[2018] C.E.L.B.

THE
CARDOZO ELECTRONIC
LAW BULLETIN

GLOBAL FRONTIERS OF COMPARATIVE LAW

REGOLE DI RESPONSABILITÀ E SELF-ASSESSMENT: ANALISI COMPARATISTICA DEL COMPLESSO EQUILIBRIO TRA DIRITTO E TECNICA NEI MODELLI DI PREVENZIONE DEL DANNO

Salvatore Vigliar

[Essay published on March 2018]

THE CARDOZO INSTITUTE
ISSN 1128-322X

The Cardozo Law Bulletin is a peer-reviewed, English and Italian language journal concerned to provide an international forum for academic research exploring the thresholds of legal theory, judicial practice and public policy, where the use of a 'comparative law and literature' approach becomes crucial to the understanding of Law as a complex order.

The Cardozo Law Bulletin, established in 1995 as one of the world first Law Journals on the Web, invites the submission of essays, topical article, comments, critical reviews, which will be evaluated by an independent committee of referees on the basis of their quality of scholarship, originality, and contribution to reshaping legal views and perspectives.

SUBMISSIONS: The Cardozo Law Bulletin only accepts submissions made in accordance with the MLA (Modern Language Association) style, the most commonly used to write papers and cite sources within the liberal arts and humanities.

http://www.jus.unitn.it/cardozo/

CHIEF EDITOR: Pier Giuseppe Monateri

I CONTRIBUTI SONO SOTTOPOSTI A REFERAGGIO DOPPIO CIECO

ISSN 1128-322X

Regole di responsabilità e self-assessment: analisi comparatistica del complesso equilibrio tra diritto e tecnica nei modelli di prevenzione del danno

SALVATORE VIGLIAR

SOMMARIO: 1. Introduzione. – La valutazione di impatto nel settore ambientale: l'esperienza nordamericana dell'Envorinmental Impact Statement. – 3. Analisi dei rischi e danni ambientali nell'esperienza internazionale ed europea. – 4. Privacy Impact Assessment e modelli giuridici imitati. – 5. Prime esperienze nazionali ed evoluzione comunitaria. – 6. Privacy Impact Assessment nel Regolamento in materia di protezione dei dati personali. – 7. Valutazione di impatto e regole di responsabilità.

1. Introduzione

A due anni dalla sua emanazione, il 25 maggio 2018 il Regolamento europeo sulla protezione dati personali diventerà esecutivo.

Si tratta di un testo legislativo che segna una svolta epocale nel settore della privacy (rectius: della gestione e della protezione dei dati personali) e che attua un radicale ripensamento dei principi e dei cardini che avevano sinora modellato le scelte del legislatore comunitario. Tra i principi fondanti del nuovo testo normativo, merita una particolare attenzione, proprio perché esemplificativo della mutata impostazione legislativa, quello dell'autoresponsabilità e dell'autovalutazione da parte del titolare del trattamento, chiamato a giudicare la pericolosità e la rischiosità (ovvero l'attitudine a produrre danni[1]) delle sue operazioni di trattamento di dati personali[2].

Il principio di self-assessment non è però nuovo, né circoscritto al settore della privacy: anzi, come già affermato in dottrina[3], esso potrebbe potenzialmente estendersi a tutte le aree del diritto, rappresentando un modello nuovo di responsabilità o, quanto meno, un criterio per parametrare, da un lato, la pericolosità di una determinata azione (parlandosi, in tal caso di risk-assessment) e, dall'altro, per costituire un elemento ai fini della valutazione del danno risarcibile nei settori in cui vi si fa ricorso.

---

[1] Come sarà meglio illustrato nel prosieguo, sebbene la disciplina in materia di protezione dei dati personali preveda delle sanzioni amministrative, che possono essere comminate da Autorità amministrative di garanzia in caso di inadempienza relativa alle misure previste dal Regolamento generale, tuttavia, la mancata adozione di tali misure è anche fonte di responsabilità aquiliana (a condizione, ovviamente, che sia dimostrato un danno subito dal soggetto interessato). L'adozione di un modello fondato sull'esposizione al rischio, richiama, ovviamente, numerosi scritti "classici" in materia di illecito aquiliano, tra i quali meritano di essere ricordati almeno M. Comporti, *Esposizione al pericolo e responsabilità civile*, Napoli, rist. 2004 (orig. 1965); S. Rodotà, *Il problema della responsabilità civile*, Milano, 1965; P. Trimarchi, *Rischio e responsabilità oggettiva*, Milano, 1961; A. Tunc, *La responsabilité civile*, 2ème éd., Paris, 1989; nonché, nell'ambito della dottrina americana, v., per tutti, G. Calabresi, *Costo degli incidenti e responsabilità civile*, trad. it., pref. di S. Rodotà, Milano, 1975.

[2] Su tale impostazione, v. diffusamente F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 15 ss.

[3] S. Levemore, *Self-Assessed Valuation Systems for Tort and Other Law*, 68 *Virginia L. Rev.* 771 (1982): "*Theoretically, the applicability of self-assessment is almost endless*".

L'introduzione di tale principio, che sembra essere alla base dell'intero Regolamento comunitario, offre al civilista, soprattutto in chiave comparatistica, numerosi spunti di riflessione.

Il primo, inevitabilmente, muove dall'analisi dei modelli regolamentari precedenti, elaborati prevalentemente nell'area di common law, per mezzo del ricorso a strumenti di soft law. Si è discusso ampiamente di risk assessment, infatti, in numerose aree, quali, a titolo esemplificativo, il diritto ambientale e la responsabilità sanitaria.

Un secondo filone di indagine, che origina e scaturisce naturalmente dal primo, è associato, invece, alle influenze che, partendo dalle esperienze nazionali, hanno operato sul legislatore comunitario nella fase in cui ha elaborato una riforma radicale, come quella di cui si discute, della legislazione in materia di trattamento dei dati personali. Indubbiamente, una struttura complessa come quella del Regolamento, che si snoda per novantanove articoli e oltre cento Considerando, è il frutto di percorsi multiformi, difficilmente riconducibili ad un unico modello di imitazione.

Tuttavia, pur nella consapevolezza di tali limiti e di tali complessità di indagine, appare proficuo ripercorrere i principi generali che, a partire da quelli di precauzione e di prevenzione (che paiono essere utilizzati congiuntamente all'interno del Regolamento)[4], hanno modellato le soluzioni e le opzioni legislative.

Dal principio di precauzione[5], il Regolamento sembra aver tratto la consapevolezza dell'impossibilità di eliminare in nuce i rischi di data breach[6]: in

---

[4] Sulla differenza tra i due principi, si rinvia, per tutti, a M.G. Stanzione, *Principio di precauzione e diritto alla salute. Profili di diritto comparato*, in *Comparazione e dir. civ.*, 2: "*In quest'ultimo aspetto risiede la principale differenza con il principio di prevenzione, il quale si applica soltanto in presenza di rischi scientificamente accertati e dimostrabili, ovverosia in presenza di rischi noti, misurabili e controllabili. La precauzione, al contrario, interviene quando la scienza non è in grado di dare risposte certe su rischi inaccettabili per la collettività. Essa serve per gestire rischi potenziali ma non ancora individuati oppure non del tutto dimostrabili per insufficienza o inadeguatezza dei dati scientifici*".

[5] Per un inquadramento del principio di precauzione, v. F. De Leonardis, *Il principio di precauzione nell'amministrazione di rischio*, Milano, 2005; P. Jourdain, *Principe de précaution et responsabilité civile*, Parigi, 2000; E. Al Mureden, *Principio di precauzione, tutela della salute e responsabilità civile*, Bologna, 2008, *passim*.

[6] Sul tema, sia consentito il rinvio a S. Vigliar, *Data Breach e sicurezza informatica*, in S. Sica – V. D'Antonio – G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016, 241 ss.

altri termini, conformemente a quelli che sono i pilastri di tale principio, si attua un'anticipazione del momento della tutela, per mezzo della predisposizione di strumenti idonei a limitare tali rischi. Peraltro, e anche in tal caso si tratta di una soluzione che trova forti analogie in altri settori, non si dettano misure tipiche o tipizzate, ma si lascia all'operatore l'individuazione delle prassi organizzative o delle tecnologie più adeguate, seppur tenendo conto del costo sociale, gravante su soggetti pubblici e privati, di tali strumenti di tutela.

Allo stesso modo, risulta evidente l'impossibilità di una determinazione ex ante dei danni, sul piano sia privatistico sia pubblicistico, associati ad una violazione dei dati personali (si pensi, banalmente, ad un furto di dati), laddove i tradizionali strumenti civilistici sembrano mal adattarsi alla moltiplicabilità potenziale dell'illecito, per mezzo della riproducibilità di interi archivi di dati, e alla difficoltà, sul piano concreto, di arginare la circolazione di tali dati e di consentire al titolare del trattamento o ai soggetti interessati di riacquisire un dominio reale sui dati stessi[7].

