ACTUALIDAD JURIDICA IBEROAMERICANA

IDIBE
Instituto de Derecho Iberoamericano

tirant lo blanch

Cátedra de Derecho Notarial de la Universidad de Alicante

ACTUALIDAD JURÍDICA IBEROAMERICANA / EDICIÓN SEMESTRAL / FEBRERO 2023 / VALENCIA-ESPAÑA

Publicación de circulación Internacional
Actualidad Jurídica Iberoamericana
https://www.revista-aji.com

Editan:
Instituto de Derecho Iberoamericano.
C/ Luis García Berlanga, núm. 7, 1-15 Valencia, España. 46023.
Correo Electrónico: contacto@idibe.org
web: www.idibe.org

Tirant lo Blanch.
C/Artes Gráficas, 14, 46010 Valencia (España).
Telf. +34 963 61 00 48.
Correo electrónico: tlb@tirant.com
web: www.tirant.com

ISSN 2386-4567

Actualidad Jurídica Iberoamericana se encuentra indexada en los siguientes índices de calidad: REDIB, ANVUR, LATINDEX, CIRC, MIAR y SCOPUS.

Así mismo se encuentra incluida en los siguientes catálogos: Dialnet, RODERIC, Red de Bibliotecas Universitarias (REBIUN), Ulrich's, Dulcinea.

Impreso en España
Diagramación: Elias On - elias.on@live.com

DALLA RESPONSABILITÀ CIVILE ALLA RESPONSABILITÀ SOCIALE D'IMPRESA NELLA PROTEZIONE DEI DATI PERSONALI: ALLA RICERCA DEL RIMEDIO EFFETTIVO

FROM CIVIL LIABILITY TO CORPORATE SOCIAL RESPONSIBILITY IN THE PROTECTION OF PERSONAL DATA: IN SEARCH OF THE EFFECTIVE REMEDY

Actualidad Jurídica Iberoamericana Nº 18, febrero 2023, ISSN: 2386-4567, pp. 658-685

Alessandro
BERNES

ARTICOLO CONSEGNATO: 11 de octubre de 2022
ARTICOLO APPROBATO: 5 de diciembre de 2022

ABSTRACT: Il mutato approccio di gestione del rischio ex ante nel trattamento di dati personali, attraverso una valutazione preventiva e basata sul possibile pregiudizio che l'uso dei dati personali può determinare in capo all'interessato (accountability), si riflette anche sul ruolo assunto dalla responsabilità (liability) del titolare del trattamento per violazione della disciplina della data protection causativa di danno e del tradizionale strumento del risarcimento, quale rimedio ex post. Un'indagine in tal senso fa sorgere il dubbio sull'effettività della tutela per equivalente, specie nel caso di lesioni modeste, le cui gravità e serietà non possono essere comprese se non nella loro dimensione "massiva" e "sociale", rivolgendosi piuttosto lo sguardo verso altri "provvedimenti risarcitori", alla luce delle recenti normative in tema di tutela dei diritti degli utenti digitali.

PAROLE CHIAVE: Responsabilità; illecito; responsabilizzazione; dati personali; rischio; rimedio; danno; sociale.

ABSTRACT: *The new risk-based approach in the processing of personal data, due to a prior assessment on the possible harms that data processing may cause to the data subject (accountability), it is also reflected in the liability of the data controller for the infrigements of the regulation causing a damage. This relationship points out also the ineffectiveness of the he compensatory remedy in the case of modest injuries, whose gravity and seriousness have to be seen in their "massive" and "social" dimension. Hence, it should be possibile to move from a compensatory remedy to other "redress measures", in the light of recent regulations on the protection of users' digital rights.*

KEY WORDS: *Responsability; liability; accountability; personal data; risk; remedy; social; damage.*

SOMMARIO.- I. UNA PREMESSA.- II. L'AMBIGUITÀ DELLA "RESPONSABILITÀ" NEL GDPR.- III. LA CONNESSIONE FRA *LIABILITY E ACCOUNTABILITY*.- IV. UNA TERZA ACCEZIONE DI "RESPONSABILITÀ" (SOCIALE?).- V. ALLA RICERCA DI UN RIMEDIO EFFETTIVO.- VI. DAL RISARCIMENTO DEL DANNO AI "PROVVEDIMENTI RISARCITORI".

I. UNA PREMESSA.

Sicuramente il Regolamento n. 679/2016/UE (di seguito, il "GDPR"), esito di lunghi lavori preparatori, si è prefisso un obiettivo ambizioso: mutare l'approccio relativo alla gestione delle attività costituenti trattamento dei dati personali nei termini di prevenzione dei rischi e, solo in subordine, di riparazione dei danni eventualmente cagionati[1]. In particolare, si riconosce oggi al soggetto che determina le finalità e i mezzi del trattamento di dati personali – il titolare – un potere-dovere di "auto-controllo" quanto al rischio del verificarsi di possibili pregiudizi in capo alle persone fisiche-interessati, superando la logica previgente del mero adempimento formale agli obblighi di legge ovvero dell'eventuale autorizzazione al trattamento ad opera dell'*authority* di supervisione[2]. Ciò è reso possibile attraverso l'introduzione di un complesso sistema di norme e strumenti anche tecnici, volti a garantire un monitoraggio non solo preventivo, ma anche continuo dei pericoli inerenti all'uso dei dati personali.

Le molte novità introdotte dal GDPR inducono senz'altro l'interprete ad uno sforzo di coerenza sistematica anche con riguardo al significato da attribuire alla "responsabilità", ascrivibile al titolare del trattamento di dati personali. In queste brevi considerazioni su un tema sicuramente molto ampio, l'attenzione sarà riposta su alcuni aspetti, particolarmente interessanti, relativi alla polisemia del termine "responsabilità", apparentemente riscontrabile nella traduzione italiana del GDPR[3]. Per un verso, infatti, "responsabilità" sembra richiamare il tradizionale istituto che regola le conseguenze di un fatto illecito, in base ad un'allocazione dei costi tra soggetti, quando si afferma che chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere

1 Per tutti, Finocchiaro, G.: "Introduzione al Regolamento europeo sulla protezione dei dati", *Nuove leggi civ. comm.*, 2017, p. 10 ss.

2 Vedi Califano, L.: "Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali", in *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679* (a cura di L. Califano e C. Colapietro), Editoriale Scientifica, Napoli, p. 34 ss.

3 Sottolinea come «problemi di traduzione esistono, ogni lingua ha dei termini difficilmente traducibili» Lucchini Guastalla, E.: "Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori", *Contr. e impr.*, 2018, p. 121.

• Alessandro Bernes
Ricercatore di Diritto privato, Università Ca' Foscari Venezia
alessandro.bernes@unive.it

il risarcimento del danno[4]. Diversamente, la medesima espressone è altrove utilizzata con un'accezione di sintesi circa l'obbligo, cui è tenuto il titolare del trattamento, di predisporre misure tecniche ed organizzative adeguate alla protezione dei dati personali, basate sui principi di prevenzione e precauzione[5]. Ancora, è possibile scorgere, tra le norme del Regolamento, un'apertura ad altri, possibili significati del termine "responsabilità", muovendo da una logica preventiva verso l'agire responsabile, prossimo alla – dibattuta – categoria della responsabilità sociale d'impresa. In altre parole, il mutato *risk-based approach* sembra riflettersi pure sulla "responsabilità" del titolare del trattamento verso la società, anche a prescindere dalla violazione della disciplina della *data protection* ovvero dalla causazione di un certo danno[6].

Un'indagine in tal senso fa sorgere qualche dubbio circa l'effettività, o meglio, l'idoneità della forma di tutela sanzionatoria *ex post* e del relativo rimedio, il risarcimento per equivalente, in una prospettiva di anticipazione della protezione della persona fin dalla "progettazione" del trattamento. Ci si deve chiedere, quindi, se non sia più opportuno ripensare – sempre in un'ottica di diritto privato – a qualche forma di riparazione in forma specifica, molte volte più semplice da realizzare nei rapporti digitali che nel mondo reale, oggi rinvenibile, per il vero, nella disciplina relativa alla fornitura di servizi e contenuti digitali (Dir. 2019/790/UE) e delle azioni collettive (Dir. 2020/1828/UE). Così, il "materializzarsi" del rischio sembra non trovare per forza la principale azione avverso gli effetti dannosi nel risarcimento del danno, in base alle regole della responsabilità (soltanto) in senso civilistico.

