IAIC MiBACT DGBIC CREDA

DIRITTO MERCATO TECNOLOGIA

FONDATA E DIRETTA DA
Alberto M. Gambino

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

15 dicembre 2023

"Responsabilità" e "danno" da illecito trattamento dei dati personali. Il modello europeo all'indomani del caso VB c. NAP

Giorgio Sica

Nuova Editrice Universitaria

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

Norme di autodisciplina

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

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

Sede della Redazione

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

"RESPONSABILITÀ" E "DANNO" DA ILLECITO TRATTAMENTO DEI DATI PERSONALI. IL MODELLO EUROPEO ALL'INDOMANI DEL CASO *VB* C. *NAP*

Giorgio Sica
Dottorando di ricerca in diritto privato comparato
presso l'Università di Napoli "Federico II"

SOMMARIO: 1. Circolazione dei dati e significato sistematico della responsabilità civile nel prisma della *data protection*; 2. Il caso *VB* c. *NAP*: quesiti pregiudiziali e *rationes decidendi* della Corte di giustizia dell'Unione Europea; 3. Giudizio di adeguatezza delle misure del trattamento *ex* art. 32 GDPR e *onus probandi*; 4. *Liability*, poco *strict*, ma molto aggravata? Profili di esonero da responsabilità *ex* art. 82 GDPR e risarcibilità del danno "immateriale".

ABSTRACT: Il presente contributo si propone di analizzare il più recente approdo interpretativo in materia di responsabilità per illecito trattamento dei dati personali. Dopo aver sondato il ruolo sistematico svolto dalla responsabilità civile rispetto alla dimensione della *data protection*, l'elaborato restringe il focus su una interessante decisione della Corte di Giustizia dell'Unione europea e sulle *rationes decidendi* ad essa sottese. Particolare rilievo assumono i profili dell'*onus probandi*, del giudizio di adeguatezza della misure del trattamento *ex* art. 32 GDPR e della risarcibilità del danno "immateriale", che congiuntamente scandiscono il più complessivo assetto di *liability*.

***ABSTRACT**: The present essay aims to analyse the most recent interpretative approach regarding to liability for unlawful processing of personal data. After having probed the systematic role played by civil liability with respect to the data protection dimension, the paper narrows its focus to an interesting decision of the Court of Justice of the European Union and the*

rationes decidendi underlying it. Particularly relevant are the profiles of the burden of proof, of the adequacy assessment of the processing measures pursuant to Article 32 GDPR, and of the compensability of the "immaterial" damage, which jointly mark the more overall liability structure.

1. Circolazione dei dati e significato sistematico della responsabilità civile nel prisma della *data protection*

Nel più ampio libro della responsabilità civile il danno da trattamento illecito dei dati personali rappresenta, per molti versi, il capitolo più interessante dell'ultimo ventennio.

In realtà, tutto ha inizio con la direttiva 46/95/CE che per la prima volta introdusse, in termini generali, una disciplina sulla protezione dei dati personali in cui risulta sintetizzata la filosofia che aveva guidato la transizione dalla privacy alla *data protection*.

La metamorfosi non è ovviamente soltanto lessicale ma, se è consentito dire, di visione di fondo. La riservatezza, nella sua dimensione originaria, in un'accezione quasi dominicale[1], era intesa in senso essenzialmente statico, cioè come tutela da ingerenza altrui nella propria sfera di vita[2]. Per converso,

[1] Come diritto di matrice liberale, il diritto alla riservatezza mutua costantemente i propri caratteri dalle trasformazioni della società contemporanea, nel quadro dell'espansione dei mercati e della pervasività della tecnica. Cfr. S. RODOTÀ, voce *Riservatezza*, in *Enc. trecc*., VI App., Roma, 2000; J. HABERMAS, *Storia e critica dell'opinione pubblica*, Bari-Roma, 1984; per una ricostruzione v. anche A. CATAUDELLA, voce *Riservatezza (diritto alla). I) diritto civile*, in *Enc. giur*., Roma, 1991, p. 1 ss.; M. GIORGIANNI, *La tutela della riservatezza,* in S. RODOTÀ (a cura di), *Il diritto privato nella società moderna*, Bologna, 1971, p. 139 ss.; ma si v. anche G. GIANNONE CODIGLIONE, *La tutela della riservatezza*, in S. SICA-V. ZENO-ZENCOVICH (a cura di), *Manuale di diritto dell'informazione e della comunicazione*, VI ed., Padova, 2022, p. 275 ss.; A.M. GAMBINO-D. MULA-A. STAZI, *Diritto dell'informatica e della comunicazione*, III ed., Torino, 2019, p. 74 ss.

[2] S.D. WARREN-L.D. BRANDEIS, *The Right to Privacy*, in 4 *Harv. L. Rev*. 193 (1890); sul celebre saggio "fondativo" di tale diritto fondamentale cfr. D.J. SOLOVE, *A Brief History of Information Privacy Law*, in K.J. MATHEWS (a cura di), *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, 2ª ed., New York, 2017, § 1, spec. 1:3:4; sulla contrapposizione tra la nozione personalistica di Warren e Brandeis e la logica di matrice dominicale riconducibile al concetto di proprietà intellettuale v. anche G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2006, p. 214 ss.

protezione dei dati personali sottintende il passaggio alla società ed all'economia della comunicazione, che presuppone, quale elemento fondante, l'incessante scambio e circolazione di informazioni[3].

