniche che modificano la veridicità dei dati al fine di eliminare la forte correlazione che esiste tra i dati e la persona; la generalizzazione, invece diluisce gli attributi delle persone interessate modificando la rispettiva scala o ordine di grandezza. In argomento si rimanda ancora a I. Walden, *Anonymising Personal Data*, in 10 *Int'l J.L. & Info. Tech*. 224 (2002); G. Finocchiaro, voce *Anonimato*, in *Dig. disc. priv*., sez. civ., agg. V, Torino, 2010, pp. 12 e ss.

[27] Si veda, a tal proposito ancora il considerando n. 39, per cui «(…) I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento».

 ISSN 2037-5662

3. Lasciando ad altra sede l'approfondimento delle regole sulla c.d. *data security*[28] con particolare riguardo alle ipotesi di violazione degli obblighi imposti dal legislatore, pare opportuno verificare se il modello «minimo» di prevenzione del rischio adottato dall'art. 17, dir. 95/46 abbia subìto sostanziali modifiche.

La seconda sezione del Regolamento è dedicata alla sicurezza dei dati personali: l'art. 32 obbliga sia il titolare che il responsabile del trattamento ad attuare «misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio», tenendo in considerazione lo stato dell'arte e i costi di attuazione, nonché la natura, l'oggetto, il contesto e le finalità del trattamento «come anche il rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche».

I rischi connessi alle istanze di adeguatezza delle misure di sicurezza da adottare nell'esecuzione del trattamento sono in particolare rappresentati dalla distruzione, perdita, modifica, divulgazione o accesso non autorizzati ai dati personali trattati, conservati o trasmessi (art. 32, n. 2)[29].

Rispetto all'art. 17, dir. 95/46, il Regolamento consolida la regola di «appropriatezza del livello di sicurezza rispetto ai rischi presentati dal trattamento»: l'art. 32, n. 1 indica un modello di condotta ed organizzazione adeguato a garantire gli obiettivi di sicurezza, basato sulla «spersonalizzazione»

[28] Si veda S. Vigliar, *Privacy e comunicazioni elettroniche: la direttiva 2002/52/CE*, in *Dir. inf.*, 2003, pp. 401 e ss.; S. Sica, *Sicurezza e riservatezza nelle telecomunicazioni: il d.lgs. n. 171/98 nel «sistema» della protezione dei dati personali*, ivi, 1998, p. 775 ss.

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

 ISSN 2037-5662

dei dati attraverso procedure di pseudonimizzazione e cifratura e, ancora, sulla garanzia di riservatezza, integrità, disponibilità e resilienza dei servizi di trattamento, sulla loro capacità di ripristino a seguito di incidente fisico o tecnico e infine sull'attuazione periodica di procedure di testing, verifica e valutazione dell'efficacia complessiva delle misure[30].

L'intervento tecnico-organizzativo, commisurato alla tipologia del trattamento, ai rischi ad esso sottesi, allo stato di evoluzione tecnologica nonché ai costi di attuazione che esso implica[31], è strutturato in modo tale da garantire la sicurezza dei dati in maniera uniforme nei diversi stadi di permanenza nella disponibilità del prestatore.

La disposizione si chiude con un incentivo all'adozione di codici di condotta o meccanismi di certificazione approvati, intesi come elementi validi per dimostrare l'adeguatezza delle misure. É infine previsto sul titolare e il responsabile un obbligo generale di rendere edotto sulle regole di sicurezza qualunque soggetto che, operando sotto la propria autorità, abbia accesso ai dati personali trattati[32].

4. Le previsioni di cui agli artt. 6, n. 4 e 32 n. 2 rappresentano due declinazioni del generale principio di trattamento dei dati personali in maniera non rischiosa, aventi rispettivamente come oggetto le attività di trattamento diverse da quelle previamente autorizzate e il modello tecnico ed organizzativo da adottare al fine di ottemperare agli standard di adeguata riservatezza e sicurezza dei sistemi di trattamento.

A queste regole si accosta poi l'innovativa disciplina sulla valutazione dell'impatto e la consultazione preventiva, di cui alla terza sezione del Rego-

[30] Sul punto si v. Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks*, cit., p. 2 s.