Dalla lettura del testo del Regolamento si ricava altresì che l'adozione di un principio di prevenzione/precauzione non incide direttamente sulle norme in materia di responsabilità aquiliana che, di fatto, restano sostanzialmente invariate, almeno per quanto riguarda le alternative di fondo, che sono indirizzate verso l'applicazione di un criterio di imputazione di carattere oggettivo. Al contrario, il risk-based approach, che rappresenta il fil rouge della lettura del testo, convive con le regole di responsabilità, influenzandone potenzialmente la portata applicativa, come si avrà modo di chiarire più

[7] È affermazione diffusa quella secondo cui la seconda stagione della *privacy*, conclusasi quella delle prime esperienze legislative degli anni settanta e ottanta, sia caratterizzata dal concetto di controllo sui dati personali e sulle loro utilizzazioni, anziché sul riconoscimento di uno *ius excludendi alios*, che sarebbe reso impossibile dalle esigenze di sviluppo della società dell'informazione. In merito a tale evoluzione, che parte dal diritto alla *privacy* quale espressione della società borghese, per arrivare ad una nozione di controllo sulle proprie informazioni personali, il rinvio è, per tutti, a S. Rodotà, *Intervista su privacy e libertà*, Roma-Bari, 2005, *passim*.

diffusamente nel prosieguo[8].

È risaputo, del resto, che il principio di precauzione, sorto, a livello europeo, in ambito dottrinale tedesco, sia poi circolato rapidamente a livello internazionale, sino a divenire un principio di diritto comunitario, così come affermato anche dalla Corte di Giustizia[9]. Pertanto, è in tale prospettiva che dovrebbe essere interpretato il Regolamento in materia di protezione dei dati personali: non monoliticamente calato nel solo contesto della privacy, ma, liberandosi dalle tentazione di una riconduzione in compartimenti stagni, in un'ottica più ampia, che tenga conto sì delle problematiche già emerse in altri settori, ma, altresì, della sua riconducibilità ai principi generali del diritto comunitario.

2. La valutazione di impatto nel settore ambientale: l'esperienza nordamericana dell'Envorinmental Impact Statement

I primi esempi di dichiarazione di impatto e di self-assessment si registrano a partire dagli anni settanta negli Stati Uniti, nel settore della tutela dell'ambiente.

In particolare, nel National Environmental Policy Act (NEPA) del 1970 si richiedeva una dichiarazione di impatto ambientale" (EIS – Envorinmental Impact Statement), che le agenzie governative federali erano chiamate a produrre in merito alla qualità dell'ambiente nel territorio di propria competenza.

Nell'attuale assetto legislativo, il documento preliminare è ancora l'Environmental Asset, che deve esplicitare le ragioni di una determinata proposta con impatto ambientale, nonché le eventuali alternative per il raggiungimento degli obiettivi prefissati, nonché, infine, i soggetti contattati nella stesura della proposta. Nel caso in cui, al termine di tale verifica preliminare, non

[8] Naturalmente, si tratta di un profilo che dovrà essere osservato nel prossimo futuro, alla luce delle sanzioni che saranno comminate dalle singole Autorità garanti e, sul piano privatistico, dai pronunciamenti delle corti nazionali in caso di azioni risarcitorie.

[9] Cfr., a titolo esemplificativo, Corte Giust., 5.10.1999, C–175/98, *Lirussi,* in *Raccolta,* 1999, 6881; *Corte* Giust., 21.3.2000, C–6/99, *Greenpeace,* in *Raccolta*, 2000, 1651.

siano evidenziati specifici rischi, non è necessario procedere alla redazione di una dichiarazione di impatto[10].

Appare evidente, seppur in termini embrionali, che il modello adottato sia assimilabile a quello previsto dal Regolamento sulla protezione dei dati personali, laddove la fase di redazione della "valutazione di impatto" è solo eventuale e dipende dalle risultanze evidenziate dalla catalogazione delle tipologie di dati personali, finalità e trattamenti e dalla comunicazione dei dati stessi e, dunque, dagli specifici rischi evidenziati in sede di analisi.

Ritornando all'environmental asset, il National Environmental Policy Act lascia ampia discrezionalità ai soggetti chiamati ad effettuare l'autovalutazione, non dettando una lista di enti o istituzioni che debbano essere consultati preventivamente. Tuttavia, dalla lettura delle relazioni alla legge risulta evidente l'opportunità di confrontarsi con stakeholder pubblici, al fine di ottenere un parere, sebbene informale e non obbligatorio, sulla fattibilità degli interventi prospettati.

Nel medesimo periodo, anche nel Regno Unito si è fatto ricorso all' Envorinmental Impact Statement per alcuni progetti di British Petroleum e British Gas nel Mare del Nord: tuttavia, questi documenti rientrano nell'ambito della soft-law, dal momento che si tratta di attestazioni non imposte da alcuna normativa formale e, quindi, al più qualificabili come buone prassi utilizzate per preventivare e arginare i possibili danni ambientali.

Nell'ambito del diritto ambientale, il ricorso agli EIS ha destato, nell'ambito del diritto nordamericano, molte critiche, che possono essere riassunte nella lunghezza e nei costi delle procedure da adottare e nelle controversie legali che scaturiscono dalla pubblicazione di tali documenti, prodromici all'avvio delle attività pianificate[11].

---

[10] In questo caso, è necessario redigere un documento denominato FONSI (*Finding of No Significant Impact*).

[11] *Robertson v. Methow Valley Citizens*, 490 U.S. 332 (1989). In dottrina, v. R. Clarke, *Privacy impact assessment: Its origins and development*, in *Computer Law & Security Report*, 25(2) 123, 132 (2009).

In particolare, detti studi preliminari, pubblicati da agenzie federali, ma spesso compilati da società di consulenza esterna, erano generalmente molto voluminosi ed estremamente dettagliati, scoraggiando l'opera di controllo dei regolatori e determinando, di fatto, l'approvazione di alcuni progetti a prescindere dal loro reale impatto sul territorio.

Ancor prima dell'esperienza nel settore ambientale, il Congresso degli Stati Uniti aveva sviluppato un Technology Assessment (TA), svolto da parte dell'Office of Technology Assessment, nel quale si erano valutati gli impatti delle innovazioni scientifiche e tecnologiche sulla società e sui cittadini[12]. Questi documenti, utilizzati sino alla metà degli anni novanta, erano finalizzati ad eliminare eventuali effetti dannosi cagionati dalle modifiche tecnologiche e a determinare benefici efficienti in alcuni settori, quale quello sanitario, nei quali il ricorso alle innovazioni informatiche era considerato maggiormente necessario[13].

I tentativi qui solo sommariamente descritti, sviluppati a partire dagli anni settanta, pur risultando interessanti da un punto di vista di ricostruzione storica, non assumono però particolare rilevanza sotto il profilo dei rapporti privatistici e delle regole di responsabilità.

Difatti, i progetti menzionati erano concepiti in ambito pubblicistico, in quanto promossi o dettati da agenzie governative e funzionali a dimostrare esclusivamente l'impatto sociale delle proposte sostenute e delle attività pianificate, senza ripercussioni significative sulla regolamentazione dei rapporti obbligatori, né sull'apprezzamento di eventuali responsabilità connesse ai danni ambientali.

---

[12] Cfr. S. Boutillon, *The Precautionary Principle: Development of an International Standar*d, 23 *Mich. J. Int'l L.* 429 (2002).

[13] Anche a livello comunitario, sull'esempio dell'esperienza statunitense, si era attuato un *technology assessment*; cfr. European Parliamentary Technology Assessment, *What is a Technology Assessment* http://www.eptanetwork.org/EPTA/what.php

3. Analisi dei rischi e danni ambientali nell'esperienza internazionale ed europea

Come sopra accennato, il principio di precauzione trova, nel diritto ambientale, la sua prima forma di manifestazione. Se il richiamo all'interno della Dichiarazione della Conferenza delle Nazioni Unite sull'Ambiente Umano del 1972 appare quasi squisitamente nominale, una reale consacrazione si ha con la Dichiarazione conclusiva della UNCED (United Nation Conference on Environment and Development), del 1992, il cui art. 15 afferma testualmente che, "al fine di proteggere l'ambiente, gli Stati applicheranno largamente, secondo le loro capacità, il metodo precauzionale. In caso di rischio di danno grave o irreversibile, l'assenza di certezza scientifica assoluta non deve servire da pretesto per rinviare l'adozione di misure adeguate ed effettive, anche in rapporto ai costi, dirette a prevenire il degrado ambientale"[14].

A livello comunitario, l'iter del diritto ambientale, primo di essere racchiuso nel novero dei diritti fondamentali dal Trattato, vede le sue prime affermazioni nel Vertice di Parigi del 1972[15] e nella Conferenza di Bonn del medesimo anno che, seppur in forma meramente declamatoria, segnano l'ingresso della protezione ambientale tra le priorità della Comunità Europea, per mezzo dei Programmi di Azione Ambientale. Allo stesso modo, nel tentativo di tratteggiare il percorso comunitario, meritano di essere ricordati il "Secondo programma di azione" del 17 maggio 1977, e il "Terzo programma di azione" del 7 febbraio 1983.

Il 1987, proclamato anno europeo dell'ambiente, segna un punto di svolta, sia con l'adozione del "Quarto programma di azione" sia, soprattutto, con il Trattato di Roma e l'Atto Unico Europeo del 1986, che inserì un titolo specifico (il VII) dedicato all'"Ambiente" (artt. 130R, 130S e 130T). Per quanto interessa in questa sede, appare rilevante che, per la prima volta, sia stata stabilita una tripartizione nell'azione europea, declinata come azione preventiva, riparazione

[14] Sul punto, nuovamente M.G. Stanzione, *Principio di precauzione e diritto alla salute*, cit., 3.