II. L'AMBIGUITÀ DELLA "RESPONSABILITÀ" NEL GDPR.

È noto come un certo regime di responsabilità per danni derivanti (illecito) trattamento di dati personali è ravvisabile nell'art. 82 GDPR, rubricato "Diritto al risarcimento e responsabilità". Qui si prevede che «un titolare del trattamento (…) risponde per il danno cagionato dal suo trattamento che violi il presente regolamento» (par. 2), se non «dimostra che l'evento dannoso non gli è in alcun modo imputabile» (par. 3)[7]. Correlativamente «chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno» (par. 1)[8].

4 Art. 82 GDPR.

5 Art. 24 GDPR.

6 Hijmans, H.; Raab, C.: "Ethical Dimensions of the GDPR, AI Regulation, and Beyond", *Direito Público*, 2022, 18(100), p. 68.

7 Per esigenze di economia della trattazione, esula dalla presente indagine l'analisi dell'imputazione dell'illecito al responsabile del trattamento (*data processor*).

8 Il concetto di «violazione del Regolamento» è più ampio rispetto a quello riportato nell'art. 4(12) GDPR («"violazione dei dati personali": la violazione di sicurezza che comporta accidentalmente o in modo illecito

Va sottolineato come l'art. 82 GDPR si limiti a definire gli elementi principali del regime di responsabilità, lasciando aperta la questione relativa alla natura della stessa[9]. Non intendiamo qui soffermarci sulla discussa qualificazione giuridica di una siffatta responsabilità che, fin dall'entrata in vigore della precedente Direttiva n. 46/1995, interroga gli interpreti[10]. Invero, l'elemento principale di complessità deriva dalla compenetrazione fra il diritto europeo e i diritti nazionali[11]: un'interazione fisiologica, tenuto conto che la concreta applicazione di Direttive e Regolamenti richiede un adattamento interno degli ordinamenti nazionali e, in particolare, delle loro categorie[12]. Basti pensare che il criterio di imputabilità dell'illecito, contenuto nell'art. 82, par. 3, GDPR – per il quale il titolare è esonerato dalla responsabilità per i danni discendenti dalla violazione della normativa in materia di protezione di dati personali solo se dimostra che l'evento dannoso non gli è in alcun modo imputabile – è molto più vicino a quanto previsto, nel nostro ordinamento, dall'art. 1218 c.c. in materia di inadempimento delle obbligazioni, piuttosto che per la responsabilità civile[13]. Così, c'è chi sostiene che il regime di responsabilità delineato dall'art. 82 GDPR assuma natura "contrattuale", a prescindere dal fatto che il trattamento di dati personali si inserisca all'interno di un rapporto negoziale con l'interessato, come di frequente accade per i *social network*[14]. Altri ritengono, invece, sulla scorta del pregresso dato normativo contenuto nell'art. 15 Cod. privacy, si tratti di una

la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati»), abbracciando ogni ipotesi di mancata osservanza dei principi e delle regole stabilite dal Regolamento.

9 Sul punto, Ratti, M.: "La responsabilità da illecito trattamento di dati personali nel nuovo Regolamento", in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (a cura di G. Finocchiaro), Zanichelli, Bologna, 2017, p. 615 ss.

10 L'art. 23 della Dir. 46/95/CE lasciava agli Stati membri la definizione del regime di responsabilità per il danno cagionato da un trattamento illecito o 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 [oggi, titolare] del trattamento. Così, il legislatore italiano, già con l'art. 18, l. 31 dicembre 1996, n. 675, aveva previsto che chiunque cagionasse un danno ad altri per effetto del trattamento di dati personali fosse soggetto alla responsabilità per esercizio di attività pericolose di cui all'art. 2050 c.c. Tale disposizione è stata riprodotta nell'art. 15, d.lgs. 30 giugno 2003, n. 196 (c.d. Codice privacy), oggi abrogato in seguito all'adeguamento della normativa interna al GDPR, attraverso il d.lgs. 10 agosto 2018, n. 101. Per il regime previgente, si rinvia all'analisi di Franzoni, M.: "Responsabilità derivante da trattamento di dati personali", in *Diritto dell'informatica* (a cura di G. Finocchiaro e F. Delfini), Wolters Kluwer, Milano, 2014, p. 829 ss.

11 Camardi, C.: "Liability and Accountability in the "Digital" Relationships", in *Privacy and Data Protection in Software Services* (edited by R. Senigaglia, C. Irti e A. Bernes), Springer, Singapore, 2022, p. 25, la quale rileva come a fronte del diritto eurounitario e a dispetto del suo primato e della sua costante forza uniformatrice, si apre sempre un processo potenzialmente controverso di applicazione nelle diverse realtà nazionali.

12 Il superamento della tradizionale distinzione tra responsabilità contrattuale e extracontrattuale nella disciplina europea, peraltro, è stato già evidenziato da Lipari, N.: *Le categorie del diritto civile*, Giuffré, Milano, 2013, p. 199: «[n]on avrebbe quindi rilievo, operando sulla spunta dei vecchi schemi categoriali, evidenziare, ad esempio, che la responsabilità del produttore è responsabilità di tipo extracontrattuale se poi la medesima responsabilità, con conseguente applicazione della medesima disciplina, può essere attivata anche da chi, in ipotesi, abbia acquistato direttamente dal produttore. Inversamente assumere che la responsabilità del prestatore di servizi sia una responsabilità contrattuale perde qualsiasi rilievo classificatorio se poi la medesima azione può essere esercitata anche dal terzo estraneo che ha risentito del danno».

13 Sulla ambiguità in cui è incorsa la giurisprudenza nell'applicazione dell'art. 15 Cod. privacy, vedi Bilotta, F.: "La responsabilità civile nel trattamento dei dati personali", in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato* (a cura di R. Panetta), Giuffré, Milano, 2019, p. 452 ss.

14 Bilotta, F.: "La responsabilità civile nel trattamento dei dati personali", cit., p. 453.

responsabilità extracontrattuale, *sub-specie iuris* di esercizio delle attività pericolose (art. 2050 c.c.)[15]. Interessante, ancora, l'opinione di chi enfatizza la natura "ancipite" della responsabilità in esame, a cavallo cioè tra contrattuale ed extracontrattuale, rinvenendo la fonte degli obblighi (informativi e di protezione), gravanti sul titolare del trattamento, in un fatto (o un atto) contemplato dalla legge, rinviando all'ultima parte dell'enunciato normativo di cui all'art. 1173 c.c.[16].

Ad ogni modo, come si accennava, la scelta qualificatoria e, di conseguenza, la disciplina applicabile appare questione di poco rilievo, dal momento che i molti profili rilevanti della responsabilità per danni discendenti da un illecito trattamento sono comunque regolamentati dallo stesso art. 82 GDPR[17]. Del resto, la filosofia del legislatore europeo è quella di assicurare in ogni caso la riparazione dei danni subiti in presenza di una violazione di una norma del Regolamento, prescindendo dalla fonte negoziale o meta-negoziale del danno[18]. Più problematica è, come si avrà modo di vedere, la questione relativa all'utilità pratica del rimedio risarcitorio (per equivalente) che viene accordato all'interessato-danneggiato; ciò, di fatto, può condizionare la volontà degli interessati ad agire per chiedere il ristoro dei danni dinanzi all'autorità giudiziaria, con gli oneri (e i costi) che tutto questo comporta.

Al fine di comprendere il significato (complesso) del termine "responsabilità", l'art. 82 deve essere coordinato con le altre norme del Regolamento e, in particolare, quelle che disciplinano gli obblighi cui sono chiamati i soggetti che eseguono operazioni costituenti trattamento dei dati personali. Nella traduzione italiana del GDPR, infatti, la medesima espressione "responsabilità" viene impiegata non solo nella norma dove si riconosce al danneggiato il risarcimento del danno patito, ma anche nella rubrica dell'art. 24 ("Responsabilità del titolare del trattamento").

Stando al dettato normativo da ultimo ricordato, «[t]enuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché

15 Per tutti Gambini, M.: "Responsabilità e risarcimento nel trattamento di dati personali", in *I dati personali nel diritto europeo* (V. Cuffaro, R. D'Orazio e V. Ricciuto), Giappichelli, Torino, 2019, p. 1057, laddove parla, in riferimento all'art. 82 GDPR, di una responsabilità aquiliana basata sulla colpa ma aggravata da una presunzione di colpa. Diversamente, conclude per l'esistenza di una responsabilità oggettiva basata sul rischio dell'attività di trattamento, Tosi, E.: *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Giuffrè, Milano, 2019, p. 125 ss.

16 Cfr. Bravo, F.: "Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali", in *Persona e mercato dei dati. Riflessioni sul GDPR* (a cura di N. Zorzi-Galgano), Cedam-Wolters Kluwer, Padova-Milano, 2019, p. 402, il quale rileva che tra il titolare e l'interessato può comunque insorgere (e nella pratica ciò avviene) un rapporto di natura contrattuale. Parla invece di obbligazioni *ex lege* Piraino, F.: "Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato", *Nuove leggi civ. comm.*, 2017, p. 389.