La prima disciplina comunitaria in materia è la cristallizzazione di tale modello e dell'approdo alla privacy in senso "procedimentale", basata sull'architrave dell'*Informed Consent*. La risposta al quesito sul se una simile evoluzione abbia generato conseguenze di rilievo e, soprattutto, sia stata garanzia di effettività di tutela del soggetto interessato richiederebbe un più ampio approfondimento[4]. Probabilmente la risposta dovrebbe quantomeno essere dubitativa, tant'è che di fronte all'ultima frontiera, la "monetizzazione" dei dati[5], ci si interroga sulla necessità di una tutela collettiva, di impronta consumeristica, a fronte della debolezza del consenso individuale, sempre

[3] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, p. 28 ss.; G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997, p. 350 ss.; V. FROSINI, *La libera circolazione dei beni e dei servizi informatici nel mercato comune europeo*, in *Dir. inf*., 1995, spec. p. 21 ss.

[4] La propensione della disciplina europea sulla protezione dei dati personali ad apprestare una tutela dei dati personali dinamica e di tipo rimediale, basata sulla previsione di poteri diretti di reazione dell'interessato e che svolge altresì effetti conformativi di tipo preventivo sulle attività di trattamento svolte da titolari e responsabili, *in vece* dell'adozione di un modello declamatorio e rigido di definizioni e di situazioni giuridiche di stampo proprietario, è rilevata da A. DI MAJO, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in V. CUFFARO-V. RICCIUTO-V. ZENO-ZENCOVICH (a cura di) *Trattamento dei dati e tutela della persona*, Milano, 1999, p. 228 s., nonché ID., *La tutela civile dei diritti*, Milano, 2003, p. 149 («L'espressione "diritti" sta più propriamente per "rimedi"») e ancora C. CASTRONOVO, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in *Trattamento dei dati e tutela della persona*, cit., p. 660 ss.

[5] Sul punto, da ultimo v. E. RAGANELLA (a cura di), *La monetizzazione dei dati personali*, Milano, 2023, *passim*, ma v. anche S. SICA-G. GIANNONE CODIGLIONE, *I social network sites e il "labirinto" delle responsabilità*, in *Giur. merito*, 12, 2012, p. 2714 ss.; di contratti di scambio discute C. PERLINGIERI, *Profili civilistici dei* social networks, Napoli, 2014, p. 88 ss., 90, ma si v. anche V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 23 ss., 38 ss.; P. PERLINGIERI, *Privacy digitale e protezione dei dati personali tra persona e mercato*, in *Foro nap*., 2, 2018, p. 481 ss.; A. QUARTA-G. SMORTO, *Diritto privato dei mercati digitali*, Firenze, 2020, p. 211 ss.; S. VIGLIAR, *Consenso, consapevolezza e responsabilità nei* social network sites, Padova, 2012.

più "foglia di fico" del trattamento lecito e viziato alla base da un'asimmetria della posizioni[6].

Nondimeno, uno degli aspetti di maggior rilievo si rinviene nella circostanza per cui dalla direttiva 46/95, passando, in Italia, per la l. n. 675/96 ed il d. lgs. n. 196/2003 (c.d. Codice della protezione dei dati personali)[7] e sino al più recente *step* del GDPR (Regolamento UE 2016/679)[8], alla responsabilità civile è stato assegnato un compito preciso di bilanciamento del rischio ineluttabile che la (necessaria) circolazione dei dati reca con sé.

A ben vedere, si tratta di un vero e proprio *fil rouge*, di cui è possibile perfino tracciare il percorso. L'art. 23 della citata direttiva, al comma 1, fissava il fondamentale principio alla stregua del quale «gli Stati membri dispongono che chiunque subisca un danno cagionato da trattamento illecito o

---

[6] In argomento v. A.M. GAMBINO, *Clausole vessatorie e internet*, in V. RICCIUTO-N. ZORZI, *Il contrattato telematico*, Padova, 2002, p. 183 ss.; G. RESTA-V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ*., 2, 2018, p. 411 ss.; A. STAZI-F. CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Dir. inf*., 2, 2019, p. 442 ss.; F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, 2018, *passim*; ID., *Lo ''scambio di dati personali'' nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. impr*., 1, 2019, pp. 34-58; C. ALVISI, *Dati personali e diritti dei consumatori*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, *I dati personali nel diritto europeo*, cit., p. 669 ss., M. SCHMIDT-KESSEL,*Consent for the Processing of Personal Data and its Relationship to Contract*, in A. DE FRANCESCHI-R. SCHULZE (a cura di), *Digital revolution. New Challenges for Law*, Muenchen, 2019, pp. 75-83.

[7] Per un approfondimento S. SICA-P. STANZIONE (dir. da), *La nuova disciplina della privacy*, Bologna, 2004; PC.M. BIANCA-F.D. BUSNELLI (a cura di), *La protezione dei dati personali*, Padova, 2007; R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003; F. CARDARELLI-S. SICA-V. ZENO-ZENCOVICH (a cura di), *Il codice dei dati personali*, Milano, 2004;E. GIANNANTONIO-M.G. LOSANO-V. ZENO ZENCOVICH, *La tutela di dati personali. Commentario alla L. 675/96*, Padova, 1999.