[31] Il riferimento ai costi, già presente nell'art. 17 dir. 95/56, non è ad esempio contemplato dall'art. 17, d.lgs. 196/2003, per cui «i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta».

[32] Obbligo enunciato in maniera speculare dall'art. 29 del regolamento con riguardo a tutti coloro che operino sotto la responsabilità del responsabile o del titolare del trattamento avendo accesso ai dati personali.

 ISSN 2037-5662

lamento, che sostituisce l'obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali previsto dall'art. 18, dir. 95/46.

Ai sensi dell'art. 35, nel contesto di attività di sfruttamento che implicano l'uso di nuove tecnologie e che presentano rischi elevati per i diritti e le libertà delle persone fisiche, il titolare è tenuto ad effettuare una valutazione dell'impatto sortito da tali trattamenti sul generale assetto di protezione dei dati personali.

La valutazione d'impatto rappresenta dunque una tappa obbligatoria per tutte quelle forme di trattamento «molto rischiose»: tra queste attività, l'art. 35, n. 3 individua in via esemplificativa la sorveglianza su larga scala e, ancora il trattamento globale, automatizzato e sistematico di informazioni riguardanti aspetti personali volto ad incidere sulla capacità decisionale di detti soggetti e che produca effetti significativi sul piano giuridico o personale. I commi da 4 a 6 del medesimo articolo prevedono poi che sia l'autorità di controllo a fornire periodicamente un elenco aggiornato delle tipologie di trattamento soggette al requisito della valutazione preventiva o, in via alternativa, a specificare quali siano le attività non sottoposte a tale obbligo.

Il titolare del trattamento, coadiuvato dall'autonoma ed indipendente figura del responsabile della protezione dei dati (c.d. *privacy officer*)[33], procede all'analisi dei punti di criticità dell'attività di sfruttamento, redigendo un documento contenente la descrizione dei trattamenti e delle loro finalità rapportata ai principi di necessità e proporzionalità e ai rischi per i diritti e le libertà dell'interessato[34], nonché il dettaglio delle misure previste per contrastarne l'occorrenza sul piano della sicurezza, della protezione degli interessi dei soggetti coinvolti e della generale conformità alla normativa[35].

[33] Sul tema si rimanda alla disamina effettuata *supra*, da G.M. Riccio, Data controller *e nuove figure privacy*.

[34] Si vedano in particolare i considerando nn. 89-94 e, in particolare, il n. 90 per cui sarebbe opportuno «(…) che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento».

[35] Secondo l'art. 36, n. 3 del Regolamento il titolare del trattamento deve altresì comunicare all'autorità di controllo: a) 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; b) le finalità e i mezzi del trattamento previsto; c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente

 ISSN 2037-5662

Ove gli esiti della disamina conducano all'individuazione di un rischio elevato in assenza dell'adozione di misure idonee ad attenuarne gli effetti pregiudizievoli (art. 36 n. 1),i risultati della valutazione d'impatto sono posti al vaglio preventivo dell'autorità amministrativa di controllo. Quest'ultima, nel caso di trattamento illecito o non adeguatamente vagliato sul piano del rischio, ha l'onere di produrre entro otto settimane dalla ricezione della richiesta (prorogabile per altre sei previa informativa al titolare) un parere scritto, esercitando altresì i poteri investigativi, correttivi, autorizzativi e consultivi di cui all'art. 58[36]. Nell'analizzare i risultati della valutazione svolta dal titolare l'autorità tiene in particolare considerazione il rispetto dei codici di condotta (art. 36, n. 8).

Il sistema di valutazione dell'impatto e la richiesta di autorizzazione preventiva all'autorità nazionale di garanzia, imposto in via generale attraverso una selezione delle tipologie di trattamento effettuata dallo stesso Garante nazionale, trova una deroga nel caso in cui il legislatore abbia previsto un'autonoma base giuridica per quella particolare ipotesi di trattamento, come prescritto dall'art. 6, n. 2 per i trattamenti necessari ad adempiere un obbligo legale al quale è soggetto il titolare o per l'esecuzione di compiti di interesse pubblico. In tali circostanze, gli artt. 35 e 36 non si applicano se la valutazione d'impatto è stata già effettuata, salvo che gli Stati membri ne ritengano comunque necessario l'adempimento.