17 Rimangono aperti profili come il termine di prescrizione dell'azione risarcitoria o, ancora, il tema della prevedibilità del danno ai sensi dell'art. 1225 c.c., comunque facilmente risolvibili, come sottolineato da Thobani, S.: "Commento all'art. 82", in *Commentario al Codice civile* (diretto da E. Gabrielli), *Delle persone* (a cura di A. Barba e S. Pagliantini), *Leggi collegate*, II, Utet- Wolters Kluwer, Milano, 2019, p. 1238 ss.

18 Lipari, N.: *Le categorie del diritto civile*, cit., p. 199, secondo il quale «[n]ella misura in cui le rispettive categorie classificatorie possano risultare ancora utili esse andranno dimensionate a posteriori in funzione di particolari esigenze ricostruttive».

dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento». Così, il titolare è tenuto a predisporre l'adozione di misure giuridiche, organizzative, tecniche e di sicurezza più opportune per garantire che il trattamento sia effettuato in conformità al GDPR e tali da prevenire il rischio di possibili lesioni dei diritti e delle libertà fondamentali delle persone fisiche[19]. Parimenti, il titolare deve, in modo costante, riesaminare e aggiornare queste misure – compresa la loro efficacia – qualora si renda necessario, nonché conservare, in modo documentato, le relative prove. In altri termini, l'obbligo di adozione di determinate misure e quello di dimostrare la conformità del trattamento rappresentano due facce della stessa medaglia per il titolare del trattamento, al quale è affidato un ruolo "pro-attivo" nella valutazione e nella gestione dei pericoli connessi alle sue attività. In questo ordine di senso, il significato di "responsabilità" è meglio rappresentato dal termine, rinvenibile nell'art. 5 GDPR, "responsabilizzazione" (*accountability* nella versione inglese, mentre si parla di *liability* con riferimento a quanto detto in precedenza in merito alla responsabilità per danni[20]), il quale sintetizza, appunto, l'approccio basato sul rischio e riassume il rispetto dei principi generali applicabili al trattamento di dati personali che il titolare deve rispettare ed essere in grado di comprovare[21].

Più nello specifico, il GDPR introduce tutta una serie di (nuovi) istituti che si ascrivono a questa chiara logica "responsabilizzante" del titolare del trattamento, con una ovvia ricaduta in termini di obblighi, doveri e oneri in capo a questo[22]. Si pensi, oltre ai principi generali del trattamento (art. 5), alle disposizioni relative al consenso (artt. 7 e 8), alle informazioni obbligatorie da rendere all'interessato

19 Ciò, si badi bene, a prescindere dalla sussistenza di un rapporto contrattuale intercorrente fra il titolare del trattamento e l'interessato, in quanto doveri sorti *ex lege*.

20 Invero, l'ambiguità semantica del termine "responsabilità" sembra sciogliersi nella versione inglese del Regolamento, ove si parla di *responsability* o, meglio, di *accountability* nella prima ipotesi, mentre di *liability* nell'ipotesi del risarcimento dei danni subiti dall'interessato. Stando al parere n. 3/2010 sul principio di responsabilità del Gruppo di lavoro Articolo 29 per la protezione dei dati, «[i]l termine inglese "accountability" (responsabilità) proviene dal mondo anglosassone, dove è di uso comune e dove il suo significato è ampiamente compreso e condiviso. Ciononostante, risulta complesso definire che cosa esattamente significhi "accountability" in pratica. In generale, comunque, l'accento è posto sulla dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità. (…) Nella maggior parte delle altre lingue europee, principalmente a causa delle differenze tra i sistemi giuridici, il termine "accountability" non è facilmente traducibile. Di conseguenza, il rischio di un'interpretazione variabile del termine, e quindi di una mancanza di armonizzazione, è sostanziale. Altri termini che sono stati suggeriti per rendere il senso di "accountability" sono: "reinforced responsibility" (responsabilità rafforzata), "assurance" (assicurazione), "reliability" (affidabilità), "trustworthiness" (attendibilità) e, in francese, "obligation de rendre des comptes" (obbligo di rendere conto) ecc. Si potrebbe altresì inferire che "accountability" si riferisce alla "attuazione dei principi relativi alla protezione dei dati"».

21 La "responsabilizzazione" ha, infatti, una duplice valenza: quella di spingere il titolare del trattamento ad adottare tutte le misure utili a prevenire atti e comportamenti su dati personali che possano impattare sugli interessati, in termini di gravità e probabilità; nonché quella di documentare quanto fatto, anche in chiave probatoria, a fronte di violazioni effettive o controlli da parte delle autorità indipendenti, così Califano, L.: "Il Regolamento UE 2016/679", cit., p. 35.

22 Finocchiaro, G.: "Il principio di accountability", *Giur. it.*, 2019, p. 2778 ss.

(art. 12 ss.), ai comportamenti obbligatori dovuti in seguito all'esercizio dei diritti dell'interessato (artt. 15-22), agli obblighi di predisposizione delle misure tecniche e organizzative in tema di protezione dei dati personali fin dalla progettazione e per impostazioni predefinita (art. 25), al registro del trattamento (art. 30), alle misure di sicurezza (art. 32), alle previsioni in materia di *data breach* (artt. 33 e 24), alle norme sulla valutazione d'impatto (artt. 35 e 36), e via dicendo, compresa l'adozione di misure atipiche (o innominate), ove l'adeguatezza della scelta spetta comunque al titolare. In sostanza, la disciplina del GDPR determina in ampia misura quali siano e in caso consistano gli obblighi, aventi natura procedimentale, in favore della persona a cui i dati si riferiscono e, al contempo, individua quale sia il soggetto gravato da tali obblighi.

È chiara, dunque, la scelta politica del legislatore europeo: prima ancora che sulla responsabilità per i danni eventualmente sofferti dall'interessato e a prescindere dal verificarsi degli stessi, è opportuno stabilire una «responsabilità generale» (*recte* fisiologica e non anche patologica) del titolare del trattamento, quanto agli obblighi che (per legge[23]) sorgono in ragione di qualsiasi trattamento di dati personali che questi abbia effettuato direttamente o che altri soggetti abbiano effettuato per suo conto, nell'ambito della struttura organizzativa[24]. Una prospettiva, questa, che senz'altro anticipa il momento temporale di origine dei bisogni di tutela degli interessati, in base ad un approccio basato sul rischio, di analisi e gestione dello stesso. In questo senso, l'esercizio dei diritti da parte del singolo interessato (accesso, cancellazione, opposizione, etc.), oltre all'eventuale ricorso all'autorità giudiziaria (risarcimento del danno) ovvero alla richiesta di intervento dell'autorità di controllo, si mostrano soltanto come alcuni dei possibili strumenti di reazione ai possibili pericoli che possono manifestarsi in costanza di un trattamento di dati personali.

III. LA CONNESSIONE FRA *LIABILITY* E *ACCOUNTABILITY*.

Entrambe le accezioni dell'espressione tradotta (impropriamente) come "responsabilità" nel GDPR richiamano la situazione di un soggetto che è obbligato a fare qualcosa oppure ne deve in qualche misura rispondere, sia pur in base a presupposti e condizioni diverse. Più precisamente, l'interessato può pretendere, già prima che si verifichi la violazione del Regolamento, la (piena) attuazione del dovere di protezione indicato negli artt. 5 e 24 GDPR: la responsabilità del titolare

23 Bravo, F. "Riflessioni critiche sulla natura della responsabilità da trattamento illecito", cit., p. 397, nonché p. 403: «(…) la "legge" prevede che, in conseguenza della predisposizione del trattamento di dati personali – rilevante quale "fatto" giuridico – sorgano in capo al titolare del trattamento una serie di obblighi funzionali alla protezione dei dati personali, per esigenze di tutela della persona fisica a cui i dati trattati si riferiscono».