[15] Nella dichiarazione finale si legge testualmente che *"l'espansione economica, che non è un fine a sé stante, deve con precedenza consentire di attenuare la disparità delle condizioni di vita. Essa deve essere perseguita con la partecipazione di tutte le parti sociali e deve tradursi in un miglioramento della qualità come del tenore di vita. Conformemente al genio europeo, si dedicherà un'attenzione particolare ai valori e beni non materiali e alla protezione dell'ambiente naturale, onde porre il progresso al servizio dell'uomo".*

dei danni alla fonte e imputazione dei danni al soggetto inquinatore[16].

La prospettiva tracciata dall'Atto Unico Europeo subisce un sensibile ampliamento nel Trattato di Maastricht del 1992, il cui art. 130R fece rientrare l'azione ambientale nel novero delle politiche dell'Unione, segnando altresì, al secondo punto, l'ingresso del già menzionato principio di precauzione[17]. Un ulteriore ampliamento si registra poi con il Trattato di Amsterdam che include, tra gli obiettivi fondamentali dell'Unione, quello della tutela ambientale.

Tale percorso è proseguito poi con la Convenzione di Nizza e con il Trattato di Lisbona, che ha ripreso gli obiettivi già manifestati nei precedenti Trattati, inserendo, per la prima volta, un esplicito rilievo ai cambiamenti climatici[18].

In ambito comunitario, la prima forma di assessment, ossia il primo procedimento di autovalutazione dei rischi di impatto ecologico, si ebbe con la valutazione di impatto ambientale (VIA) di cui alla direttiva 85/337/CEE del Consiglio, che, nel recepire le istanze del Vertice di Parigi e i primi tre piani di azione comunitaria, impone, a soggetti pubblici e privati, un'analisi preventiva[19]. Analogamente a quanto si vedrà per la c.d. PIA (privacy impact assessment), la VIA deve anche tener conto della minimizzazione dei possibili danni, introducendo misure per mitigare gli eventuali effetti pregiudizievoli

---

[16] Sul punto, anche per una panoramica esaustiva delle soluzioni comunitarie, si rinvia a B. Pozzo, *La responsabilità ambientale. La nuova Direttiva sulla responsabilità ambientale in materia di prevenzione e ripartizione del danno ambientale*, Milano, 2005, con particolare riferimento alla sezione introduttiva del volume; nonché M. Montini, *Profili di diritto internazionale*, e R. Rota, *Profili di diritto comunitario dell'ambiente*, in Aa.Vv., *Trattato di diritto pubblico dell'ambiente,* a cura di P. Dell'Anno – E. Picozza, *Principi generali*, I, Milano, 2012.

[17] Art. 130R p. 2: *"La politica della Comunità in materia ambientale mira a un elevato livello di tutela, tenendo conto della diversità delle situazioni nelle varie regioni della Comunità. Essa è fondata sui principio della precauzione e dell'azione preventiva, sul principio della correzione, anzitutto alla fonte, dei danni causati all'ambiente, nonché sul principio chi inquina paga*".

[18] Cfr. anche la Comunicazione del 29 giugno 2011 "*Un bilancio per la strategia Europa 2020*", con la quale la Commissione europea ha inserito tra i suoi obiettivi quello di "aumentare la proporzione del bilancio dell'Unione destinata al clima ad almeno il 20 %, attraverso i contributi di diverse politiche".

[19] Sul tema, per ulteriori approfondimenti, si rinvia a C. Malinconico, *La prevenzione nella tutela complessiva dell'ambiente: La valutazione di impatto ambientale*, in C. Malinconico, *I beni ambientali*, vol. V, in *Trattato di diritto amministrativo* (a cura di G. Santaniello), Cedam, 1991; A. Cutrera, *La di- rettiva 85/337/CEE sulla valutazione di impatto ambientale*, in *Riv. Giur. Amb.*, 1987, 499 ss.; S. Grassi, *Il quadro europeo sulla VIA*, in *Gazzetta Ambiente*, n. 1, 1997, 3; R. Ferrara (cur.), *La valutazione di impatto ambientale*, Padova, 2000; F. Fonderico, *Valutazione di impatto ambientale*, in *Diz. Dir. Pubb.*, diretta da S. Cassese, VI, Milano, 2006, 6171 ss.

all'ambiente.

Tralasciando i profili strettamente procedurali, che esulano dalla presente indagine, colpisce che la VIA sia stata impostata – solo a livello comunitario, mentre a livello interno ha subito profonde modifiche, in primo luogo, per dir così, di "approccio"[20] – quale analisi tecnica, fondata su protocolli predefiniti[21]. Una linea procedurale che, come si vedrà, è anche alla base della disciplina in materia di protezione dei dati personali che, in merito alla valutazione di impatto, pur lasciando un margine di discrezionalità ai titolari del trattamento, poggia su requisiti tendenzialmente oggettivi.

Successivamente, la VIA è stata integrata dalla valutazione ambientale strategica (VAS), introdotta con la direttiva n. 42 del 2001. L'ambito oggettivo dei due interventi, che pur rispondono ad una logica di fondo analoga, risulta però differente, atteso che, nel caso della VAS, la valutazione riguarda l'incidenza sull'ambiente dell'approvazione di piani e programmi e, quindi, interessa gli interventi complessivi che possono produrre effetti significativi sull'ambiente (ma non solo). Si assiste, dunque, ad un'ulteriore anticipazione della valutazione, che deve essere posta in essere in un momento anteriore alla stessa progettazione dell'opera o dell'intervento e, dunque, in una fase di mera pianificazione strategica[22].

Il mosaico è stato completato con la direttiva 2008/1/CE e dalla procedura di autorizzazione ambientale integrata (AIA)[23] che, integrata a livello interno nella VIA, in virtù del d.lgs. 128/2010, rappresenta un ulteriore strumento di controllo preventivo sull'impatto ambientale in caso di installazione ed esercizio di

---

[20] Sul punto, in chiave critica, v. R. Rota, *Profili di diritto comunitario dell'ambiente*, cit., 218.

[21] R. Rota, *La procedura di valutazione di impatto ambientale tra discrezionalità tecnica e discrezionalità amministrativa: alcune note ricostruttive*, in *Scritti in onore di Serio Galeotti*, Milano, 1998, vol. II, 353 ss.

[22] L'art. 1 della direttiva stabilisce espressamente che l'obiettivo è quello di "*garantire un elevato livello di protezione dell'ambiente e di contribuire all'integrazione di considerazioni ambientali all'atto dell'elaborazione e dell'adozione di piani e programmi al fine di promuovere lo sviluppo sostenibile assicurando che [...] venga effettuata una valutazione ambientale di determinati piani e programmi che possono avere un impatto significativo sull'ambiente*".

[23] Per ulteriori riferimenti al rapporto tra VIA e AIA, si rinvia a T. Marocco, *La direttiva IPPC e il suo recepimento in Italia*, in *Riv. Giur. Amb.*, 2004, 1, 35 ss.

impianti[24].

Come si avrà modo di approfondire nel prosieguo, tale modello di controllo preventivo si coniuga (e, a tratti, si confonde, almeno sotto il profilo dell'accertamento della responsabilità) con le regole risarcitorie e riparatorie dettate in materia di danno ambientale. La tematica, disciplinata per la prima volta nell'ordinamento italiano con l'art. 18 della Legge 8 luglio 1986, n. 349, istitutiva del Ministero dell'ambiente[25], ha subito una profonda modifica con la direttiva 2004/35/CE, che ha previsto una posizione subordinata del profilo risarcitorio rispetto al profilo riparatorio[26].

Di là da tali aspetti, così come dal differente criterio di imputazione dell'illecito (a carattere colposo, nel caso della responsabilità ambientale e a carattere semi-oggettivo, nel caso di illecito trattamento dei dati personali), ciò che interessa in

---

[24] Il processo è stato introdotto dalla direttiva n. 96/61 CE (c.d. IPPC–integrated pollution prevention and control); sul punto, v. E. Bohne, *The Implementation of the IPPC Directive from A Comparative Perspective and Lessons for Its Recast*, 5 *Journal for European Environmental and Planning Law*, 1, 319 (2008).