[8] Il considerando n. 2 del GDPR sottolinea che 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 dottrina v. S. CALZOLAIO, voce *Protezione dei dati personali* (dir. pubbl.), in *Dig. disc. pubbl*., Agg., Torino, 2017, p. 594 ss.; G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dat*i, in *Nuove leggi civ. comm*., 1, 2017, p. 1 ss.; S. GUTWIRTH-E. LEENES- P. DE HERT (a cura di), *Reforming European Data Protection Law*, Springer 2015; S. SICA-V. D'ANTONIO-G.M. RICCIO, *La nuova disciplina europea della privacy*, Padova, 2016, *passim*; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016.

da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della presente direttiva abbia il diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento». Ma, ancor più significativamente, il comma 2, appone un'indelebile impronta alla natura della responsabilità in esame, stabilendo che «il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabile».

Si tratta di una precisa scelta di campo che presuppone, si diceva, una visione sistematica così, per sintesi, descrivibile: i dati non possono non circolare, essendo il "carburante" dell'organizzazione sociale e dei processi economici, ma al "rischio da circolazione" deve corrispondere uno schema risarcitorio di *favor victimae* basato quantomeno su un onere della prova invertito[9].

Tale impronta avrebbe generato effetti benefici (e coerenti) in tutte le legislazioni nazionali derivate. La legge n. 675/96 italiana, con scelta opportuna ed ispirata, "traduceva" l'art. 23 della direttiva nell'art. 18, teso a riconoscere la risarcibilità del danno per effetto del trattamento dei dati personali ai sensi dell'art. 2050 c.c.

La disposizione, è ampiamente noto, ebbe ad aprire il dibattito, a tratti superfluo, relativo ala scelta normativa nella direzione della qualificazione *ex lege* del trattamento dei dati come "attività pericolosa" ai sensi dello stesso art. 2050 c.c.: la questione, in effetti, appassionava poco giacché, sul piano pratico, ciò che rileva è che per il legislatore italiano il danno da ("per effetto del") trattamento dei dati viene ricondotto in seno al composito settore delle cc.dd. responsabilità aggravate, qualsivoglia sia l'accezione delle stesse.

In una visione minimale, infatti, è certamente garantita alla vittima l'agevolazione probatoria dell'allegazione dei soli elementi del fatto, del

[9] 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 – 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. 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. p. 43 ss.; S. RODOTÀ, *Il problema della responsabilità civile*, Milano, 1964, spec. p. 175 ss.

danno e del nesso di causalità. Eppure, chi è consapevole del formante giurisprudenziale relativo all'art. 2050 c.c., ha ben chiaro che la via di uscita dell'esonero del convenuto è assai stretta. Se, infatti, la prova di "aver adottato le misure idonee" non si fa coincidere con la dimostrazione della sola massima diligenza esigibile, ma si impone l'indicazione del "fatto terzo", imprevedibile ed inevitabile, che ha generato l'evento[10], il passo verso una responsabilità "semi-oggettiva" è breve. E, probabilmente, è l'approdo interpretativo più coerente con la *ratio* di tutela che, si è visto, ispira la disciplina europea.

Nella medesima prospettiva si muove il Codice della protezione dei dati personali, vero e proprio testo unico di settore, resosi necessario per l'imponente implementazione nazionale ed europea della materia, ad appena sei anni dalla prima legge in argomento. L'art. 15 dello stesso, al comma 1, riproduceva la medesima formulazione dell'art. 18 della legge n. 675/96, opportunamente stabilendo, al comma 2, che «il danno non patrimoniale è risarcibile anche in caso di violazione dell'art. 11». In altre parole, ove fosse necessario, eliminava ogni dubbio sulla risarcibilità della voce di pregiudizio non patrimoniale derivante da trattamento non conforme (art. 11), con una specificazione che appare perfino superflua (oggi, in un'ottica di *compensation* integrale, qualsiasi perplessità sarebbe spazzata via) e che, tuttavia, sottolineava una volta di più l'aspirazione alla "copertura" più estesa possibile del rischio da trattamento dei dati personali.

Semmai, il Codice del 2003 è significativo in quanto nella sua prima versione (il testo è stato oggetto di costanti interventi legislativi nel tempo, per sopravvenute discipline europee o nazionali e per la notevole produzione paranormativa del Garante per la protezione dei dati personali), espressamente

[10] Le disposizioni menzionate state sempre interpretate come momento di riequilibrio dell'inevitabilità del trattamento, il più delle volte compiuto per finalità di attività di impresa. In dottrina si v. 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 ss.; ID., *Sub artt. 18 e 29, comma 9*, in E. GIANNANTONIO-M. GLOSANO-V. ZENO ZENCOVICH, *La tutela di dati personali. Commentario alla L. 675/96*, Milano, 1997, p. 176 ss.; A. MAIETTA, *Sub art. 15*, in S. SICA-P. STANZIONE, *La nuova disciplina della privacy*, Bologna, 2003, p. 66 ss.; G. COMANDÈ, *Sub art. 15*, in C.M. BIANCA-F.D. BUSNELLI, *La protezione dei dati personali*, Padova, 2007, p. 362 ss.; A. MANTELERO, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, 2007, spec. p. 183 ss.

codifica il diritto alla protezione dei dati personali come situazione soggettiva autonoma riconosciuta all'interessato. Difatti il testo originario dell'art. 1 del d.lgs. n. 196/2003 espressamente consacrava il diritto alla protezione dei dati personali nella formula del "chiunque ha diritto alla protezione dei dati personali che lo riguardano".