24 In questi termini si esprime il *considerando* § 74 GDPR.

è, ancor prima che per danni, una responsabilità di ordine procedurale[25]. Nel caso in cui si verifichi, poi, un illecito trattamento di dati personali produttivo di danno (patrimoniale e non), il danneggiato è legittimato ad agire a norma dell'art. 82 GDPR. Di conseguenza, la ricorrenza di un obbligo risarcitorio non dipende solamente da quanto è accaduto durante o al termine del trattamento, ma anche da ciò che è successo prima ancora di iniziarlo, a fronte cioè della mancanza o dell'inidoneità delle misure tecniche ed organizzative che avrebbero potuto-dovuto prevenire il danno. In questo senso, stante l'obbligo di adozione di determinate misure – il cui oggetto è specificamente contemplato dalle norme del Regolamento, ma non anche il contenuto delle stesse – e la necessità di dimostrarne l'adeguatezza in relazione allo specifico trattamento posto in essere, sembra determinarsi una vera e propria inversione dell'onere probatorio quanto al regime di responsabilità di cui all'art. 82 GDPR[26]: il danneggiato, infatti, può limitarsi ad allegare il rapporto sottostante – il trattamento di dati personali – e la violazione delle norme del Regolamento, provando il danno e il nesso causale[27]; all'opposto, seguendo la scansione dettata dagli artt. 5, 24 e 82 GDPR, è il titolare a dover dimostrare che il trattamento è lecito ovvero, se la violazione si è verificata, che essa è dipesa da cause a lui non imputabili[28]. Sicché il titolare del trattamento non risponde del danno non prevedibile e contenibile con l'adozione delle misure atte a limitarlo, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

L'aver lasciato un ampio margine di discrezionalità per le scelte che il titolare del trattamento compie non può che determinare delle conseguenze connesse alla non diligente esplicazione dell'autonomia riconosciuta dal legislatore[29]. La valutazione di adeguatezza (arg. *ex* art. 24 GDPR) delle misure da implementare ovvero delle azioni da intraprendere sembra rievocare, infatti, il noto criterio della diligenza della

25 Camardi, C.: "Note critiche in tema di danno da illecito trattamento dei dati personali", *Jus Civile*, 2020, p. 796, ove si sottolinea come «il titolare deve premunirsi delle prove necessarie a dimostrare l'adozione di queste misure e la conformità della sua organizzazione al modello operativo del regolamento, e ciò, ancora una volta, indipendentemente dalla concreta causazione di un danno: tanto esplicitamente dispone il già menzionato art. 24 del GDPR».

26 Così Bilotta, F.: "La responsabilità civile nel trattamento dei dati personali", cit., p. 461, il quale giunge a qualificare, peraltro, la responsabilità per illecito trattamento di dati personali come una responsabilità per inadempimento di natura oggettiva: «se il danno si verifica, è del tutto inconferente il grado di colpevolezza che ha caratterizzato la loro condotta: potremmo definirla una responsabilità per pura causalità».

27 La violazione del regolamento è solo condizione necessaria, ma non sufficiente per la condanna risarcitoria. Cfr. Cass. 17 settembre 2020 n. 19328, *Nuova giur. civ. comm.*, 2021, p. 142 ss., con nota di Solinas, C.: "Danno non patrimoniale e violazione del diritto alla protezione dei dati personali", ove si evidenzia che, nel caso di illecito trattamento dei dati personali il danno, sia patrimoniale che non patrimoniale, non può essere considerato *in re ipsa*, per il fatto stesso dell'esercizio dell'attività pericolosa, ma deve essere sempre oggetto di allegazione e di prova. Sul punto, ampiamente, Camardi, C.: "Note critiche in tema di danno da illecito trattamento dei dati personali", cit., p. 786 ss.

28 Thobani, S.: "Commento all'art. 82", cit., p. 1234.

29 Ciò vale in riferimento delle conseguenze delle scelte effettuate, quindi anche in termini sanzionatori e risarcitori.

prestazione cui è tenuto il debitore (art. 1176 c.c.)[30]. Anzi, la discrezionalità attribuita al titolare del trattamento (*recte* la sua auto-responsabilità) è ulteriormente specificata nel Regolamento, essendo libera ma allo stesso tempo non illimitata[31]: la conformità al GDPR è basata non solo sul principio di proporzionalità e ragionevolezza, bensì soggetta ad ulteriori condizioni, come la natura, l'ambito di applicazione, il contesto, le finalità del trattamento, nonché il rischio di lesione dei diritti e delle libertà fondamentali della persona[32]. Ed invero la prova della non imputabilità dell'evento dannoso, prevista dall'art. 82, par. 3, GDPR, richiede che il titolare del trattamento non dimostri tanto la mancata violazione delle norme del Regolamento, bensì, in positivo, che le misure tecniche, organizzative e di sicurezza predisposte corrispondano, nel metodo e nei contenuti, a ciò che in base al contesto, ai costi, alle finalità e via dicendo, poteva essergli richiesto[33]. È evidente come questa lettura valorizzi grandemente il principio di *accountability*: il titolare del trattamento può andare esente da ogni responsabilità per danni alla esibizione di certificazioni o documentazioni riguardanti l'avvenuta adozione di tutte le misure tecniche e organizzative idonee a prevenire l'evento dannoso in seguito lamentato dall'interessato, mentre risponderà dei danni derivanti dalla non adozione di altre misure tecnicamente possibili e proporzionate alle risultanze della (errata o mancata) valutazione effettuata[34].

Si conferma allora la scansione temporale individuata dal legislatore europeo, che anticipa per quanto possibile l'eventuale tutela risarcitoria *ex post*, richiedendo già l'adozione *ex ante* di misure preventive e precauzionali – di concerto alle altre previsioni incentrate sulla gestione del rischio (*data protection by design* e *by default*, valutazione d'impatto, etc.) – atte a prevenire possibili pregiudizi per gli interessati al trattamento[35]. La disciplina in materia di protezione dei dati personali, quindi, è in larga parte fondata su doveri di comportamento del titolare, dando luogo ad un modello di tutela non necessariamente risarcitorio[36]. In tal senso, l'approccio

30 Sul punto, Gambini, M.: "Algoritmi e sicurezza", *Giur. it.*, 2019, p. 1737. *Contra* Bravo, F.: "Riflessioni critiche sulla natura della responsabilità da trattamento illecito", cit., p. 417, individua il parametrio per la valutazione dell'adeguatezza della misura adottata dal titolare del trattamento, più che nel criterio diligenza nell'adempimento delle obbligazioni *ex* art. 1176 c.c., nei «contenuti oggettivamente esigibili dell'obbligo imposto dalla legge: è cioè un parametro oggettivo per valutare il "risultato" atteso dal legislatore nell'assicurare lo standard di protezione, che lo stesso GDPR ha inteso ancorare a parametri oggettivi (…)».

31 In argomento, Perlingieri, P.: "*Privacy* digitale e protezione dei dati personali tra persona e mercato", *Foro nap.*, 2018, p. 482 ss.

32 Artt. 24, 25, 28, 32, 35 GDPR.

33 Salva ovviamente la prova della non imputabilità stessa dell'evento dannoso ovvero del caso fortuito.

34 Di questo avviso Camardi, C.: "Note critiche in tema di danno", cit., p. 797.

35 Nel senso che la responsabilità in senso civilistico è solamente una delle epifanie dell'*accountability*, v. Tosi, E.: *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, cit., p. 52 ss.

36 Le tendenze della "responsabilità civile europea" sono ben esplicitate in Alessi, R.: "Il difficile percorso della «responsabilità civile europea»", *Danno resp.*, 1999, p. 377, secondo la quale la responsabilità offre ristoro all'interesse e al danno del "chiunque", poiché il risarcimento di tale danno costituisce occasione e strumento per affermare regole di comportamento, di protezione, di diligenza, destinate a regolare la presenza sul mercato di determinanti soggetti e attività.

basato sul rischio individua un primo "rimedio" efficace contro la lesione dei diritti della persona in un vero e proprio procedimento, nel quale devono essere valutate una serie di misure, sia pur sulla base di una regola di auto-responsabilità[37].

Ad ogni modo, se la mancata o inesatta adozione di certe misure (giuridiche, tecniche ed organizzative) *adeguate* dà sicuramente luogo ad una violazione dei principi e delle regole poste per il trattamento (legittimo) di dati personali, nella responsabilità per danni occorre altresì che si produca una qualche lesione dell'interesse individuale della persona fisica che lamenta delle conseguenze pregiudizievoli[38]. Infatti, oltre al *vulnus* dei diritti fondamentali della persona (identità, reputazione, riservatezza, ecc.), «il trattamento [illecito] può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati» (*considerando* § 75 del GDPR). Un quadro, questo, che testimonia comunque una certa consapevolezza del legislatore europeo dell'elevata pericolosità dell'attività di trattamento dei dati personali e del potenziale offensivo dei diritti dell'interessato generato dalle tecnologie digitali, anche in prospettiva sociale e che supera la posizione del singolo individuo[39].

37 Nel senso che il GDPR introduce una serie di «obblighi di natura procedimentale e non di obblighi finali, ossia di obblighi che, isolatamente considerati, non attribuiscono all'interessato una specifica utilità, ma che proiettano comunque la relazione tra questi e il titolare e il responsabile del trattamento nella dimensione del rapporto obbligatorio», Piraino, F.: "Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato", cit., p. 390.