[25] Sul danno ambientale, prima della riforma introdotta dalla direttiva, v., all'interno di una copiosissima bibliografia, P. Trimarchi, *Per una riforma della responsabilità civile per danno all'ambiente*, Milano, 1994, *passim*; B. Pozzo, *Danno ambientale ed imputazione della responsabilità*, Milano, 1996, *passim* (e *ivi* ampi richiami anche alla legislazione straniera); B. Pozzo, *Verso una nuova responsabilità civile per danni all'ambiente in Europa: il nuovo libro bianco della commissione delle comunità europee*, in *Riv. giur. amb.*, 2000, 623 ss.; S. Sica, *Responsabilità per danno ambientale e crisi dell'illecito civile*, in *Rass. dir. civ*., 1988, 1031 ss.; M.C. Capponi, *L'illecito ambientale nella formulazione di cui all'art. 18, comma 1, l. 8 luglio 1986 n. 349 dal "danno" alla compromissione*, in *Riv. dir. impr.*, 1990, 489 ss.; V. Carbone, *Trasferibilità assicurativa del danno ambientale tra indirizzi comunitari e ordinamento italiano*, in *Danno e resp.*, 1997, 653 ss.; A. Somma, *Il risarcimento del danno ambientale nelle esperienze tedesca e nordamericana: Geschaftsfuhrung ohne auftrag e Public trust doctrine*, in *Riv. giur. amb.*, 1999, 593 ss.; E. Giancotti, *Il danno ambientale tra legge speciale e codice civile*, in *Riv. crit. dir. priv.*, 1998, 541 ss.; D. Chindemi, *Il danno ambientale*, in *Nuova giur. civ. comm.*, 1993, II, 431 ss.; A. Luminoso, *Sulla natura della responsabilità per danno ambientale*, in *Rass. giur. sarda*, 1989, 837 ss.; L.V. Moscarini, *Responsabilità aquiliana e tutela ambientale*, in *Riv. dir. civ.*, 1990, I, 489 ss.; E. Moscati, *Il danno ambientale tra risarcimento e pena privata*, in *Riv. giur. sarda*, 1990, 881 ss.; M. Granieri – R. Pardolesi, *Oltre la funzione riparatoria della responsabilità civile nella tutela ambientale*, in *Danno e resp.*, 1998, 845 ss.; F. Giampietro, *La responsabilità per danno all'ambiente nella proposta di direttiva comunitaria sui rifiuti e nella disciplina generale dell'art. 18 legge n. 349 del 1986*, in *Giust. civ.*, 1991, II, 223 ss.; M. Comporti, *Nuovi principi e nuove norme in tema di responsabilità per danno ambientale*, in *Riv. it. med. leg.*, 1999, II, 1485 ss.; M. Franzoni, *Il danno all'ambiente*, in *Contr. e impr.*, 1992, 1015 ss.; G. Gebers, *Libro bianco sulla responsabilità per danni all'ambiente*, in *Riv. giur. amb.*, 2000, 611 ss.; L. Prati, *La "fonte genetica" del danno ambientale nella recente giurisprudenza*, in *Danno e resp.*, 1998, 136 ss.

[26] Cfr. U. Salanitro, *L'evoluzione dei modelli di tutela dell'ambiente alla luce dei principi europei: profili sistematici della responsabilità per danno ambientale*, in *Nuove leggi civ. comm.*, 2013, 795 ss.; F. Bonelli, *Il risarcimento del danno all'ambiente e la direttiva 2004/35/CE: la nuova disciplina dettata dalla L. 166/2009*, in *Dir. comm. internaz.*, 2013, 21 ss.; A. G. Annunziata, *Il nuovo sistema di riparazione del danno ambientale alla luce della l. 6 agosto 2013, n. 97: obbligatorietà del risarcimento in forma specifica e nuovo "antropocentrismo dei doveri"*, in *Contr. e impr.*, 2015, 133 ss.

questa sede è l'intersezione delle regole di responsabilità con i processi tecnico-amministrativi, che accomuna le due esperienze[27].

4. Privacy Impact Assessment e modelli giuridici imitati

Si è già osservato, in apertura, che il Regolamento europeo sulla protezione dei dati personali, nella sua complessità, è la risultante di molteplici influenze e modelli di riferimento e di imitazione.

Da un lato, il regolamento trova, quale suo antesignano diretto, il diritto tedesco: molte soluzioni – si pensi, ad esempio, al responsabile per la protezione di dati personali o data protection officer - sono ricalcate, quasi pedissequamente, sulle scelte tratteggiate dal diritto tedesco[28]. Da un punto di vista politico, prima ancora che giuridico, il riferimento al diritto tedesco pare trovare una sua giustificazione razionale, per una parte, in logiche di efficacia, dal momento che si adotta un modello giuridico-normativo risultato negli anni, appunto, efficace, per un'altra parte, in prospettiva economica, ma prima ancora nuovamente politica, è da ricercare nella sua "efficacia", ovvero nell'idoneità dimostrata dal modello tedesco di contemperare i costi sostenuti dalle imprese per l'adeguamento al nuovo contesto legislativo.

---

[27] Un aspetto sicuramente differente è dato dall'oggetto giuridico tutelato. Sono note – ma solo accennabili in questa sede, per ovvie ragioni di economicità dell'esposizione – le difficoltà incontrate dalla dottrina nella perimetrazione della tutela ambientale, che si sono riverberate anche sulla operatività degli strumenti di tutela. Nell'ambito della dottrina italiana è nota la tripartizione operata da M.S. Giannini, *Ambiente: saggio sui diversi suoi aspetti giuridici*, in *Riv. trim. dir. pubbl.*, 1973, 15, che, muovendo dall'assunto secondo cui "*nel linguaggio normativo l'ambiente, per quanto di continuo evocato, non è definito né definibile, non ne sono precisate le condizioni d'uso, né è riducibile in enunciati prescrittivi*", assegna tre distinti significati: il primo relativo al paesaggio; l'altro alla difesa del suolo dell'acqua e dell'aria; il terzo, infine, utilizzato nella normativa urbanistica. Altra parte della dottrina ha proposto altre qualificazioni, cfr., *ex multis*, A. Predieri, voce *Paesaggio*, in *Enc. Dir.*, XXXI, Milano, 1981, 503; B. Cavallo, *Profili amministrativi della tutele dell'ambiente: il bene ambientale tra tutela del paesaggio e gestione del territorio*, in *Riv. trim. dir. pubbl.*, 1990, 397, nonché, in prospettiva privatistica, F. Di Giovanni, *Strumenti privatistici e tutela dell'ambiente*, Padova, 1982.

[28] Il responsabile della protezione dei dati presenta numerose analogie con il *datenschutzbeauftragter* di cui al *Bundesdatenschutzgesetz* tedesco del 2003. Il diritto tedesco, al pari dell'originaria formulazione dell'art. 37 del Regolamento, prevede che sia obbligatoria la nomina del *datenschutzbeauftragter* (DSB) in presenza di un numero minimo di dipendenti (250) preposti a mansioni che implicano il trattamento di dati personali; cfr. K.A. Bamberger - D.K. Mulligan, *Privacy Europe: Initial Data on Governance Choices and Corporate Practices*, 81 George Wash. L. Rev. 1529, 1604 (2013); nonché, nella dottrina italiana, v. G.M. Riccio, *Data Protection Officer e altre figure*, in S. Sica – V. D'Antonio – G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016, 33 ss.

Non è un mistero, infatti, che la gestazione faticosa del Regolamento sia riuscita a trovare un suo punto di approdo nell'equilibrio in buona parte imposto dalla presidenza greca durante lavori preparatori[29]: un intervento, quello in parola, che ha determinato la rimodulazione di talune soluzioni inizialmente individuate e ha portato all'adozione di un modello misto, che sorge dalla confluenza, cui già si è fatto cenno, di modelli di imitazione differenti[30].

Allo stesso modo, deve sottolinearsi che il modello statunitense è stato considerato più in chiave di antitesi che di congruenza: del resto, una frattura tra l'ordinamento americano e quello europeo era già stato evidenziato dalla scelta degli organi comunitari di censurare l'attività di raccolta indiscriminata di dati personali (c.d. bulk collection of personal data)[31] per finalità di controllo e, almeno sul piano teorico, di antiterrorismo, che poi aveva condotto alla decisione, invero traumatica per i suoi riflessi pratici, della Corte di Giustizia nel caso Schrems, con l'invalidazione dei Safe Harbors Principles, gli accordi che consentivano il trasferimento di dati personali dall'Europa agli Stati Uniti (e viceversa)[32].

---

[29] Cfr. C. Vander Maelen, *Digital Privacy Protection Against Corporate Actors in the European Union: Benefits, Flaws and Repercussions*, Ghent University, 2017, 18.

[30] Naturalmente, si fa riferimento al concetto di "modello misto", che è altro rispetto ai sistemi giuridici cc.dd. misti, su cui, v., da ultimo, J. Du Plessis, *Comparative Law and the Study of Mixed Legal Systems*, Oxford, Oxford University Press, 2006; G.C.K. Reid, *The Idea of Mixed Legal Systems*, 78, *Tulane Law Review*, 5 (2003).

[31] Cfr. F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 *Law & Cont. Probl.* 101, 108; *contra* P. Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, *Georgia Tech Scheller College of Business Research Paper*, No. #36. Cfr. altresì *Considerando 59* dei *Privacy Shield*: "*In this regard, the representations of the Office of the Director of National Intelligence (ODNI) provide further assurance that these requirements, including the definition of bulk collection in PPD-28 (n. 5), express a general rule of prioritisation of targeted over bulk collection. According to these representations, Intelligence Community elements "should require that, wherever practicable, collection should be focused on specific foreign intelligence targets or topics through the use of discriminants (e.g. specific facilities, selection terms and identifiers). While PPD-28 explains that Intelligence Community elements must sometimes collect bulk signals intelligence in certain circumstances, for instance in order to identify new or emerging threats, it directs these elements to prioritise alternatives that would allow the conduct of targeted signals intelligence. Hence, bulk collection will only be allowed where targeted collection via the use of discriminants is not possible "due to technical or operational considerations". This applies both to the manner in which signals ntelligence is collected and to what is actually collected. According to representations of the ODNI all this ensures that the exception does not swallow the rule*".