5. La portata precettiva e preventiva delle norme sin qui oggetto di analisi deve essere infine posta a confronto con il rinnovato sistema di regole attinenti il profilo della responsabilità[37].

Sul piano soggettivo, gli obblighi di trattamento conforme, lecito e sicuro rispetto ai rischi sono ripartiti in maniera più articolata e precisa ed arricchiti dalle norme contenute al capo IV del Regolamento.

Ai sensi dell'art. 24, il titolare del trattamento è obbligato ad attuare misure tecniche ed organizzative adeguate a garantire un trattamento conforme, nonché a darne prova in ossequio al principio di *accountability*, espres-

regolamento; d) ove applicabile, i dati di contatto del titolare della protezione dei dati; e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35; f) ogni altra informazione richiesta dall'autorità di controllo.

[36] Il Garante nazionale può infatti disporre Sui poteri delle autorità di controllo v. *infra* D. Mula, *One-stop-shop e ruolo delle Autorità Garanti.*

[37] Per un approfondimento v. *infra*, A.G. Parisi, *Responsabilità e sanzioni.*

 ISSN 2037-5662

samente richiamato dal già citato art. 5, n. 2, con riguardo all'osservanza dei principi generali sul trattamento[38].

Questa prescrizione è altresì rafforzata dalla norma relativa all'implementazione delle istanze di privacy *by design* (art. 25)[39], ovvero all'adozione di pratiche di trattamento volte ad attuare efficacemente i principi di protezione (quali la pseudonimizzazione e la minimizzazione) e, ancora a limitare in via preventiva e preimpostata il trattamento ai soli dati personali necessari per ogni specifica finalità.

Il principio di cooperazione con l'autorità di controllo di cui all'art. 31 è integrato dal precedente art. 30, obbligando il titolare del trattamento svolto in un'impresa o organizzazione con più di 250 dipendenti (o comunque nel caso di attività di tipo rischioso) a curare e tenere, anche in formato elettronico, un registro delle attività di trattamento, disponibile su richiesta della stessa autorità nazionale di controllo.

Il Regolamento prevede infine che gli obblighi posti in capo al titolare – e il relativo regime di imputabilità – possano venire temperati dalla previsione di figure intermedie quali quelle del c.d. contitolare del trattamento (art. 26), del rappresentante del titolare o del responsabile del trattamento non stabilito nell'Unione (art. 27) e infine del responsabile del trattamento (art. 28).

Quanto alle sanzioni civili, ai sensi dell'art. 82 del Regolamento, chiunque abbia subito un danno patrimoniale o non patrimoniale connesso alla violazione del Regolamento ha il diritto di ottenerne il risarcimento dal titolare o dal responsabile del trattamento. Anche in questo caso, la lettera della norma indica una chiara inversione di tendenza, con una maggiore propensione a mitigare il regime di responsabilità civile per illecito trattamento dei dati personali.

Tale strategia è attuata su tre diversi livelli: in primo luogo, a differenza della disciplina ad esempio vigente in Italia, i soggetti legittimati passivamen-

[38] Il considerando n. 74 specifica altresì come sia «opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. 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».

[39] Anche su questo argomento si rimanda agli approfondimenti svolti *infra* da R. D'Orazio, *Privacy* by default *e privacy* by design.

 ISSN 2037-5662

te sono il solo titolare ed il responsabile del trattamento e non «chiunque» abbia cagionato il danno[40].

Inoltre, rispetto all'art. 23, dir. 95/46, il Regolamento esonera il titolare e il responsabile ove essi abbiano dato prova che l'evento dannoso non è in alcun modo a loro imputabile, nel senso di avere effettuato il trattamento in conformità del dettato normativo o, nel caso del responsabile, nel rispetto dei compiti ad esso specificamente assegnati per via normativa o dal titolare[41]. In altre parole, la regola di condotta è ripartita tra le diverse figure e modulata rispetto all'adempimento dei precisi obblighi indicati dal Regolamento, temperando in astratto la *probatio diabolica* dell'estraneità della causa del danno alla propria sfera di rischio – nella disciplina italiana ad esempio intesa come mera prova del fortuito, della forza maggiore o di un elemento equivalente[42] – come è possibile desumere dalla lettura del combinato dispo-

[40] E in questo frangente in maniera chiara recita anche il già citato considerando n. 18.