38 Soprattutto per i pregiudizi che attengono alla sfera non patrimoniale della persona. Sul punto, Cass., 4 giugno 2018, n. 14242, *Giur. it.*, 2019, p. 43 ss., con nota di Thobani, S.: "Il danno non patrimoniale da trattamento di dati tra danno presunto e danno evento", ove si afferma che «[i]l danno non patrimoniale risarcibile (…) pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali tutelato dagli artt. 2 e 21 Cost. e dall'art. 8 della CEDU, non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno" (quale perdita di natura personale effettivamente patita dall'interessato), in quanto anche per tale diritto opera il bilanciamento con il principio di solidarietà ex art. 2 Cost., di cui il principio di tolleranza della lesione minima è intrinseco precipitato, sicché determina una lesione ingiustificabile del diritto non la mera violazione delle prescrizioni poste dall'art. 11 del codice della privacy ma solo quella che ne offenda in modo sensibile la sua portata effettiva».

39 Camardi, C.: "Note critiche in tema di danno", cit., p. 788.

IV. UNA TERZA ACCEZIONE DI "RESPONSABILITÀ" (SOCIALE?).

Si è detto come il trattamento dei dati personali rappresenti un'attività dall'alto potenziale tecnico, la quale richiede di valutare preventivamente la probabilità e la gravità del verificarsi del rischio di possibili pericoli in capo agli interessati e prevenire *vulnus* connessi alle libertà e ai diritti fondamentali della persona che possono esserne pregiudicati. Guardando più attentamente all'applicazione pratica delle regole espressione dell'*accountability*, il complesso sistema del Regolamento, per il vero, sembra andare oltre al concetto di responsabilità in senso civilistico, sia esso relativo ad un illecito ovvero alla esecuzione di taluni obblighi di condotta. In particolare, alle volte il trattamento necessita, nel caso concreto, di precauzioni che vanno al di là di quelle adottate per la *compliance* del settore di riferimento; perciò, l'obbligo di adozione delle misure tecniche ed organizzative può non coincidere con una certa previsione legalmente imposta. Viene da chiedersi, quindi, fino a che punto i titolari del trattamento possano essere chiamati ad implementare misure che vadano oltre al mero rispetto "formale" delle prescrizioni del GDPR, cioè che siano realmente efficaci per la protezione della comunità degli utenti[40].

Nella disamina del significato di "responsabilità" del titolare del trattamento si inserisce, pertanto, una terza e diversa accezione: fondare a carico dei titolari del trattamento l'adozione di determinate misure (tecniche, organizzative e di sicurezza) commisurate pure all'aspettative di coloro dei cui dati si tratta, per certi versi, rievoca la discussa figura della responsabilità sociale d'impresa[41].

L'ottica in cui ci si pone qui va ben oltre l'idea di rispetto della normativa – intesa come livello "minimo" di partenza – per stimolare invece un orientamento "pro-attivo" in tutti i sensi, di impulso volontario e virtuoso, da parte degli stessi protagonisti dell'ambiente digitale, nella direzione di un governo socialmente responsabile delle loro attività[42]. Del resto, il concetto "classico" di azienda, operante secondo criteri di economicità per conseguire una certa utilità, oggi deve confrontarsi con la minimizzazione dei costi sociali e valorizzazione degli impatti positivi, quale presupposto per garantire proprio la migliore *performance*

40 Quelle, C.: "Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach", *Eur. Journal of Risk Regulation*, 2018, 9, p. 502 ss.

41 Stante l'impossibilità di dar conto di una letteratura vastissima sull'argomento, per una sintesi delle questioni giusprivatistiche connesse alla *Corporate Social Responsibility*, Bellisario, E: "La responsabilità sociale delle imprese fra autonomia e autorità privata", *Danno e resp.*, 2013, p. 809 ss., nonché il volume Alpa G., Conte G. (a cura di): *La responsabilità dell'impresa*, Giuffrè, Milano, 2015; ma cfr. altresì, di recente, la disamina di Bevivino, G.: *La responsabilità sociale delle imprese. Strumenti attuativi e rimedi*, Esi, Napoli, 2018, p. 65 ss., nonché Bertelli, F.: *Le dichiarazioni di sostenibilità nella fornitura dei beni di consumo*, Giappichelli, Torino, p. 20 ss.

42 Sul punto, basti osservare come Libro Verde dell'Unione Europea del 18 luglio 2001, intitolato "Promuovere un quadro europeo per la responsabilità sociale d'impresa", dal quale si evince come un comportamento imprenditoriale socialmente responsabile non si risolve nel semplice rispetto degli obblighi normativi ma richiede un maggiore investimento nel capitale umano, nell'ambiente e negli altri rapporti con le parti interessate.

d'impresa, basata sulle (incrementate) potenzialità del mercato digitale. In altri termini, all'operatore economico è richiesto non solo di non provocare alcun danno (fonte di responsabilità) ovvero evitare che possa prodursi, ma anche di contribuire alla realizzazione di certe esternalità positive, adottando misure, strategie, processi e azioni che tengano conto del rispetto della persona[43]. Più nello specifico, il fine perseguito dalla *data protection* è quello di massimizzare i benefici derivanti dalla circolazione dei dati per la collettività e, al contempo, ridurre i rischi legati allo sviluppo di tecnologie, soprattutto per i diritti e le libertà fondamentali della persona[44].

È evidente allora la dimensione "sociale" del trattamento dei dati personali, declinabile in un'attenta analisi del profilo del rischio nell'adozione di determinate misure (tecniche, organizzative e di sicurezza) da parte del titolare. Anzi, è proprio lo stesso paradigma dell'*accountability* a ritenersi frutto di una "giuridificazione" della responsabilità sociale d'impresa, cioè del rendere vincolanti regole o impegni di matrice non legislativa[45]. Infatti, se si guarda al GDPR, e in particolare alla "responsabilizzazione", è possibile scorgere in capo al titolare del trattamento un obbligo – questo sì, giuridico – di diligenza professionale, correttezza e buona fede, nell'adozione delle misure richieste, che sembra andare oltre alla *mera* verifica di compatibilità con le disposizioni del Regolamento, nella direzione di una maggior tutela della persona e dei suoi diritti fondamentali. In sostanza, appare insufficiente che le misure adottate, in concreto, assicurino il semplice rispetto della normativa in materia; tali accorgimenti devono, invece, essere ulteriormente integrati, sia pur su base volontaria, allo scopo di garantire la massima efficacia pratica, in forza di una valutazione di opportunità compiuta dallo stesso titolare del trattamento[46]. In fin dei conti, la trasparenza e la serietà di una rigorosa valutazione e gestione del rischio rappresentano uno dei principali elementi di appetibilità delle imprese da parte degli utenti, poiché l'accresciuta consapevolezza dell'importanza dei dati personali sposta l'attenzione verso l'affidabilità degli operatori del mercato. Ciò rappresenta un elemento importante per fondare la base delle scelte dei potenziali clienti effettuano nel momento in cui si trovano a dover scegliere di quali prodotti o servizi avvalersi[47].

43 D'Ambrosio, M.: *Progresso tecnologico, "responsabilizzazione" dell'impresa ed educazione dell'utente*, Esi, Napoli, 2017, p. 118, per il quale è doveroso che le innovazioni portate dalla scienza e dalla tecnica rispondano anche al miglioramento della qualità dei rapporti umani, non solo alle logiche di impresa e del mercato.

44 Secondo Di Ciommo, F.: "Civiltà tecnologica e, mercato e insicurezza: la responsabilità del diritto", *Riv. crit. dir. priv.*, 2010, p. 590, per non ostacolare l'evoluzione tecnologica del mercato e la produttività delle imprese, l'unico principio che appare in grado di rispettare l'esigenza di promuovere tale evoluzione, a beneficio della collettività e, allo stesso tempo, ridurre al minimo i rischi derivanti dall'esposizione ai nuovi pericoli, è la responsabilità. A ciò si aggiunga che, negli ultimi anni, si assiste ad un drastico calo della fiducia nei mercati digitali, ad uno diffuso scontento circa la profilazione e ad una crescente domanda di "etica" per le imprese che operano nel settore.

45 Hijmans, H., Raab C.: "Ethical Dimensions of the GDPR, AI Regulation, and Beyond", cit., p. 68.

46 Gambini, M.: "Algoritmi e sicurezza," cit., p. 1737.

47 Califano, L.: "Il Regolamento UE 2016/679", cit., p. 39 ss., ove si sottolinea l'effetto benefico della capacità di fidelizzazione degli utenti e di accrescimento di competitività del mercato.