[32] Corte di Giustizia, 6 ottobre 2015, C-362/14, Maximillian Schrems c. Data Protection Commissioner. In merito alla pronuncia in questione, v. i contributi raccolti in G. Resta – V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbors Principles" al "Privacy Shield"*, Roma, 2016.

Dall'altro lato, non può non osservarsi che, seppur parzialmente, vi sia un'influenza per dir così endogena sul Regolamento stesso, che trae spunto, come suggerisce l'esperienza descritta dinanzi sul diritto ambientale, dagli antesignani normativi del diritto comunitario.

In questo senso, per rimanere nell'area del diritto alla protezione dei dati personali e del tema centrale del presente lavoro, non deve essere dimenticato che il Gruppo di lavoro Articolo 29 (Working Party Article 29 o WP29), che raccoglie i Garanti europei, aveva più volte fatto riferimento, nei propri pareri, alla necessità di adottare un criterio di self-assessment[33]. In tale prospettiva, si assiste ad una sorta di feedback legislativo o di doppio processo di imitazione giuridica[34]: il diritto comunitario è influenzato dai suoi prodromi e, in parte, dalle policy consideration dei propri regolatori; tuttavia, tali modelli sono, a loro volta, il frutto di un processo di imitazione di sistemi non europei che, però, una volta recepiti e assorbiti dal diritto comunitario risultano, per dir così, "depurati".

È quanto avvenuto nell'ambito del diritto alla tutela dei dati personali, laddove i principi di assessment, che trovano i loro riferimenti nella legislazione nord americana e in talune prassi extra-giuridiche, basate essenzialmente su criteri aziendalistici, partono comunque da un obiettivo di tutela che è tipicamente europeo, laddove il Regolamento, in linea con i valori sanciti nella Carta di Nizza, afferma la centralità della persona umana e la necessità di apprestare strumenti di protezione e di tutela efficaci[35].

Né va trascurata la circostanza che l'adozione di un modello di soft law, o meglio di no-law, soddisfa la necessità di dettare regole comuni (non già uniformi, ma uniche) per tutti gli Stati membri, non tenendo conto delle singole tradizioni nazionali. È lapalissiano, infatti, che la ricerca di un comune minimo

---

[33] Cfr., per un'analisi di tali pareri, L. Bolognini, *Adozione di strumenti per la sicurezza del trattamento*, in Bolognini-Bistolfi-Pelino (a cura di), *Il Regolamento Privacy europeo - Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 378 ss.

[34] G. Benacchio, *Diritto privato della Comunità europea. Fonti, modelli, regole*, Padova, 1998, 142.

[35] Sul tema, per tutti, P. Stanzione, *Persona. Diritto civile*, in *Enc. giur.*, XXIII, Roma, 1991, 1 ss. (ora anche in G. Autorino – P. Stanzione, *Diritto civile e situazioni esistenziali*, Torino, 1997, 11 ss.); P. Perlingieri, *La personalità umana nell'ordinamento giuridico*, Napoli, 1972, *passim*.

denominatore, in grado di accomunare tutte le esperienze nazionali, avrebbe determinato, come pure avvenuto per altre sezioni del regolamento, una confusione e un'incertezza giuridica ancora maggiori. Al contrario, nel complesso equilibrio che doveva condurre all'unificazione delle regole[36], la norma giuridica è stata supportata dall'elemento tecnico che, per sua natura, presenta caratteri unici e oggettivi (come nel caso delle certificazioni)[37].

---

[36] Si ricorda che si discorre di unificazione, quando non solo la norma è prodotta da un organo legislativo unitario, ma la sua interpretazione e la sua applicazione è univoca; si parla di uniformazione, invece, quando la norma è emanata da un organo legislativo unitario, ma l'applicazione è rimessa alla libera interpretazione degli Stati; infine, si ha armonizzazione, quando l'organo legislativo unitario pone delle regole tendenzialmente uniformi e i singoli Stati possono distaccarsene, purché non alterino il modello base. Questo aspetto è sottolineato anche da R. Sacco, in A. Gambaro - R. Sacco, *Sistemi giuridici comparati*, Torino, 2000, 36 ss.; S. Sacco, *I problemi dell'unificazione del diritto in Europa*, in *Nuova rivista di diritto commerciale, diritto dell'economia, diritto sociale*, 1953, II, 49 ss.; S. Ferreri, *Unificazione, uniformazione*, in *Dig. disc. priv.,* sez. civ., XIX, Torino, 1999, 504 ss.

[37] Il dato tecnico lo si rinviene anche nelle misure di *privacy by design* e di *privacy by default*, su cui si rinvia ad A. Cavoukian, *Privacy by Design in Law, Policy, and Practice. A White Paper for Regulators, Decision- makers and Policy-makers* (*Information and Privacy Commissioner of Ontario*, Canada, 2011), disponibile all'URL https://www.ipc.on.ca/images/resources/pbd-law-policy.pdf; nonché I.S. Rubinstein, *Regulating Privacy by Design* 26 *Berkeley Tech. L. J.* 1409 (2011). Al riguardo, è interessante notare la libertà che il legislatore comunitario ha concesso al titolare del trattamento: siamo al cospetto, infatti, di norme non già sprovviste di sanzione, atteso che, anzi, le sanzioni sono considerevolmente aumentate rispetto al passato, ma di norme, sia fatta passare l'espressione, senza precetto. In altri termini, il regolamento fissa degli obiettivi da raggiungere, in termini di sicurezza e di protezione dei dati, ma rimette al titolare la possibilità di selezionare le misure ritenute più idonee a garantire tale obiettivo. Questa soluzione presenta almeno un pregio e almeno un difetto. Il pregio è indiscutibilmente rappresentato dalla circostanza che, in uno scenario in cui le innovazioni tecnologiche cambiano con estrema rapidità, la norma giuridica non sia costretta a rincorrere la soluzione tecnica. Del resto, a livello interno, tale soluzione si era già manifestata nel caso dell'allegato B al Codice della privacy, che prevedeva una serie di misure di sicurezza per garantire uno standard minimo. Da un punto di vista degli standard di diligenza, per il titolare del trattamento era sufficiente rispondere a tali misure di sicurezza per non incorrere in alcuna sanzione. Il limite di tale ricostruzione era determinato dal fatto che tali misure risultavano, in realtà, non minime, ma, in molti casi, inefficaci: si pensi, a titolo meramente esemplificativo, al caso degli antivirus che, stando a quanto era previsto nell'allegato B del Codice privacy, dovevano essere aggiornati con scadenza almeno semestrale e, quindi, in un arco temporale obiettivamente inefficace a confrontare i reali attacchi informatici. Il Regolamento in materia di protezione dei dati personali, invece, ribalta tale prospettiva non prevedendo, come si diceva, nessuna misura specifica, ma limitandosi a considerare adeguate quelle che siano in linea con lo sviluppo tecnologico del momento. Deve osservarsi, peraltro, che nella predisposizione delle misure di sicurezza il titolare del trattamento è chiamato ad adottare quelle che risulta lecito attendersi in relazione non solo alla tipologia di dati trattati e alla tipologia di trattamenti posti in essere, e, quindi allo specifico profilo di rischio connesso a tali attività, ma, secondo alcuni, altresì tenendo conto di quelle che sono le capacità patrimoniali del titolare stesso. Per la verità, una simile lettura rischierebbe in parte di vanificare gli intenti del Regolamento: difatti, laddove si ritenesse, erroneamente, che le misure di sicurezza sono parametrate alla capacità patrimoniale del titolare del trattamento, ciò significherebbe imporre diversi standard di diligenza che dipendono dalle "tasche

5. Prime esperienze nazionali ed evoluzione comunitaria

Le prime leggi europee in materia di protezione dei dati personali (Svezia nel 1973 e Austria, Danimarca, Francia e Norvegia nel 1978) erano fondate su di un modello classico, in virtù del quale era imposta un'obbligazione predefinita al titolare del trattamento, dalla cui violazione discendeva un obbligo risarcitorio o una sanzione amministrativa[38].

Essenzialmente, la nozione di assessment, applicata al settore della tutela dei dati personali, si è affermata a partire dalla fine dello scorso secolo, grazie all'opera propositiva delle singole autorità nazionali. Invero, come è stato osservato[39], le discussioni embrionali hanno interessato poco la dottrina e sono state promosse a livello istituzionale, prima in ambiti di policy e, successivamente, in seno alle singole autorità nazionali.

Risulta dunque azzardato ipotizzare una reale (rectius: diretta) influenza di un singolo modello nazionale sulle soluzioni adottate, all'interno del Regolamento, da parte del legislatore comunitario.

Al contrario, più proficua si rivela l'analisi dei lavori preparatori del Regolamento stesso, al fine di tentare di individuare i processi imitativi sviluppati dagli organi europei.

La lettura dei lavori preparatori del Regolamento, infatti, evidenzia che il ricorso alla valutazione di impatto è stata determinata, in estrema sintesi, dalla presunta mancanza di percezione dei rischi da parte dei titolari del trattamento nel momento in cui commissionavano l'adozione di nuove tecnologie informatiche[40].

---

profonde" del titolare, ammettendo, quindi, un'esposizione al rischio per le libertà e i diritti fondamentali dei soggetti interessati.

[38] Per un primo quadro ricognitivo dei principali testi europei sulla *privacy* si rinvia a V. Frosini, Diritto alla riservatezza e calcolatori elettronici, in G. Alpa - M. Bessone (a cura di), *Banche-dati e diritti della persona*, Padova, 1984, 29 ss.