È stato sottolineato che per effetto di una simile declamazione il diritto in questione dismetteva la sua originaria funzione "servente" rispetto agli altri diritti e libertà fondamentali[11], nel senso di ricevere tutela soltanto in quanto collegato alle ulteriori situazioni oggetto di tutela primaria, per dare accesso all'idea per cui la lesione del diritto a vedere i propri dati adeguatamente protetti risulta tutelabile *ex se*.

2. Il caso *VB* c. *NAP*: quesiti pregiudiziali e *rationes decidendi* della Corte di giustizia dell'Unione Europea

L'evoluzione normativa da ultimo (ma certamente non in via "ultimativa", considerato il carattere del settore) risulta integrata dalla nuova disciplina generale contenuta nel citato GDPR. Quest'ultimo in punto di responsabilità, abrogando ogni testo previgente al riguardo, all'art. 82, ha così statuito: «un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento […]. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità […] se dimostra che l'evento dannoso non gli è in alcun modo impu-

[11] Il già menzionato art. 2, primo comma del Codice per la protezione dei dati personali previgente prescriveva infatti che il trattamento dei dati personali si dovesse svolgere «nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali». In generale sul rapporto tra principio di dignità e sistema dei diritti fondamentali nelle moderne società di mercato v. S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, p. 179 ss., ma ancora prima ID., *Elaboratori elettronici e controllo sociale*, cit., p. 81 ss.; sulla tutela dell'identità personale come diritto autonomo e sovente connesso alla protezione dei dati personali v. anche v. G. FINOCCHIARO, voce *Identità personale*, in *Dig. disc. priv.*, sez. civ., 2010, p. 721 ss.; G. RESTA, *Identità personale e identità digitale*, in *Dir. inf.*, 2007, p. 511 ss.

tabile»[12]. La regolamentazione vigente dunque ribadisce, senza soluzione di continuità, il *favor victimae* che contrassegna la materia dal 1995 in avanti.

Alla luce di tali imprescindibili premesse e nella medesima logica, appare di estrema rilevanza la recente controversia decisa dalla Corte di Giustizia Europea (Terza Sezione) con la pronuncia del 14 dicembre 2023, nella causa C-340/21, tra *VB* c. *Natsionalna agentsia za prihodite (NAP)*[13], che dunque è opportuno ripercorrere.

La NAP è l'autorità emanazione del Ministero delle Finanze bulgaro che si occupa, tra l'altro, del recupero dei crediti pubblici, essendo, altresì, titolare del trattamento dei dati personali dei soggetti ai quali si riferisce la propria attività. Da notizie di stampa nel 2019 si apprese che, a seguito di un attacco *hacker*, molti dei dati detenuti da NAP (relativi a circa sei milioni di interessati) erano stati acquisiti illegittimamente e divulgati via internet da terzi. Taluni degli interessati avevano così proposto azioni risarcitorie tese a conseguire il ristoro dei danni morali patiti, sul presupposto della mancata protezione dei dati medesimi ed allegando il danno immateriale conseguente al timore di un utilizzo abusivo dei propri dati.

La difesa della NAP è consistita essenzialmente nella dimostrazione di aver adottato tutte le misure necessarie, a monte, per prevenire il *breach*, ed a valle per la limitazione degli effetti pregiudizievoli per gli interessati.

Con decisione del 27 novembre 2020 l'*Administrativensad Sofiagrad* (giudice amministrativo di prima istanza) respingeva il ricorso, rilevando come la parte attrice non avesse provato l'inadeguatezza delle misure di sicurezza adottate dalla convenuta; inoltre per il giudice di prime cure non era ravvisabile alcun pregiudizio immateriale patito dal ricorrente.

---

[12] S. SICA, *La responsabilità civile per il trattamento illecito dei dati personali*, in A. MANTELERO-D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, pp. 161-174; G.M. RICCIO, *sub art. 82, Reg. UE n. 679/2016*, in G.M. RICCIO-G. SCORZA-E. BELISARIO, *GDPR e Normativa Privacy. Commentario*, Milano, 2019, pp. 199-201; M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, *I dati personali nel diritto europeo*, cit., p. 1017 ss.; G. FROSIO, *The Right to Be Forgotten: Much Ado About Nothing*, in 15 *Colo. Tech. L.J.* 307 (2017). Una critica alla disciplina previgente è ad esempio mossa da P.G. MONATERI, *Illecito e responsabilità civile*, II, Torino, 2002, p. 92 ss.

[13] CGUE, Terza sez., causa C-340/21, sent. 14 dicembre 2023, in *Racc. dig*., 2023.

La *Varhovenadministrativensad* (Corte suprema amministrativa della Bulgaria), adita in sede di gravame, ha inteso proporre rinvio pregiudiziale, ora risolto con la decisione della Corte di giustizia dell'Unione Europea in esame.

Per il giudice del rinvio particolarmente rilevanti risultavano i quesiti che è significativo riportare analiticamente:

«1) Se gli articoli 24 e 32 del GDPR debbano essere interpretati nel senso che è sufficiente che abbia avuto luogo una divulgazione o un accesso non autorizzati ai dati personali, ai sensi dell'articolo 4, punto 12, del GDPR, da parte di persone che non sono dipendenti dell'amministrazione del titolare del trattamento e non sono soggette al suo controllo, per ritenere che le misure tecniche e organizzative adottate non siano adeguate.