Non a caso, dunque, la scelta delle misure tecniche ed organizzative cui è tenuto il titolare del trattamento è improntata su certi criteri di adeguatezza, di proporzionalità e di ragionevolezza, che riflettono, sul piano giuridico, l'idea di un "agire responsabilmente", al fine di rendere effettiva, in pratica, la protezione dei dati personali. Ecco il perché del riferimento – rinvenibile, per esempio, negli artt. 24, 25, 32 GDPR – a tener in considerazione, nell'adozione delle misure, dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche[48].

D'altro canto, è evidente come l'*accountability* affianchi ad un profilo meramente giuridico una dimensione *latu sensu* etica che promuove un "decisionismo responsabile", il quale sia in grado di promuovere un dialogo rispettoso della legalità e della capacità di tutelare effettivamente la persona[49]. In altre parole, il GDPR sembra approdare – considerata l'evidente difficoltà per il diritto positivo di stare al passo con l'innovazione tecnologica – ad un "obbligo volontario", o meglio all'individuazione di un dovere di protezione della persona umana che conformi la stessa attività (e le modalità) di trattamento dei dati personali: è "responsabilità" dei titolari del trattamento quello di ridurre, prevenendoli, i costi, non solo economici ma anche sociali sopportati dalla collettività per i pericoli e i pregiudizi che possono derivare dall'utilizzo dei dati stessi.

Alla luce di quanto considerato, la "responsabilità" nel GDPR e, in particolare, l'*accountability* del titolare può assumere rilevanza sotto plurimi livelli: un primo è costituito da un obbligo di legge riconosciuto per tutti i titolari del trattamento, comprendente, in sintesi, l'attuazione di misure tecniche, giuridiche e organizzative "minime", nonché la conservazione delle relative prove (*accountability* in senso stretto); un secondo livello è quello relativo alla prova liberatoria della non imputabilità dell'evento al seguito del verificarsi di una violazione del Regolamento causativa di danno e fonte di responsabilità (*liability*); un terzo livello richiama, invece, la concretizzazione di sistemi di responsabilità di natura volontaria eccedenti le misure minime, in relazione ai principi fondamentali di protezione dei

48 Cfr. Bevivino, G.: "La responsabilità sociale delle imprese fra autonomia privata, nuovi obblighi di legge e prospettiva rimediale", in *Analisi giur. ec.*, 2018, p. 107, ove si sottolinea come più recente evoluzione normativa pare andare verso una progressiva «positivizzazione» di obblighi volti al soddisfacimento degli interessi degli *stakeholders* nello svolgimento dell'attività d'impresa o, più genericamente, tesi alla realizzazione delle istanze reclamate dalla *CSR*. Un ulteriore esempio, in tema di *data protection*, potrebbe essere quello introdotto in sede di modifica all'art. 166, co. 7, Cod. Privacy da parte del D.L. n. 139/2021 ("Decreto Capienze") – seppure in relazione al diverso profilo della determinazione delle sanzioni amministrative – per cui «il Garante può ingiungere il titolare del trattamento a realizzare campagne di comunicazione istituzionale volte alla promozione della consapevolezza del diritto alla protezione dei dati personali, sulla base di progetti previamente approvati dal Garante».

49 Cocuccio, M.: "Dimensione "patrimoniale" del dato personale e tutele risarcitorie", *Dir. fam. pers.*, 2022, p. 252.

dati e/o in termini di modalità di attuazione o di garanzia dell'efficacia delle misure poste in essere[50].

La regola dell'auto-controllo o dell'auto-responsabilità demanda, pertanto, agli operatori del digitale il compito di istituire le misure di prevenzione e reazione più adeguate alla protezione degli stessi interessati. Giova osservare come manchi però uno *standard* predeterminato rispetto alle misure tecniche ed organizzative che i soggetti che operano con dati personali devono adottare nelle diverse situazioni[51]. Invero, è chiara la scelta del legislatore di non voler individuare rigidamente i livelli di protezione cui l'operatore commerciale deve attenersi, variabili a seconda della specificità dei diversi settori industriali e della incessante innovazione tecnologica[52]. Se la legge, per un verso, non può e non vuole stabilire nel dettaglio, attraverso il comando normativo e la tecnica giuridica formale, quali strumenti adottare nella situazione specifica, è fondamentale, per altro verso, l'apporto del "diritto dei privati", secondo un principio di vicinanza del rischio, sottolineandone la funzione regolativa del mercato[53]. In tal senso, si auspica l'adozione e la successiva circolazione di modelli virtuosi di comportamento, regole tecniche, codici etici e di condotta, linee guida e protocolli del settore, *standard* di sicurezza, orientamenti per la messa in atto di opportune misure, nonché strategie di prevenzione[54].

Affidare il compito dell'agire responsabilmente alla sola auto-regolamentazione spontanea non appare di per sé sufficiente[55]. È necessario procedere, ancora una volta, alla "giuridicizzazione" di quelle che sono le *best practices* del settore, sì garantendo alle fonti regolative non statuali una certa effettività e, di conseguenza, innalzando il livello di responsabilità (*recte* diligenza professionale) richiesta nell'adozione delle misure volte alla protezione dei dati personali. In sostanza, a queste regole, di matrice privata e volontaria, deve essere garantita la precettività e l'azionabilità, almeno attraverso un indiretto riconoscimento nelle fonti di diritto statuale ovvero in seguito a procedure di controllo e approvazione delle autorità

50 Così, ancora, Cocuccio, M.: "Dimensione "patrimoniale" del dato personale e tutele risarcitorie", cit., p. 251. V. ancora il *considerando* § 74 GDPR.

51 Misure, invece, specificamente "tipizzate" nella previgente versione del Cod. privacy, in riferimento all'Allegato B, intitolato "disciplinare tecnico in materia di misure minime di sicurezza".

52 Si rinvio all'analisi di Romeo, F.: "Il governo giuridico delle tecniche dell'informazione e della comunicazione", in *I dati personali nel diritto europeo* (a cura di V. Cuffaro, R. D'Orazio e V. Ricciuto), cit., p. 1270, secondo cui il governo della tecnica presuppone la conoscenza delle sue regole, dal momento che il diritto deve essere in grado di interagire con essa al fine di orientare i risultati verso gli scopi posti dalla norma giuridica.

53 Sul diritto privato in funzione regolativa, di recente, Zoppini, A.: *Il diritto privato e i suoi confini*, Il Mulino, Bologna, 2020, p. 201 ss.

54 Si guardi al *considerando* § 77, laddove «gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati».

55 Esemplare è Senigaglia, R.: "La vincolatività dei codici etici: ossimoro o sineddoche?", *Riv. crit. dir. priv.*, 2011, p. 580 ss.

indipendenti o da altri organismi tecnici competenti[56]. Assume, quindi, una portata centrale, nell'ambito del complesso quadro regolamentare fatto da strumenti di regolazione autoritativa e di disciplina convenzionale, l'ibridazione del modello pubblico-privato (*co-regulation*), dove al ruolo (pro-)attivo dell'impresa si aggiunge comunque la garanzia di promozione e sanzione delle regole sì "auto-imposte"[57].

Per esempio, l'art. 57 GDPR, relativo i compiti delle autorità di controllo, indica espressamente quello di incoraggiare l'elaborazione di codici di condotta e di approvare formalmente quelli che forniscono garanzie sufficienti, a norma del procedimento indicato nell'art. 40 GDPR[58]. Ciò si traduce in una strategia di normazione integrata, che delinea, appunto, un'autonomia (privata) degli operatori professionali comunque "controllata" dall'esterno[59]. E se l'assoluta volontarietà di queste procedure sembra mettere un freno alla positiva concorrenza degli operatori al miglioramento di *standard* di qualità dei trattamenti, non va dimenticato che, proprio nell'ottica di quella "multiforme" *accountability* cui è tenuto il titolare del trattamento, l'adesione ai codici di condotta o ai meccanismi di certificazione può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento (art. 25, par. 3, GDPR) o, ancora, può costituire un elemento decisivo per dimostrare la conformità ai medesimi (art. 32 GDPR), laddove, diversamente, rischia di essere alquanto difficile fornire la prova liberatoria della responsabilità per danni. Si chiude, quindi, il cerchio del (complesso) sistema della "responsabilità" delineata dal Regolamento: dalla volontaria elaborazione di *standard* alla loro "positivizzazione" in un documento dotato di una certa effettività, dalla pratica implementazione di alcune misure ivi contenute da parte dei titolari del trattamento agli obblighi risarcitori scaturenti per eventuali danni derivanti dalla loro mancata o inesatta adozione.