[39] R. Clarke, *Privacy impact assessment*, cit.

[40] Cfr. European Commission, DG Justice, *Freedom and Security Report*, in *New Challenges to Data Protection - Final Report*, June 2010, 50, par. 131, disponibile all'URL https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1636706: "*Privacy Enhancing Technologies and Privacy-Friendly Identity Management both have significant potential to protect individual privacy. However, most important of all is persuading policy-makers and business leaders to pay appropriate attention to the privacy implications of new information*

La soluzione a tale problematica viene individuata, nel Report preparatorio presentato alla Commissione, nell'adozione di un privacy impact assessment (PIA) obbligatorio, sul modello di altri ordinamenti extraeuropei[41], da un lato, e in misure di privacy by design e by default, dall'altro[42].

In una successiva comunicazione della Commissione al Parlamento e al Consiglio si afferma chiaramente la necessità che la valutazione di impatto sia obbligatoria, seppur nei soli casi in cui il trattamento riguardi dati sensibili oppure dati che presentano un particolare profilo di rischio, in connessione con le tecnologie concretamente adottate[43].

Come si avrà modo di illustrare a breve, tali sono i cardini attorno ai quali ruota la disciplina poi penetrata nell'art. 35 del Regolamento, che ha recepito indiscriminatamente i suggerimenti formulati.

---

systems before they are commissioned. The quantity of personal data collected and processed can be very significantly affected by details decided long before system architects and programmers start building new database applications. It is much easier to produce privacy-friendly systems if data protection issues are considered early in their design stage, with data minimization and security as key concerns. Significant privacy harms can result from systems that contain sensitive personal data on millions or tens of millions of individuals, with authorized access for hundreds of thousands of staff and long retention periods - as we see with many e-government applications - and are extremely difficult to address retrospectively".

[41] *Ibidem*, par. 131: "T*wo specific attempts should be mentioned that have been made to encourage early privacy planning by organisations. Privacy Impact Assessments are now mandatory in many jurisdictions including the US, requiring government agencies to assess privacy risks of new policies before systems are commissioned. As already noted, the Australian Government is also proposing to empower the Privacy Commissioner there to require PIAs from government agencies. The UK Information Commissioner encourages government and businesses to undertake assessments in order to address privacy concerns from the outset of projects, focusing on a systematic process that manages risk and incorporates the views of all those affected by new systems. Privacy By Design is an approach originally developed by the Ontario Privacy Commissioner that supports the production and operation of systems that minimise the collection, storage, processing and retention of personal data. This encompasses business policies and practices as well as the details of technologies used. It employs privacy impact assessments through the whole life-cycle of a system, from initial design, through operation, upgrades, and eventual decommissioning. The methodology needs senior management support to be effective, ensuring that privacy needs are included in the business cases for new systems and that they are met through the system life-cycle*".

[42] Sull'evoluzione in seno agli organi comunitari, v. A. Mantelero, *Riforma della direttiva comunitaria sulla data protection e privacy impact assesment, verso una maggiore responsabilità dell'autore del trattamento?*, in *Dir. inf.*, 2012, 145 ss.

[43] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Un approccio globale alla protezione dei dati personali nell'Unione europea*, COM/2010/0609 def.: "*integrare nel quadro giuridico l'obbligo per i responsabili del trattamento di realizzare in casi specifici una valutazione d'impatto della protezione dei dati , ad esempio per il trattamento di dati sensibili o se il tipo di trattamento presenta rischi particolari, soprattutto in connessione con determinate tecnologie, procedure e dispositivi, tra cui la profilazione o la videosorveglianza*".

6. Privacy Impact Assessment nel Regolamento in materia di protezione dei dati personali

La principale differenza tra le esperienze giuridiche passate in rassegna e il Regolamento in materia di protezione dei dati personali consiste nel fatto che, in quest'ultimo caso, ricorrendo determinati presupposti, l'assessment è richiesto in via obbligatoria e non solo quale strumento di soft law.

Ciò determina, evidentemente, una sostanziale modifica dell'approccio del destinatario della norma giuridica: difatti, nel primo caso, l'assessment e la risk analysis assumono una funzione principalmente organizzativa a livello aziendale, rispondendo alla necessità, in primo luogo per la struttura societaria investita della valutazione, di controllare e di ponderare ex ante la pericolosità (ergo l'attitudine al rischio) dell'iniziativa pianificata; nel caso del trattamento dei dati personali, invece, si adempie ad un obbligo giuridico-normativo, che, teoricamente, potrebbe non essere ritenuto necessario dall'impresa o dall'ente pubblico.

Si ripresenta, dunque, uno scenario più volte paventato in dottrina: quello, cioè, in cui il diritto alla protezione dati personali si trasforma in un mero adempimento formale, laddove la tutela sostanziale riconosciuta ai singoli cede il passo ad una logica di protezione dei soggetti imprenditoriali (rectius: dei titolari del trattamento), che sono messi in condizione di evitare qualsivoglia rischio sanzionatorio avendo adempiuto ai "passaggi", per l'appunto formalistici, imposti dal legislatore[44].

Del resto, è dimostrato in dottrina[45] che i metodi coercitivi punitivi adottati dai regolatori conducono verso forme di (si consenta l'espressione) "ritualismo giuridico": si allude, in particolare, al fenomeno secondo cui i destinatari

[44] È questa la condivisibile opinione di S. Sica, *Art. 1350. Degli atti che devono farsi per iscritto*, in *Commentario al Cod. civ.* dir. da F.D. Busnelli, Milano, 2003, 180 ss. In generale, sul dibattito intorno al formalismo, valga ancora il richiamo a G. Cian, *Forma solenne e interpretazione del negozio*, Padova, 1969, 8 ss.; N. Irti, *Idola libertatis. Tre esercizi sul formalismo giuridico*, Milano, 1985, *passim*; P.Perlingieri, *Forma dei negozi e formalismo degli interpreti*, Napoli, 1989, *passim*.

[45] F. Haines, *The Paradox of Regulation: What Regulation Can Achieve and What It Cannot*, Edward Elgar Publishing, 67 (2011).

dell'obbligo di assestement tenderanno ad indirizzare i propri sforzi verso la dimostrazione del rispetto delle regole imposte, anziché adottare forme flessibili di analisi del rischio e di mitigazione delle possibili conseguenze dannose.

Va detto, però, che il Regolamento privacy è fondato su un approccio basato sul rischio e, al contempo, sulla responsabilizzazione del titolare del trattamento. Siamo al cospetto di un principio più volte richiamato nel testo comunitario (ad esempio, nell'art. 24), che impone al titolare di adottare le misure tecniche, da un lato, e organizzative, dall'altro, tali da ridurre i rischi connessi con il trattamento dei dati.

Al tempo stesso, il Regolamento muove dall'esigenza di snellire gli adempimenti amministrativi, primo fra tutti l'obbligo di notifica, e di assegnare al titolare del trattamento l'onere l'onere di dimostrare l'adempimento delle misure richieste per legge.

Il profilo dell'eliminazione dell'obbligo di notifica, introdotto dalla Direttiva 95/46/CE e recepito negli art. 37 ss. del Codice privacy, appare alquanto rilevante nel contesto che interessa in questa sede: difatti, l'adempimento in parola era stato tacciato, da parte della dottrina e degli operatori del settore, di "formalismo inutile", ovvero non funzionale ad elevare il livello di protezione dei dati personali[46].

L'approccio del Regolamento, del resto, appare differente anche rispetto alla previsione dell'obbligo di verifica preliminare di cui all'art. 17 del Codice privacy (c.d. prior checking), verifica finalizzata ad ottenere un riscontro da parte dell'Autorità in caso di progettazione di trattamenti di dati che presentino particolari rischi per i diritti e per le libertà fondamentali dei soggetti interessati.

Il privacy impact assessment, invece, nelle intenzioni del legislatore comunitario, si pone quale strumento di gestione del rischio, frutto di un processo di

[46] S. Sica, *Art. 1350. Degli atti che devono farsi per iscritto*, cit., 183, ma v. anche A. Mantelero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (Artt. 32-39)*, in G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 321.

valutazione e di analisi dei pericoli associati ad un determinato trattamento, in relazione o alle finalità o alla tipologia di dati personali implicati.

Il privacy impact assessment non risulta però necessario per tutti i trattamenti ma, ai sensi dell'art. 35, esclusivamente per quei trattamenti che, potenzialmente, potrebbero presentare un rischio elevato per i diritti e le libertà delle persone fisiche. La medesima norma prevede, innanzitutto, che ciò possa avvenire "in particolare in caso di uso di nuove tecnologie": si tratta di un riferimento, evidentemente, esemplificativo, ma non casuale. Il richiamo alle tecnologie evoca, infatti, antichi spettri che, da sempre, si agitano nel settore in questione. Ne costituiscono una riprova i principali casi giudiziari che hanno interessato, anche a livello comunitario, la protezione dei dati personali, coinvolgevano direttamente l'utilizzo di tecnologie dell'informazione, quali i motori di ricerca[47].

Il legislatore, peraltro, non ha qualificato la nozione di rischio elevato, prestando il fianco a talune critiche[48].