2) In caso di risposta negativa alla prima questione, quale debba essere l'oggetto e la portata del controllo giurisdizionale di legittimità nell'esame dell'adeguatezza delle misure tecniche e organizzative adottate dal titolare del trattamento ai sensi dell'articolo 32 del GDPR.

3) In caso di risposta negativa alla prima questione, se il principio di responsabilità di cui agli articoli 5, paragrafo 2, e 24 del GDPR, in combinato disposto con il considerando 74 di tale regolamento, debba essere interpretato nel senso che, in un procedimento giudiziario conformemente all'articolo 82, paragrafo 1, del citato regolamento, incombe sul titolare del trattamento l'onere di provare che le misure tecniche e organizzative sono adeguate ai sensi dell'articolo 32 del GDPR.

4) Se una perizia possa essere considerata un mezzo di prova necessario e sufficiente per determinare se le misure tecniche e organizzative adottate dal titolare del trattamento, in un caso come quello di specie, fossero adeguate, qualora l'accesso e la divulgazione non autorizzati di dati personali siano conseguenza di un "attacco hacker".

5) Se l'articolo 82, paragrafo 3, del GDPR debba essere interpretato nel senso che la divulgazione o l'accesso non autorizzati a dati personali ai sensi dell'articolo 4, paragrafo 12, di tale regolamento che, come nel caso di specie, ha avuto luogo mediante un "attacco hacker" da parte di persone che non sono dipendenti dell'amministrazione del titolare del trattamento e che non sono soggette al suo controllo, configura un evento che non è in alcun modo

imputabile a quest'ultimo e che gli consente di essere esonerato dalla responsabilità.

6) Se l'articolo 82, paragrafi 1 e 2, del GDPR, in combinato disposto con i considerando 85 e 146 di tale regolamento, debba essere interpretato nel senso che, in un caso come quello di specie, in cui ha avuto luogo una compromissione della protezione dei dati personali, verificatasi sotto forma dell'accesso non autorizzato e nella diffusione di dati personali mediante un "attacco hacker", le sole inquietudini e ansie e i soli timori provati dalla persona interessata in merito ad un eventuale futuro uso improprio dei dati personali rientrino nella nozione di danno immateriale, che deve essere interpretata estensivamente, e facciano sorgere il diritto al risarcimento, qualora tale uso improprio non sia stato accertato e/o la persona interessata non abbia subito alcun ulteriore danno».

Insomma, si tratta di quesiti attinenti alle linee di fondo del modello di responsabilità, sia in termini di *an* che di *quantum* e con riguardo in specifica maniera alla portata ed al perimetro del regime esoneratorio. Di qui l'interesse estremo della decisone in esame pronunciata dalla CGUE, la prima così esplicita in argomento, e dei principi di diritto che è il caso di riprendere testualmente:

«1) Gli articoli 24 e 32 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), devono essere interpretati nel senso che una divulgazione non autorizzata di dati personali o un accesso non autorizzato a tali dati da parte di terzi, ai sensi dell'articolo 4, punto 10, di tale regolamento, non sono sufficienti, di per sé, per ritenere che le misure tecniche e organizzative attuate dal titolare del trattamento in questione non fossero adeguate, ai sensi di tali articoli 24 e 32.

2) L'articolo 32 del regolamento 2016/679 dev'essere interpretato nel senso che l'adeguatezza delle misure tecniche e organizzative attuate dal titolare del trattamento ai sensi di tale articolo deve essere valutata dai giudici nazionali in concreto, tenendo conto dei rischi connessi al trattamento di cui

trattasi e valutando se la natura, il contenuto e l'attuazione di tali misure siano adeguati a tali rischi.

3) Il principio di responsabilità del titolare del trattamento, enunciato all'articolo 5, paragrafo 2, del regolamento 2016/679 e concretizzato all'articolo 24 di quest'ultimo, deve essere interpretato nel senso che nell'ambito di un'azione di risarcimento fondata sull'articolo 82 di tale regolamento, al titolare del trattamento di cui trattasi incombe l'onere di dimostrare l'adeguatezza delle misure di sicurezza da esso attuate ai sensi dell'articolo 32 di detto regolamento.

4) L'articolo 32 del regolamento 2016/679 e il principio di effettività del diritto dell'Unione devono essere interpretati nel senso che al fine di valutare l'adeguatezza delle misure di sicurezza che il titolare del trattamento ha attuato ai sensi di tale articolo, una perizia giudiziaria non può costituire un mezzo di prova sistematicamente necessario e sufficiente.

5) L'articolo 82, paragrafo 3, del regolamento 2016/679 deve essere interpretato nel senso che il titolare del trattamento non può essere esonerato dal suo obbligo di risarcire il danno subito da una persona, ai sensi dell'articolo 82, paragrafi 1 e 2, di tale regolamento, per il solo fatto che tale danno deriva da una divulgazione non autorizzata di dati personali o da un accesso non autorizzato a tali dati da parte di «terzi», ai sensi dell'articolo 4, punto 10, di detto regolamento, dato che tale responsabile deve allora dimostrare che il fatto che ha provocato il danno in questione non gli è in alcun modo imputabile.