Un ulteriore esempio è dato dalla Direttiva 770/2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, dove all'art. 8 si afferma che per la valutazione del difetto di conformità occorre far riferimento «agli scopi per cui sarebbe abitualmente utilizzato un contenuto digitale o un servizio digitale del medesimo tipo, tenendo conto, se del caso, dell'eventuale diritto dell'Unione e nazionale e delle norme tecniche esistenti, oppure, in

56 I codici di condotta, ad esempio, raggiungono i massimi livelli di vincolatività quando trovano titolo nella legge, direttamente o indirettamente, come ricordato da Scotti, A.: *I codici di condotta tra mercato, impresa e contratto*, Giuffré, Milano, p. 17.

57 Così anche P. Laghi, *Cyberspazio e sussidiarietà*, Napoli, ESI, 2015, p. 115, il quale si riconosce la maggiore idoneità regolativa dell'autonomia privata mantenendo un ruolo di direzione e di orientamento del potere pubblico che consente di supplire ad essa allorché si dimostri incapace di realizzare un assetto equilibrato.

58 In argomento, per tutti, Poletti, D., Causarano, M. C.: "Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione", in Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy* (a cura di E. Tosi), Giuffré, Milano, 2019, *p.* 369 ss. Analogo discorso può farsi, poi, con i meccanismi di certificazione di cui all'art. 42 GDPR.

59 Cfr. Rodotà, S.: *Tecnologie e diritti*, Il Mulino, Bologna, 1995, p. 51 ss.; più di recente, Laghi, P.: *Cyberspazio e sussidiarietà*, Esi, Napoli, 2015 p. 110 ss.

mancanza di tali norme tecniche, dei codici di condotta dell'industria specifici del settore applicabili». La difformità, quindi, sembra prescindere dalle caratteristiche materiali del bene, ma va ad abbracciare anche elementi "deontologici", che mirano al soddisfacimento di interessi anche non patrimoniali della persona. Per quanto qui interessa, il richiamo esplicito ai codici di condotta e alle regole tecniche – quali elementi di origine para-statuale i primi e addirittura extra-giuridica i secondi – integrano espressamente ora un criterio di valutazione del difetto di conformità che, come si vedrà, è presupposto per un rimedio di natura ripristinatoria, diverso dal risarcimento del danno.

V. ALLA RICERCA DI UN RIMEDIO EFFETTIVO.

Uno dei profili più interessanti del rapporto fra la disciplina contrattuale e la protezione dei dati personali è quello della estensione dei rimedi consumeristici all'interessato al trattamento[60]. In particolare, l'utente, quando si obbliga a prestare i suoi dati personali all'operatore professionale in luogo del pagamento del prezzo del servizio o contenuto digitale[61], non gode esclusivamente dei diritti previsti dal GDPR (accesso, rettifica, cancellazione, risarcimento del danno, e via dicendo), ma anche, in seguito al recepimento della Direttiva 770/2019, e soprattutto dei rimedi in precedenza riconosciuti all'acquirente di beni di consumo "materiali": sono, precisamente, la risoluzione del contratto e il ripristino di conformità[62].

È interessante ora soffermarsi su alcuni profili meritevoli di attenzione in riferimento ad uno di questi "nuovi" rimedi che il consumatore/interessato al trattamento può esercitare nei confronti del fornitore del servizio, ossia il ripristino di conformità, ove l'interesse dell'utente pare meglio soddisfatto in forma specifica, secondo la logica del dispositivo tecnico di reazione all'ordine giuridico violato, che si pone immediatamente a ridosso del bisogno di tutela o dell'interesse del consumatore[63].

Brevemente, volendo sintetizzare i passaggi fondamentali del discorso occorre, anzitutto, chiedersi se, nel caso in cui l'utente si obblighi a fornire i propri dati personali quale remunerazione del servizio o del contenuto digitale, egli possa richiedere la conformità contrattuale *anche* per il mancato rispetto dei principi e delle regole stabiliti dal Regolamento generale sui dati personali. Risolto affermativamente questo primo quesito, occorre domandarsi poi *quando* si verifichi un difetto di

60 Sul punto, Irti, C.: *Consenso "negoziato" e circolazione dei dati personali*, Giappichelli, Torino, 2021, p. 119 ss., nonché Versaci, G.: *La contrattualizzazione dei dati personali dei consumatori*, Esi, Napoli, 2020, p. 137 ss.

61 Sulla "mercificazione" dei dati personali, si veda, da ultimo, Ricciuto, V.: *L'equivoco della privacy. Persona vs. dato personale*, Esi, Napoli, 2022.

62 Per ovvie ragioni, si esclude la riduzione del prezzo.

63 Cfr. la definizione di rimedio nel diritto privato europeo rinvenibile in Mazzamuto, S.: "La prospettiva dei rimedi in un sistema di *civil law*: il caso italiano", *Contr. e impr.*, 2019, p. 841.

conformità per il fornitore del servizio digitale che non rispetti il GDPR. Una volta ravvisata la difformità, e realizzati così i presupposti della fattispecie-difetto di conformità, occorre soffermarsi *su che cosa* concretamente si traduce l'esercizio del rimedio ripristinatorio[64].

Principiando dal primo degli interrogativi, cioè se la non-conformità rispetto della disciplina dettata al GDPR possa assumere la natura di vizi o meglio irregolarità giuridiche, preme sottolineare che la disciplina dei rimedi contrattuali previsti dalla Direttiva 770/2019 trova applicazione solo quando la fornitura di dati personali costituisce una prestazione cui è tenuto il consumatore per remunerare il fornitore del servizio, nella logica economica di scambio[65]. Chiarito questo punto, vi è da dire che negli articoli della Direttiva dedicati ai requisiti di conformità non si fa e*splicito* riferimento all'osservanza degli obblighi previsti dal GDPR. Eppure, il *considerando* § 48, dopo una generale (ri-)affermazione del rispetto del GDPR anche in relazione ai contratti di fornitura dei servizi digitali, continua dicendo che «in funzione delle circostanze del caso, gli elementi che determinano un difetto di conformità rispetto ai requisiti di cui al Regolamento generale sulla protezione dei dati, inclusi i principi fondamentali quali i requisiti in materia di minimizzazione dei dati, protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita, costituiscano un difetto di conformità del contenuto digitale o del servizio digitale rispetto ai requisiti di conformità (soggettivi e oggettivi) di cui alla presente direttiva»[66]. Ancorché lo stesso *considerando* semplifichi la risposta circa l'interrogativo sulla violazione del GDPR quale difetto di conformità – concludendo perentoriamente per l'estensione dei rimedi contrattuali anche a tale ipotesi – va osservato come l'art. 3, par. 8 della Direttiva affermi – o confermi, alla stregua del principio di effettività delle tutele[67] – la complementarità delle disposizioni del Regolamento sulla protezione dei dati. Sembra allora altrettanto corretto ritenere che il rispetto del GDPR possa

64 Esula dall'analisi qui condotta il recepimento della Direttiva 770/2019 nell'ambito nel nuovo Capo I-*bis* del Codice del consumo intitolato "Dei contratti di fornitura di contenuto digitale e di servizi digitali" (art. 135-*bis* ss.), in quanto sostanzialmente coincidente, nel merito, con le riflessioni condotte attraverso lo studio del testo normativo del legislatore europeo.

65 Infatti, l'art. 3 della Direttiva fa espressamente salvo – e quindi esclude l'applicazione dei rimedi contrattuali prima ricordati – quando i dati personali forniti dal consumatore sono trattati dall'operatore esclusivamente per la fornitura del servizio o per l'assolvimento degli obblighi di legge cui è soggetto. In pratica, i rimedi contrattuali possono trovare applicazione esclusivamente quando la base giuridica del trattamento non è l'esecuzione del contratto o l'obbligo legale, bensì il consenso dell'interessato, nonché il legittimo interesse del titolare del trattamento, ammissibile, peraltro, per finalità di marketing diretto. Per l'apparente gratuità delle c.d. non-monetary transactions, dove i fornitori di un servizio digitale gratuito vanno a sfruttare commercialmente i dati (personali) resi o generati dagli utenti, si veda Irti, C.: *Consenso "negoziato" e circolazione dei dati personali*, cit., p. 61 ss.

66 È interessante osservare come il *considerando* prosegua, poi, riportando alcuni esempi di non conformità di natura oggettiva, quale l'assenza di software di cifratura per la comunicazione sicura di dati personali a terzi – in questo caso per mancato rispetto del principio di *data protection by design* – o ancora la mancata adozione di misure di sicurezza adeguate ai potenziali rischi del trattamento relativo ai servizi di pagamento online, lasciando i dati personali alla mercé di *spyware* o *malware*, in violazione degli artt. 24, 25 e 32 del GDPR.