[41] Cfr. il considerando n. 153: «Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile. Il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento. Ciò non pregiudica le azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri. Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito. Qualora i titolari del trattamento o i responsabili del trattamento siano coinvolti nello stesso trattamento, ogni titolare del trattamento o responsabile del trattamento dovrebbe rispondere per la totalità del danno. Tuttavia, qualora essi siano riuniti negli stessi procedimenti giudiziari conformemente al diritto degli Stati membri, il risarcimento può essere ripartito in base alla responsabilità che ricade su ogni titolare del trattamento o responsabile del trattamento per il danno cagionato dal trattamento, a condizione che sia assicurato il pieno ed effettivo risarcimento dell'interessato che ha subito il danno. Il titolare del trattamento o il responsabile del trattamento che ha pagato l'intero risarcimento del danno può successivamente proporre un'azione di regresso contro altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento».

[42] S. Sica, *Le tutele civili*, cit., p. 554. Nella giurisprudenza di legittimità italiana si v. da ultimo Cass. civ., sez. VI, 5 settembre 2014, n. 18812, *Com. Montecatini Terme c. Garante protezione dati personali*, in *Rep. Foro it*., 2014, Persona fisica [4940], n. 111, per cui «i danni cagionati per effetto del trattamento dei dati personali in base all'art. 15 d.leg. 30 giugno 2003 n. 196, sono assoggettati alla disciplina di cui all'art. 2050 c.c., con la conseguenza che il danneggiato è tenuto solo a provare il danno e il nesso di causalità con l'attività di trattamento dei dati, mentre spetta al convenuto la prova di aver adottato tutte le misure idonee ad evitare il danno».

 ISSN 2037-5662

sto di cui ai commi secondo e terzo dell'art. 82[43]. A consolidare il principio di corresponsabilità, l'art. 82, nn. 4 e 5, prevede che nel caso in cui vi siano uno o più titolari o responsabili implicati nel medesimo illecito trattamento, ogni soggetto è obbligato in solido a corrispondere l'intera somma dovuta a titolo di risarcimento, salva poi la possibilità di agire per ottenere il regresso sugli altri condebitori.

Quanto alle sanzioni pecuniarie aventi carattere amministrativo, l'art. 83 ne riconosce valenza suppletiva-punitiva, valutabile caso per caso in relazione alla sussistenza di particolari condizioni (quali il dolo o la colpa del titolare o del responsabile, l'adempimento degli obblighi di sicurezza e privacy *by design* di cui agli artt. 25 e 32 o la violazione reiterata o ripetuta nel tempo)[44]. Le sanzioni amministrative di tipo pecuniario possono altresì sostituire o integrare le misure conformativo/ingiuntive disposte dalle medesime autorità di controllo ai sensi dell'art. 58.

Infine, l'art. 84 in generale assegna alle altre sanzioni (tra cui quelle penali) un ruolo di chiusura del sistema di tutele, rimarcando la necessità che esse siano effettive, proporzionate e dissuasive.

[43] «(…) Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile. (…)»

[44] In particolare, l'art. 82 prevede che le sanzioni amministrative pecuniarie, aventi ammontare non superiore a dieci milioni di euro (o sino al 2% del fatturato mondiale per le imprese), siano inflitte, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure, avendo cura di valutare elementi quali: a) la natura, la gravità e la durata della violazione; 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; i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2; 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.

 ISSN 2037-5662

6. Come si è avuto modo di osservare, il nuovo Regolamento generale sulla protezione dei dati personali affronta in maniera articolata il tema della valutazione e della gestione del rischio, toccando profili di tutela preventiva e successiva, quali il trattamento dei dati, la sicurezza, gli obblighi di valutazione dell'impatto e consultazione dell'autorità di controllo, le regole di responsabilità.

Questo complesso eterogeneo di disposizioni può essere ricondotto entro uno schema di sintesi, rintracciando alcuni elementi di rilevanza.