6) L'articolo 82, paragrafo 1, del regolamento 2016/679 deve essere interpretato nel senso che il timore di un potenziale utilizzo abusivo dei suoi dati personali da parte di terzi che un interessato nutre a seguito di una violazione di tale regolamento può, di per sé, costituire un danno "immateriale", ai sensi di tale disposizione».

Sostanzialmente la Corte fa sue le conclusioni dell'Avvocato generale, Giovanni Pitruzzella, che altrettanto significativamente si era espresso nei termini appresso riportati:

«Gli articoli 5, 24, 32 e 82 del Regolamento 2016/679 devono essere interpretati nel senso che:

– la mera esistenza di una "violazione dei dati personali", come definita all'articolo 4, paragrafo 12, non sia di per sé sufficiente per concludere che le misure tecniche e organizzative attuate dal titolare del trattamento non erano "adeguate" a garantire la protezione dei dati in questione;

– nel verificare l'adeguatezza delle misure tecniche e organizzative attuate dal titolare del trattamento dei dati personali, il giudice nazionale adito deve effettuare un controllo che si estende a un'analisi concreta sia del contenuto di tali misure sia del modo in cui sono state applicate e dei loro effetti pratici;

– nell'ambito di un'azione di risarcimento danni ai sensi dell'articolo 82 del GDPR, il titolare del trattamento dei dati personali ha l'onere di dimostrare l'adeguatezza delle misure che ha attuato ai sensi dell'articolo 32 di tale regolamento;

– in conformità al principio dell'autonomia procedurale, spetta all'ordinamento giuridico interno di ciascuno Stato membro determinare i metodi di prova ammissibili e il loro valore probatorio, compresi i mezzi istruttori che i tribunali nazionali possono o devono ordinare, al fine di valutare se un titolare del trattamento dei dati personali abbia attuato misure adeguate ai sensi di tale regolamento, nel rispetto dei principi di equivalenza e di efficacia definiti dal diritto dell'Unione;

– il fatto che la violazione di tale regolamento che ha causato il danno in questione sia stata commessa da un terzo non costituisce di per sé un motivo per esonerare il titolare del trattamento dalla responsabilità e, per beneficiare dell'esenzione prevista da tale disposizione, il titolare del trattamento deve dimostrare che la violazione non gli è in alcun modo imputabile;

– il pregiudizio consistente nel timore di un potenziale futuro uso improprio dei suoi dati personali, di cui l'interessato abbia dimostrato la sussistenza, può costituire un danno morale che dà diritto a un risarcimento, a condizione che l'interessato dimostri di aver subito individualmente un danno emotivo reale e certo, circostanza che spetta al giudice nazionale adito verificare in ogni singolo caso»[14].

[14] Conclusioni dell'Avvocato generale Giovanni Pitruzzella presentate il 27 aprile 2023, Causa C□340/21, *VB c. Natsionalnaagentsia za prihodite*, in *Racc. dig*., 2023.

3. Giudizio di adeguatezza delle misure del trattamento *ex* art. 32 GDPR e *onus probandi*

La soluzione adottata pare certamente equilibrata e per gran parte convincente.

Dal capo 1) si ricava il rifiuto di uno schema di responsabilità oggettiva a carico del titolare; ed in realtà, nessuno, in dottrina e sin qui nelle giurisprudenze nazionali, si era spinto a sostenere che titolare e responsabili costituissero le *deep pocket* cui ricondurre *tout court* il rischio del trattamento dei dati.

Del tutto condivisibile è l'ulteriore conclusione secondo cui la verifica di adeguatezza delle misure adottate è la più tipica *quaestio facti*. La valutazione giudiziale, tuttavia, non può essere discrezionalmente casistica; specifica la Corte che dall'articolo 32, paragrafi 1 e 2, risulta che l'adeguatezza di siffatte misure tecniche e organizzative deve essere valutata secondo una duplice prospettiva. Da un lato, occorre individuare i rischi di violazione dei dati personali indotti dal trattamento di cui trattasi e le loro eventuali conseguenze per i diritti e le libertà delle persone fisiche. Ed è significativo che tale valutazione debba essere effettuata in concreto, prendendo in considerazione il grado di probabilità dei rischi individuati e il loro grado di gravità.

Dall'altro lato, occorre verificare se le misure attuate dal titolare del trattamento siano adeguate a tali rischi, tenuto conto dello stato dell'arte, dei costi di attuazione nonché della natura, della portata, del contesto e delle finalità di tale trattamento[15].

[15] Nella giurisprudenza di legittimità italiana si v. per esempio il caso del riconoscimento della r.c. di una pubblica amministrazione per la lesione del diritto alla riservatezza quando non si adoperi con tutte le misure necessarie ad evitare il danno ovvero la diffusione dei dati personali, perché l'art. 18 della legge n. 675/1996 segue la disciplina dell'art. 2050 cod. civ. (Nel caso di specie veniva riconosciuto il risarcimento del danno patito per la lesione del diritto alla riservatezza di un soggetto che aveva cambiato sesso, perché l'ufficio elettorale del Comune aveva trasmesso non soltanto il dato anagrafico, ma l'intero dossier comprensivo del procedimento di mutamento di sesso, non essenziale ai fini della nuova iscrizione anagrafica nel Comune di trasferimento). Così, seppur con riferimento alla disciplina previgente, Cass., sez. III, 15 luglio 2014, n. 1613, in *Foro it.*, 2015, I, c. 120, ma v. anche Cass., sez. III, 26 giugno 2012, n. 10646, in *Danno e resp.*, 2013, p. 399, con nota di A. BALDASSARRE; Cass., sez. VI, 5 settembre 2014, n. 18812, 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.lgs. 30 giugno 2003 n. 196, sono assoggettati alla disciplina di

E soprattutto, se è pur vero che «il titolare dispone di un certo margine di discrezionalità per determinare le misure tecniche e organizzative adeguate» ciò non esime il giudice nazionale dal sottoporre ad autonomo vaglio la ponderazione compiuta del titolare.