Infatti, il secondo paragrafo dell'art. 25 contiene un'elencazione che, come dimostrato dall'utilizzo dell'espressione "in particolare", non può essere ritenuta tassativa; nei casi indicati dalla norma, tuttavia, il titolare del trattamento, previa consultazione con il data protection officer, deve comunque procedere alla valutazione di impatto[49].

Un ampliamento di questo elenco è stato però dettato dal Gruppo di lavoro Articolo 29 nelle proprie Linee Guida, che hanno elencato nuovi criteri per l'individuazione di fattori di cui tener conto per la determinazione della necessità

---

[47] Cfr. Corte di giustizia, 13 maggio 2014, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, causa C-131/12, su cui si rinvia ai numerosi commenti pubblicati in *Diritto dell'Informazione e dell'Informatica*, Milano, n. 4-5, 2014, ora raccolti in G. Resta - V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015.

[48] A. Mantelero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati,* cit., 287 ss.

[49] I casi sono i seguenti: "*una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*".

di una valutazione di impatto[50]. Tali criteri, peraltro, devono sussistere in maniera cumulativa (o, per meglio dire, devono essere presenti almeno due dei criteri elencati dal Gruppo di lavoro Articolo 29), per cui la semplice presenza di uno di tali indici non risulta sufficiente a far sorgere, in capo al titolare del trattamento, l'obbligo di redigere un privacy impact assessment. È pur vero, che, stando a quanto affermato nelle Linee guida, in caso di dubbio, il titolare dovrebbe comunque procedere alla valutazione di impatto, a conferma di un orientamento generale del Regolamento che muove dalla necessità di rispondere all'esigenza di minimizzare i rischi connessi al trattamento dei dati personali.

La lista può essere accresciuta – prevede l'art. 35 par. 4 –, a livello nazionale, dalle singole Autorità garanti, che pubblicano un elenco delle tipologie di trattamento soggette alla valutazione di impatto: tale lista deve essere comunicata al Comitato europeo della protezione dei dati di cui all'art. 68 del Regolamento[51]. In tal modo, si dovrebbe prevenire il rischio di una difformità tra singoli Stati membri ossia, in altri termini, il rischio che determinati trattamenti risultino soggetti alla PIA in alcuni ordinamenti e non lo siano in altri.

Al contrario, la soluzione adottata dovrebbe consentire di riunire le esperienze maturate dai diversi Garanti nazionali in presenza di procedure di prior checking, durante le quali le singole Autorità sono chiamate a pronunciarsi su progetti e trattamenti innovativi e potenzialmente rischiosi per i diritti e le libertà dei soggetti interessati.

La pubblicazione di una lista dovrebbe contribuire anche a ridurre i costi transattivi associati ad eventuali consulenze esterne finalizzate a stabilire

---

[50] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, Adopted on 4 April 2017 As last Revised and Adopted on 4 October 2017.

[51] Il par. 5 prevede invece la facoltà – e, quindi, non l'obbligo – per le Autorità garanti di "*redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati*". Anche in tale ipotesi è prevista la comunicazione della lista al Comitato. Appare importante ricordare che, ai sensi del par. 6, "*Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione*".

l'obbligatorietà o meno della PIA, che saranno previste come necessarie dal Comitato europeo per la protezione dei dati o dai Garanti nazionali[52].

Parimenti, sebbene né il Gruppo di lavoro Articolo 29 né, per quanto è dato sapere, le Autorità nazionali abbiano pubblicato un modello di privacy impact assessment – come avvenuto, invece, nel caso dei registri del trattamento[53] –, una possibile riduzione dei costi connessi all'elaborazione del documento richiesto potrebbe essere determinata dalla previsione, in seno al par. 7 dell'art. 35, del contenuto minimo, che dovrà indicare, quanto meno, una descrizione sistematica dei trattamenti previsti e delle relative finalità, con indicazione dell'interesse legittimo perseguito dal titolare del trattamento; una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità previste; una valutazione dei rischi per i diritti e le libertà dei soggetti interessati; e, da ultimo, le misure (non solo tecnologiche)[54] previste "per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione".

La nozione di rischio recepita nel Regolamento non sembra differire, da un punto di vista ontologico, rispetto a quella già accolta in altri settori e, in particolare, nella normativa tecnica[55]: si tratta, quindi, di "uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità"; allo stesso modo, la gestione dei rischi è la risultante "delle attività

---

[52] Deve essere ricordato, sempre nell'ottica del contemperamento dei costi transattivi, che il titolare del trattamento è legittimato a redigere una PIA unica in caso di trattamenti simili, limitando ed accorpando il lavoro di analisi dei rischi connessi al trattamento. Si tratta di una soluzione non solo ammissibile, ma altresì consigliata dal Gruppo di lavoro Articolo 29; cfr. WP 248 rev.01, cit., par III, A.

[53] Si veda, al riguardo, quanto diffuso dall'Autorità francese per la protezione dei dati personali: CNIL, *Comment se préparer au règlement européen sur la protection des données?*, disponibile all'URL: https://www.cnil.fr/fr/comment-se-preparer-au-reglement-europeen-sur-la-protection-des-donnees

[54] Risulta importante, ad avviso di chi scrive, che siano tenute in considerazione le misure organizzative e gestionali, come, ad esempio, le prassi e le *policy* aziendali che, nell'ottica della riduzione del rischio, dovrebbero essere comunicate ai singoli soggetti incaricati (a partire dai dipendenti del titolare del trattamento).

[55] Cfr. a riguardo la nozione di valutazione del rischio che, ai sensi della ISO Guide 73:2009, è qualificata come "*l'insieme dei processi di identificazione dei rischi, di analisi del rischio e di valutazione del rischio*".

coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi"[56].

L'intersezione tra il settore della protezione dei dati personali e le metodologie già sviluppate e applicate in altri ambiti, in cui la valutazione del rischio è già diffusa (come, oltre che in quello ambientale, anche nell'ambito sanitario) risulta evidente nell'adozione delle metodologie specifiche da adottare in sede di assessment, che, per l'appunto, possono essere modellate per ricalcare quelle già invalse e validate in altri campi. Si pensi, a titolo esemplificativo, alle norme internazionali, come quelle sviluppate dall'ISO[57], che consentono altresì di garantire una forma di unificazione delle regole sul piano tecnico e tecnologico, ancor prima che sul piano giuridico[58].

7. Valutazione di impatto e regole di responsabilità

Interrogarsi sul ruolo che rivestono, nell'ambito dell'autovalutazione, le norme del Regolamento, impone altresì di chiedersi quale sia la relazione tra dette norme e le regole ordinarie che, nel settore considerato, presiedono alla responsabilità aquiliana.

In altri termini, resta da chiarire in che modo principi di autoresponsabilità e di autovalutazione, enunciati nel Regolamento, si coniugano con gli articoli dedicati alla responsabilità del titolare del trattamento.

---

[56] cfr. WP 248 rev.01, cit., punto III.

[57] In particolare ISO 31000:2010-*Risk management* e ISO 27005:2011 - *Information security risk management*

[58] Del resto, l'interazione tra le regole tecniche e regole giuridiche è rinvenibile anche in altri punti del Regolamento, *in primis* nell'art. 42 relativo alla certificazione. Si ricorda che, ai sensi dell'articolo citato, il Regolamento incoraggia gli Stati membri, le Autorità di controllo, il Comitato e la Commissione ad istituire meccanismi di certificazione della protezione dei dati nonché sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al Regolamento dei trattamenti effettuati dai titolari e dai responsabili. La certificazione, pensata quale ulteriore tassello della *self responsibility* del titolare del trattamento, non è obbligatoria e non attesta l'adeguamento alle previsioni comunitarie, considerato che il Garante può sempre contestare la conformità delle certificazioni adottate dal titolare del trattamento (art. 42 comma 4). Le certificazioni (al momento non esistono certificazioni "validate" pensate esclusivamente per le attività di trattamento dei dati personali) possono essere rilasciate dal Garante (art. 42 comma 5) oppure, in alternativa, dagli Organismi di certificazione che si siano preventivamente accreditati (al momento, il solo ente accreditatore, nel nostro ordinamento, è Accredia - designato in base al Regolamento EU n 765/08, conformemente alla norma EN- ISO/IEC 17065/2012).

È noto che, sin dalla direttiva del 1995, il legislatore comunitario ha optato per un modello di responsabilità di natura (tendenzialmente) oggettiva, individuando, nel titolare del trattamento, il soggetto in grado di rispondere ai danni connessi all'utilizzo di dati personali[59].

Ancor prima, è d'uopo ricordare che, storicamente, alla responsabilità aquiliana sono state assegnate due funzioni: scartata la funzione punitiva[60], la dottrina ha sempre riconosciuto alle regole sull'illecito aquiliano una funzione, da un lato, deterrente, e dall'altro, riparatoria[61].

Fatte tali premesse, è possibile, sia alla luce del Regolamento sulla protezione dei dati personali sia delle normative di settore (a partire da quelle ambientali, che affermano un principio di precauzione fondato sull'autovalutazione), ritenere che alle funzioni storiche della responsabilità civile se ne sommino altre o che, leggendo in diversa prospettiva l'evoluzione legislativa, tali funzioni siano raggiunte, almeno sotto il profilo della deterrenza, non solo per mezzo delle tradizionali norme sui fatti illeciti, ma anche attraverso disposizioni che sanciscono un obbligo preventivo, che preesiste al verificarsi di un danno effettivo?