La disciplina del trattamento dei dati personali pare divisa in due grandi blocchi, seppur tra di essi comunicanti: in primo luogo si rinvengono le attività di trattamento di «prima generazione», riferite ad un'accezione qualitativa di dato personale. Tali trattamenti, collegati ad una nozione «base» di rischio, vengono disciplinati, con qualche piccolo aggiustamento, in conformità alla previgente disciplina di cui alla direttiva 95/46/CE.

Dall'altra parte si staglia una differente tipologia di attività, collegata alla prima sotto il profilo della fonte di legittimazione e delle regole generali, ma riferibile ad una nozione di tipo quantitativo di dato personale e relativa ad attività di accumulo e combinazione secondaria dei dati previamente raccolti. In questo contesto, l'ordinamento ravvisa un livello di rischio per i diritti e le libertà dei consociati maggiormente elevato[45], cui si ricollega un potenziamento delle disposizioni in tema di trattamento e protezione(su tutti, si vedano gli artt. 6, 25 e 32 del Regolamento).

Alcuni tra i trattamenti di «seconda generazione», in questo caso individuati preventivamente per via amministrativa (o legislativa), sono altresì oggetto di un'autorizzazione preventiva da parte delle autorità di controllo, chiamate a valutare i documenti organizzativo-programmatici stilati dagli

[45] A questo proposito, il considerando n. 76 discerne tra attività «rischiose» e altre che presentino «rischi elevati»: «La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato». Il Regolamento pare altresì contemplare una nozione di attività a «basso rischio», rispetto a cui non si applica l'obbligo per il titolare ed il responsabile non stabilito nell'Unione di nominare un proprio rappresentante (v. art. 27, n. 2, lett. a), «(…) l'obbligo di cui al paragrafo 1 (…) non si applica a) al trattamento se (…) è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento; (…)».

 ISSN 2037-5662

stessi titolari dei trattamenti[46]. Sempre modulata rispetto alla valutazione del rischio, ma in un'ottica precauzionale di temperamento degli eventi pregiudizi discendenti da una fattispecie di violazione dei dati personali (c.d. *data breach*) è la disciplina della notifica e quella della comunicazione all'autorità nazionale di controllo e all'interessato. In tali ipotesi, il diverso grado di rischio (elevato o basso-improbabile) viene valutato a posteriori dal titolare, in ossequio al principio di responsabilizzazione di cui all'art. 5, n. 2, poichè appunto riferito ai potenziali (o attuali) effetti che la violazione sortisce sui diritti e le libertà della persona fisica[47].

La rilettura sistematica delle prescrizioni in commento evidenzia, in definitiva, l'emersione di una comune tendenza normativa: l'attività di impresa (o l'organizzazione) che implichi (o abbia come oggetto) il trattamento di dati personali viene sostanzialmente incentivata ad adottare procedure atte alla minimizzazione, se non ancora alla eliminazione del rischio, nel senso di rendere inapplicabili sin dall'inizio gli obblighi generali di protezione e trattamento conforme[48].

[46] V. il considerando n. 84, per cui «per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo».

[47] Si discute infatti di violazioni che comportano un basso o improbabile rischio di pregiudizio, non obbligando il titolare a notificare la violazione dei dati personali all'autorità di controllo «senza ingiustificato ritardo» e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza: v. art. 33, n. 1, per cui «(…) il titolare del trattamento notifica la violazione all'autorità di controllo competente (…) 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. (…)» e, ancora in violazioni ad «elevato rischio», rispetto alle quali il titolare è tenuto ad informare senza indebito ritardo l'interessato (v. art. 34, n. 1, «Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo»).

[48] Si legga a tal fine il considerando n. 78, per cui «la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe

 ISSN 2037-5662

L'informazione, ove non più collegabile all'identità di una persona fisica, viene così quasi del tutto sottratta alla disciplina generale sulla protezione dei dati[49].

Ancora in maniera più chiara, la rinnovata regola di responsabilità civile prende atto dei numerosi obblighi cui è sottoposto il prestatore, limitandosi a colpire il danno scaturente da mancato, non corretto o inadeguato ottemperamento delle dettagliate prescrizioni legislative, lasciando apparentemente fuori dalle ipotesi di risarcibilità *ex* art. 82 tutti i danni estranei, sotto un profilo soggettivo ed oggettivo, all'adempimento di tali misure[50].