Tale enunciato va strettamente collegato alla basilare conferma del riparto probatorio in materia, con inequivocabile onere di prova dell'adeguatezza a carico del titolare, tenuto a fornire gli elementi atti a considerare assolto il proprio compito organizzativo. E ciò pur sempre senza tralasciare che «per controllare l'adeguatezza di misure tecniche e organizzative attuate ai sensi dell'articolo 32 del GDPR, un giudice nazionale non deve limitarsi a constatare in che modo il titolare del trattamento interessato abbia inteso adempiere gli obblighi ad esso incombenti in forza di tale articolo, bensì è tenuto ad effettuare un esame di tali misure nel merito, alla luce di tutti i criteri menzionati in detto articolo nonché delle circostanze proprie del caso di specie e degli elementi di prova di cui tale giudice dispone al riguardo».

Peculiare è poi la questione della "necessità" di una perizia giudiziaria in punto di adeguatezza: la Corte ovviamente non la esclude in assoluto, ma vi nega l'idoneità di "mezzo di prova sistematicamente necessario e sufficiente".

4. *Liability*, poco *strict*, ma molto aggravata? Profili di esonero da responsabilità *ex* art. 82 GDPR e risarcibilità del danno "immateriale"

Probabilmente, il cuore dell'interpretazione proposta attiene all'art. 82, par. 3, del GDPR, allorquando la Corte precisa che la disposizione deve essere intesa nel senso che l'esonero del titolare non può essere conseguito «per il solo fatto che tale danno deriva da una divulgazione non autorizzata di dati personali o da un accesso non autorizzato».

Il quadro si completa con l'affermazione per cui tale responsabile deve allora dimostrare che il fatto che ha provocato il danno in questione non gli è in alcun modo imputabile.

---

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».

Così ricostruita, la fattispecie in esame fa segnare piena continuità con la traiettoria intrapresa dalla direttiva 46/95, nella prospettiva funzionale del meccanismo risarcitorio, vero e proprio contrappeso dell'ineliminabile rischio connesso alla circolazione dei dati, quest'ultima, a sua volta intesa come imprescindibile componente dei processi socio-economici.

Si può dunque sostenere che nel già evocato libro della responsabilità civile, considerata in chiave finalistica, questa in oggetto costituisce davvero una pagina importante. Al contempo, essa rappresenta la conferma del portato storico dell'istituto aquiliano, nella sua componente polifunzionale[16] che, nella dimensione europea del settore in esame, pare trovare sbocco in una formula di responsabilità aggravata, non oggettiva, ma con una via di uscita esoneratoria molto ristretta, come è forse auspicabile a fronte della crescente dimensione del rischio di determinate attività[17].

Il che, sul piano pratico, fa ritenere corretta la scelta applicativa italiana che, prima del GDPR, aveva optato per l'art. 2050 c.c. come il riferimento più coerente con la *ratio* della disciplina europea; parimenti conforta l'opinione, questa volta per il tramite giurisprudenziale, in base alla quale la decifrazione dell'art. 82 GDPR nell'esperienza italiana vada attuata mediante la funzione vicaria dell'art. 2050 c.c., nella migliore accezione che dottrina e corti ne hanno proposto.

---

[16] Cfr. in via preliminare G. ALPA, *La responsabilità civile*. cit., spec. p. 131 ss.; C. SALVI, *La responsabilità civile*, in *Tratt. Iudica-Zatti*, Milano, 2008, p. 38; G. PONZANELLI, *La responsabilità civile. Profili di diritto comparato*, Bologna, 1992; S. SICA, *Note in tema di sistema e funzioni della regola aquiliana*, in *Danno e resp*., 2002, 8-9, p. 911 ss.

[17] Si pensi al dibattutissimo tema delle regole di responsabilità civile dell'internet service provider: in una sconfinata letteratura sul tema si rimanda ad A.M. GAMBINO, *Le responsabilità civili dell'Internet* service provider, Napoli, 2006; S. SICA, *Il sistema delle responsabilità*, in S. SICA-G. COMANDÈ, *Il commercio elettronico*, Torino, 2001, p. 220; G.M. RICCIO, *La responsabilità civile degli internet* providers *nel d.lgs. n. 70/2003*, *in Danno e resp*., 2003, p. 1158; G. GIACOBBE, *La responsabilità civile per l'uso di Internet*, in V. RICCIUTO-N. ZORZI, *Il contratto telematico*, in *Tratt. dir. comm. e dir. pubbl. econ. Galgano*, XXVII, Padova, 2002, p. 219 ss.; G. PONZANELLI*, Verso un diritto uniforme per la responsabilità degli* internet service providers*,* in S. SICA-P. STANZIONE, *Commercio elettronico e categorie civilistiche*, Milano, 2000, p. 368 ss.; F. DI CIOMMO, *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, 2003; ID., voce *Internet* (responsabilità civile), in *Enc. giur*., Roma, 2002; R. BOCCHINI, *La responsabilità civile degli intermediari del commercio elettronico*, Napoli, 2003.