Il Regolamento in materia di protezione dei dati personali, per quanto riguarda il risarcimento del danno, non ha innovato particolarmente la materia. L'art. 82

---

[59] Discorre di responsabilità semi-oggettiva, in relazione all'art. 18 della Legge 31 dicembre 1996, n. 675, S. Sica, *Commento* sub *art. 18*, in E. Giannantonio - M. G. Losano - V. Zeno-Zencovich, *La tutela dei dati personali. Commentario alla l. 675/96*, Padova, 1997, 176 ss.; per un commento alla disposizione in questione, v. anche M. Franzoni, *Dati personali e responsabilità civile*, in *Resp. civ. prev.*, 1998, 902 ss.; G. Comandè, *Danni cagionati per effetto del trattamento dei dati personali*, in F.D. Busnelli - C.M. Bianca, *Tutela della privacy*, in *Nuove leggi civ. comm.*, 1999, 482 ss.; F.D. Busnelli, *Il «trattamento dei dati personali» nella vicenda dei diritti della persona : la tutela risarcitoria*, in V. Cuffaro - V. Ricciuto - V. Zeno-Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, 177 ss.; G. Alpa, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, *Dir. inf.*, 1997, 703 ss.; R. Clarizia, *Legge 675/96 e responsabilità civile*, in *Dir. inf.*, 1998, 235 ss.; G. Buttarelli, *Banche dati e tutela della riservatezza*, Milano, 1997, 350 ss. ; M. Bin, *Privacy e trattamento dei dati personali*, in *Contr. e impr./Europa*, 1997, 459 ss.

[60] G.P. Fletcher, *Punishment and Compensation*, 14 *Creighton L. Rev.* 691 (1981); P. Catala – J.A. Weir, *Delict and Torts: A Study in Parallel*, in 37 Tulane L. Rev. 582 (1963).

[61] Cfr., tra i tanti, S. Rodotà, *Il problema della responsabilità civile*, Milano, 1965, 16 ss. F.D. Busnelli, *La parabola della responsabilità civile*, in *Riv. crit. dir. priv.*, 1988, 643; P.G. Monateri, *La responsabilità civile*, in *Tratt. di dir. civ.* dir. da R. Sacco, Torino, 1998, 37; S. Sica, *La responsabilità – Le responsabilità: note in tema di sistema e funzione della regola aquiliana*, in *Danno e resp.*, 2002, 353 ss.

stabilisce che "Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento". Il terzo paragrafo, invece, ponendosi nel solco della Direttiva 46/95/CE, afferma che il titolare o il responsabile del trattamento "è esonerato dalla responsabilità […] se dimostra che l'evento dannoso non gli è in alcun modo imputabile".

Appare evidente che il modello di responsabilità è nuovamente tratteggiato prescindendo dall'elemento soggettivo colposo, individuando nel titolare del trattamento la deep pocket party e, al contempo, il soggetto sul quale principi di efficienza suggeriscono di allocare i costi degli incidenti connessi al trattamento dei dati[62]. Difatti, tale soggetto, seppur chiamato a rispondere in via solidale con il responsabile (nei casi in cui anche a quest'ultimo possa essere ascritto l'illecito), risulta quello più facilmente individuabile (anche perché espressamente nominato nelle informative fornite ai soggetti interessati) in una catena che condurrebbe potenzialmente a danni non riconducibili univocamente alla condotta di un solo soggetto ossia a danni, per utilizzare un'espressione "antica", anonimi[63].

Sebbene l'art. 82 non contenga novità di rilievo, se non per quanto riguarda la declamazione delle sue formule, maggiormente interessante risulta la convivenza di tale norma con l'art. 83 che, nel dettare i parametri per la determinazione del quantum delle sanzioni amministrative, stabilisce che si debba tener conto "delle misure tecniche e organizzative da essi messe in atto", nonché dell'adesione ai

---

[62] Sul tema, in termini generali, v., per tutti, G. Calabresi, *Some Toughts on Risk Distribution and the Law of Torts*, in 70 *Yale L.J.*, 499 (1961).

[63] Il riferimento è chiaramente a J. Josserand, , *La responsabilité du fait des choses inanimées*, Paris, 1897, p. 7. Sulla "esplosione" della responsabilità oggettiva, determinata dall'impossibilità di individuare il reale autore dell'illecito, v., all'interno di una bibliografia sconfinata, K. Zweigert – H. Kotz, *Introduzione al diritto comparato*, trad. it., II, Milano, 1995, 347 ss.; C. Larroumet, *Réflexions sur la responsabilité civile. Évolution et problèmes actuels en droit comparé*, Montreal, 18 ss.; P. Trimarchi, *Rischio e responsabilità oggettiva*, Milano, 1961, 11 ss.; C.M. Bianca, *La responsabilità*, *Diritto civile*, Milano, 1994, 536 ss.; C. Castronovo, *La nuova responsabilità civile*, Milano, 1997, 34 ss.; A. Tunc, *La responsabilité civile*, cit.; S. Rodotà, *Il problema della responsabilità civile*, Milano, 1965, 16 ss.; G. Calabresi, *Costo degli incidenti e responsabilità civile*, 1975, 17 ss.; G. Alpa - M. Bessone, *I fatti illeciti*, in *Tratt. di dir. priv.* diretto da P. Rescigno, Torino, 1982, 303 ss.; V. Zeno-Zencovich, *La responsabilità civile*, in G. Alpa - M.J. Bonell - D. Corapi - L. Moccia - V. Zeno-Zencovich, *Diritto privato comparato. Istituti e problemi*, Roma-Bari, 1999, 275 ss.; G. Alpa, *La responsabilità civile*, in *Tratt. di dir. civ.*, Milano, 1999, 65 ss.; F.F. Stone, *Touchstones of Tort Liability*, in 2 *Stanf. L. Rev.* 270 (1950).

codici di condotta o ai meccanismi di certificazione approvati e, soprattutto, di "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".

È indubbio che, come affermato più volte dalla giurisprudenza, il danno derivante dall'illecito trattamento dei dati personali debba essere parametrato all'effettiva lesione subita dal soggetto interessato e non può essere considerato quale danno in re ipsa[64]. Al contempo, tuttavia, risulta interessante riflettere sull'influenza che, in chiave crittotipica, i parametri fissati per la sanzione amministrativa possono esercitare sul giudice ordinario, in special modo nel momento in cui lo stesso deve valutare gli standard di diligenza adottati dal titolare del trattamento.

In tal senso, non può che condividersi l'opinione di parte della dottrina che, come sopra accennato, ha ritenuto che il criterio di imputazione sia di carattere semi-oggettivo, residuando un elemento colposo e, di conseguenza, imponendo in sede di qualificazione della responsabilità e di determinazione del danno una valutazione delle misure adottate per impedire o mitigare il danno cagionato.

Allo stesso tempo, la convergenza tra principio di precauzione (di cui le prassi di self-assessment sono una possibile manifestazione) e regole aquiliane deve essere letto in termini né antitetici, nel senso che il primo non influenzerebbe le altre, né cumulativi, nel senso che la precauzione assurgerebbe ad ulteriore funzione, che prescinderebbe dal realizzarsi concretamente di una lesione. Invece, a parere di

---

[64] Cfr. Cass., 8 febbraio 2017, n. 3311, in *Quotidiano Giuridico*, 2017; Cass., 3 luglio 2014, n. 15240, in *Quotidiano Giuridico*, 2014: "*L'illegittimo trattamento di dati sensibili ex art. 4 del d.lgs. 30 giugno 2003, n. 193, configurabile come illecito ai sensi dell'art. 2043 cod. civ., non determina un'automatica risarcibilità del danno, dovendo il pregiudizio (morale e/o patrimoniale) essere provato secondo le regole ordinarie, quale ne sia l'entità e quale che sia la difficoltà di assolvere l'onere probatorio, trattandosi di un danno-conseguenza e non di un danno-evento, non rilevando in senso contrario neppure il suo eventuale inquadramento quale pregiudizio non patrimoniale da lesione di diritti costituzionalmente garantiti*"; Cass., 29 settembre 2013, n. 22100, in CED Cassazione: "*In tema di risarcimento del danno non patrimoniale per violazione dell'art. 15 del d.lgs. 30 giugno 2003, n. 196 (c.d. codice della privacy), è ammissibile la prova per testimoni di tale danno, in quanto esso non può ritenersi "*in re ipsa*", ma va allegato e provato, sia pure attraverso il ricorso a presunzioni semplici, e, quindi, a maggior ragione, tramite testimonianze, che attestino uno stato di sofferenza fisica o psichica".*

chi scrive, il self-assessment dovrebbe essere utilizzato quale strumento "misto"[65] ed elemento per valutare, in sede di accertamento della responsabilità, la condotta del titolare del trattamento e la sua effettiva adesione agli standard di diligenza attesi, in relazione alle sue capacità patrimoniali e ai costi necessari per un adeguamento alle misure prescritte (rectius: suggerite) dal Regolamento, alle tipologie di dati personali e di trattamenti posti in essere e alle specifiche tecnologie utilizzate.

[65] Cfr. G. Calabresi, *La responsabilità civile come diritto della società mista*, in *Pol. dir.*, 1978, 665 ss.