Volendo adottare una prospettiva giuseconomica, il prestatore è così chiamato ad adeguarsi preventivamente allo standard di diligenza atteso e connesso alle dettagliate disposizioni in materia di trattamento o sicurezza (si pensi ancora alle istanze di privacy *by design*[51]): i maggiori costi di conformazione sostenuti, consistenti soprattutto in un adeguamento tecnico delle

adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici».

[49] Per una riflessione sugli scenari aperti da questa diversa declinazione della tutela dei dati personali sia consentito rinviare alla ricognizione effettuata *infra*, Internet of things *e nuovo Regolamento privacy*.

[50] Una critica alla disciplina previgente è ad esempio mossa da P.G. Monateri, *Illecito e responsabilità civile*, II, Torino, 2002, pp. 92 e ss.

[51] Sul punto, si v. quanto espressamente affermato dal considerando n. 29, per cui «al fine di creare incentivi per l'applicazione della pseudonimizzazione nel trattamento dei dati personali, dovrebbero essere possibili misure di pseudonimizzazione con possibilità di analisi generale all'interno dello stesso titolare del trattamento, qualora il titolare del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il trattamento interessato, l'attuazione del presente regolamento, e che le informazioni aggiuntive per l'attribuzione dei dati personali a un interessato specifico siano conservate separatamente. Il titolare del trattamento che effettua il trattamento dei dati personali dovrebbe indicare le persone autorizzate all'interno dello stesso titolare del trattamento».

 ISSN 2037-5662

procedure automatizzate di trattamento dei dati (nel senso dunque di un generale innalzamento dello standard minimo di condotta previsto per via normativa) sono connessi all'obiettivo di minimizzazione dei costi sociali degli incidenti attesi, da cui si deduce la marcata riduzione dei costi esterni ad esso imputabili in termini di responsabilità[52].

Nel bilanciamento tra interesse economico del prestatore di servizi della società dell'informazione e tutela dei diritti fondamentali dell'interessato, il nuovo Regolamento pare collocarsi in una posizione di incentivo alle attività di sfruttamento dei dati nel quadro delle istanze di sviluppo ed innovazione ad esse sottese.

Pur sempre valido ed effettivo nelle sue declamazioni, il blocco normativo consolidatosi nei vent'anni di vigenza della direttiva 95/46 e orientato a dare effettività al potere di controllo dell'interessato sulle proprie informazioni (potere questo quindi inteso nel senso di una libertà positiva)[53], pare difatti relegato in una posizione di subordine, scalzato dalla strategia di conformazione tecnica dell'attività organizzativa o di impresa e, sopratutto, di riaffermazione della privacy come libertà negativa, sottratta però alla signoria dell'interessato e declinata per via normativa come radicale ed automatica esclusione di ogni possibile forma di sfruttamento di informazioni che siano riconducibili ad una data persona fisica.

[52] In materia si veda la rilettura dell'istituto effettuata da P.G. Monateri, voce *Responsabilità civile*, in *Dig. disc. priv*., sez. civ., XVII, Torino, 1998 e ancora Aa.Vv., *Il mercato delle regole*, I, Bologna, 1999, pp. 204 e ss., G. Ponzanelli, La responsabilità civile. profili di diritto comparato, Bologna, 1992, spec. pp. 80 e ss., nonchè la basilare riflessione svolta da G. Calabresi, *Costo degli incidenti e responsabilità civile*, trad. it. a cura di A. De Vita - V. Varano – V. Vigoriti, Milano, 1975, spec. pp. 307 e ss. Ancora, per una prima riflessione sulla conformazione agli obblighi relativi alle misure di sicurezza si v. G. Buttarelli, *Banche dati e tutela della riservatezza*, Milano, 1997, p. 328, nota n. 364.

[53] Per tutti, si veda quanto rilevato da S. Rodotà, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy*, in *Eur. dir. priv*., 2004, pp. 2 e ss. e ancora Id., *Tecnologie e diritti*, cit., p. 122.

 ISSN 2037-5662