Certo, residua un profilo di non poco conto nella logica (preferibile) della *réparation intégrale* del pregiudizio patito dall'interessato, vale a dire quello del danno risarcibile. Non si allude tanto all'ammissibilità del risarcimento del danno non patrimoniale, pacifico in sede legislativa (dal Codice della protezione dei dati personali del 2003 all'odierno GDPR). Semmai v'è da chiedersi quanto la teoria italiana del danno non patrimoniale sia in grado di assecondare la visione panrisarcitoria che la materia sembra aver privilegiato.

Il tema, per la sua valenza sistematica, imporrebbe una riflessione più estesa e monografica. Tuttavia, pare possibile sostenere che il *point of balance* raggiunto nel nostro ordinamento dalle cc.dd. Sentenze San Martino[18] in poi possa trovare feconda applicazione anche in relazione al risarcimento (auspicabilmente molto esteso) del danno da trattamento illecito dei dati personali. In questo ambito va infatti considerato che la componente "morale" è forse la più significativa ed una concezione "restrittiva" dello spazio risarcitorio sarebbe inconcepibile, soprattutto se si considera che la struttura dell'*an* muove nella direzione innanzi descritta.

In questo senso è sicuramente d'ausilio la netta affermazione della CGUE, alla stregua della quale «il timore di un potenziale utilizzo abusivo dei suoi dati personali da parte di terzi che un interessato nutre a seguito di una violazione di tale regolamento può, di per sé, costituire un "danno immateriale"».

Appena un cenno merita la sovrapponibilità delle nozioni di danno "immateriale" e danno "non patrimoniale", nel contesto in cui l'espressione viene utilizzata. Piuttosto, v'è da interrogarsi sul riflesso di una simile declamazione sul versante del regime probatorio a carico dell'attore, acclarata la natura di responsabilità aggravata del titolare del trattamento e definito il perimetro del suo onere probatorio ai fini di esonero. Si può, invero, condividere la posizione dell'Avvocato Generale, che, nelle sue conclusioni nel caso in

[18] Cass. civ., sez. un., 11 novembre 2008, nn. 26972-26975, in *Resp. civ*., 2009, 38, con nota di P.G. MONATERI ed E. NAVARRETTA; in dottrina v. ancora E. NAVARRETTA, *Il danno non patrimoniale*, Milano, 2010, spec. pp. 3-49; ID., *Diritti inviolabili e risarcimento del danno*, Torino, 1996, *passim*; V. ZENO-ZENCOVICH, *La responsabilità civile*, in AA.VV., *Diritto privato comparato. Istituti e problemi*, Roma-Bari, 2012, p. 371 ss.

esame, esclude la configurabilità, per quanto in oggetto, di un danno *in re ipsa*[19].

Più chiaramente, «quando uno degli obbiettivi della disposizione da interpretare è la protezione dell'individuo, o di una determinata categoria di individui, il concetto di danno deve essere ampio». Ma è anche vero che «una volta accertata l'esistenza della violazione e del nesso causale» non può sorgere il diritto al risarcimento «a causa di mere inquietudini, ansie e timori provati dalla persona interessata in merito ad un eventuale futuro uso improprio dei dati personali».

Occorre dunque distinguere tra "disagi e fastidi" e danno vero e proprio.

La "misurazione" di tale nozione non potrà che essere casistica e di conseguenza si rinnoverà l'incessante oscillazione del pendolo della responsabilità civile per il conseguimento di un desiderabile equilibrio (instabile per definizione) tra eccessiva e ridotta tutela.

[19] Per la voce di danno non patrimoniale la dimostrazione dell'elemento aggiuntivo della lesione di un diritto costituzionalmente rilevante. Cfr. Cass., sez. VI, 11 gennaio 2016, n. 222, inedita, per cui il danno non patrimoniale risarcibile, per quanto determinato da una lesione del diritto fondamentale alla protezione dei dati personali (tutelato dagli artt. 2 e 21 cost. e dall'art. 8 Cedu) «non si sottrae alla verifica della "gravità della lesione"» e della «serietà del danno "inteso" quale perdita di natura personale effettivamente patita dall'interessato». Per una disamina complessiva relativa alla disciplina del danno non patrimoniale da violazione della normativa in materia di protezione dei dati personali v. E. TOSI, *Responsabilità per illecito trattamento dei dati personali e danno non patrimoniale*, Milano, 2019, *passim*.

Diritto Mercato Tecnologia

Numeri Speciali

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

2017 Il Mercato Unico Digitale
a cura di Gianluca Contaldi

2018 La Ricerca su Materiali Biologici di Origine Umana:
Giuristi e Scienziati a confronto
a cura di Alberto M. Gambino, Carlo Petrini e Giorgio Resta

2019 La Tassazione dell'Economia Digitale tra Sviluppi Recenti
e Prospettive Future
a cura di Alessio Persiani

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

ISSN (Online Edition): 2239 -7442