67 Da ultimo, Vettori, G.: *Effettività fra legge e diritto*, Giuffré, Milano, 2020.

qualificarsi alla stregua di un requisito di conformità, in presenza di un contratto di fornitura di servizi o contenuti digitali remunerato con dati personali[68].

Viene allora da chiedersi se e in che misura il contenuto o il servizio digitale può dirsi conforme al GDPR. Qui soccorre l'art. 8 della Direttiva, ove si sottolinea l'adeguatezza del servizio digitale, anche in assenza di clausole contrattuali specifiche, «agli scopi per cui sarebbe abitualmente utilizzato un contenuto digitale o un servizio digitale del medesimo tipo, tenendo conto, se del caso, dell'eventuale diritto dell'Unione e nazionale [tra cui il GDPR] e delle *norme tecniche esistenti, oppure, in mancanza di tali norme tecniche, dei codici di condotta dell'industria specifici del settore applicabili*»[69]. Ciò apre ad alcune considerazioni ulteriori per quanto riguarda la "positivizzazione" delle buone pratiche di mercato all'interno della nozione di conformità[70].

Attraverso il richiamo "positivo" dei codici di condotta e degli *standard* tecnici, strumenti un tempo non dotati di effetti giuridici propri transitano nel novero delle fonti del diritto, quale parametro valutativo cui l'operatore professionale deve adeguarsi per non incorrere, appunto, nel difetto di conformità. Si è già detto dell'inefficienza del legislatore ad individuare rigidamente gli obblighi di comportamento cui il titolare del trattamento dovrebbe attenersi, variabili a seconda della specificità dei diversi settori commerciali e della incessante innovazione tecnologica: il fenomeno della circolazione dei dati non può non essere governato anche dall'interno dei mercati digitali, attraverso la scelta di *design* tecnologico più adatto non solo a rispettare le norme del GDPR, ma anche a garantire una tutela effettiva dei diritti dell'interessato-consumatore[71]. Così, alla logica eteronoma (pubblica) della regolazione degli scambi nei mercati digitali devono affiancarsi l'autoregolazione e la co-regolamentazione, a conferma del fatto che l'equilibrio esistente tra sfera pubblica e privata non è mai stabile e definitivo[72].

68 Cfr. sul punto Camardi, C.: "Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali", *Giust. civ.*, 2019, p. 514 ss.

69 Art. 8, par. 1, lett. *a*.

70 V. *supra* par. IV.

71 Nella tematica ora affrontata il tipo normativo di problema della non-conformità si salda inscindibilmente con la tecnica informatica. Come osserva Irti, C.: *Consenso "negoziato" e circolazione dei dati personali*, cit., p. 169, la tecnologia nella contrattazione online non possa essere più relegata ai margini del terreno giuridico, posto che è indiscutibile la capacità degli strumenti tecnologici di influenzare il processo di formazione della volontà. Si pensi, ad esempio, ai c.d. *dark pattern* che attraverso interfacce accattivanti invogliano il consumatore a prestare ancora più dati personali. In altre parole, è sul professionista che incombe la responsabilità (giuridica, ma anche sociale) di conformare la tecnica in funzione delle esigenze di tutela della persona nell'ambiente digitale. Sul punto, sia concesso il rinvio al nostro "Enhancing Transparency of Data Processing and Data Subject's Rights through Technical Tools: the PIMS and PDS Solution", in *Privacy and Data Protection in Software Services* (edited by R. Senigaglia, C. Irti e A. Bernes), cit., p. 197 ss.

72 Bellisario, E.: "La responsabilità sociale delle imprese fra autonomia e autorità privata", cit., p. 816-817.

Ancora, l'art. 8 della Direttiva prosegue affermando che il servizio o il contenuto digitale, per essere conforme, deve presentare «la quantità e la qualità e le caratteristiche di prestazione, anche in materia di funzionalità, compatibilità, accessibilità, continuità e sicurezza, che si ritrovano *abitualmente* nei contenuti digitali o nei servizi digitali dello stesso tipo e che il consumatore può *ragionevolmente* aspettarsi, tenuto conto della natura del contenuto digitale o del servizio digitale, tenendo conto di eventuali dichiarazioni pubbliche rese da o per conto dell'operatore economico o di altri soggetti nell'ambito di passaggi precedenti nella catena delle operazioni»[73]. Il dettato normativo, ancora una volta, sembra confermare l'esistenza di una vera e propria obbligazione di conformità rispetto alle prescrizioni del GDPR gravante sull'operatore professionale: l'oggetto consisterebbe nel prestare un servizio o un contenuto digitale conforme (anche) a certi *standard* di protezione dei dati personali, mentre il contenuto si risolverebbe nella predisposizione di misure tecniche ed organizzative, in base alla natura del servizio, ai costi, ai rischi e via dicendo, che siano proporzionate e adeguate (*recte* conformi) al trattamento posto in essere[74]. In sostanza, il legislatore descrive il risultato dovuto dal professionista, e le modalità per attuarlo in astratto, lasciando alle *best practices* del settore, in concreto, i tipi di comportamento strumentali al suo raggiungimento[75].

Alla presenza di un accertato difetto di conformità fa da contraltare, tra gli altri, il rimedio ripristinatorio, i cui presupposti possono, quindi, ben essere integrati dalla violazione del GDPR, anche in base alle buone pratiche di mercato. In sostanza, il ripristino mira a tutelare "in natura" l'interesse del consumatore al conseguimento di un bene munito di determinate caratteristiche e qualità[76].

73 Art. 8, par. 1, lett. *b*.

74 L'esistenza di tale obbligazione di fornitura dei beni conformi al contratto pare suffragata da altri elementi testuali della Direttiva, laddove si configura, tra l'altro, un obbligo di aggiornamento – quale contenuto specifico e/o accessorio dell'obbligazione di fornitura di beni conformi – in capo al professionista: l'art. 8, par. 2, afferma che l'operatore economico assicura che al consumatore siano forniti gli aggiornamenti, anche di sicurezza, necessari al fine di mantenere la conformità, quando il contratto prevede che il contenuto digitale o il servizio digitale sia fornito in modo continuo per un determinato periodo di tempo, e per l'intera durata di tale periodo.

75 Rimane però una certa difficoltà di individuare tali *standard* abituali di qualità oggettiva, sulla base dei quali l'interprete avrà dei parametri per valutare la rispondenza del servizio o del contenuto digitale a quanto ragionevolmente il consumatore-interessato al trattamento si aspetta ragionevolmente di trovare.

76 Vedi Mazzamuto, S.: "La prospettiva dei rimedi in un sistema di *civil law*", cit., p. 842. Sono ravvisabili però alcune resistenze al rimedio del ripristino della conformità nell'ambito della Direttiva 770/2019. Anzitutto, l'art. 14, par. 2, afferma che «[i]l consumatore ha diritto al ripristino della conformità del contenuto o del servizio digitale, a meno che ciò non sia impossibile o imponga all'operatore economico costi che sarebbero sproporzionati, tenuto conto di tutte le circostanze del caso, tra cui il valore che il contenuto o servizio digitale avrebbe se non ci fosse alcun difetto di conformità e l'entità del difetto di conformità». Ad esempio, potrebbe essere il caso delle c.d. *low-value apps*, come quelle che modificano i trattati somatici degli individui: riprogrammarle o fornire aggiornamenti potrebbe richiedere qui costi sproporzionati, ad esempio, se sono sviluppate e messe in commercio da una *start-up* innovativa. Ancora, problematico appare il contrasto tra il GDPR e la previsione dell'art. 8, par. 5, della Direttiva, ove si esclude la rilevanza del difetto di conformità oggettiva se al momento della conclusione del contratto il consumatore è stato specificamente informato di tale difetto ed egli abbia espressamente e separatamente accettato tale scostamento. Qui la natura "pubblicistica" della disciplina della protezione dei dati personali andrebbe considerata alla stregua di una norma imperativa e quindi, come tale, inderogabile da parte dell'autonomia

VI. DAL RISARCIMENTO DEL DANNO AI "PROVVEDIMENTI RISARCITORI".

A fronte di una violazione del GDPR integrante un difetto di conformità nella fornitura del servizio o contenuto digitale, il rispristino di conformità si mostra, neanche a dirlo, migliore del rimedio caducatorio (qual è, per esempio, la nullità di protezione), ma forse anche dello stesso strumento risarcitorio. Del resto, molte volte la lesione sofferta dall'utente di servizi digitali, in caso di violazione delle prescrizioni del GDPR da parte del titolare del trattamento, è difficilmente individuabile (in termini di conseguenze dannose prodotte) o quantificabile (trattandosi per lo più di danno non patrimoniale)[77]. A ciò si aggiunga la ridotta consapevolezza degli utenti digitali rispetto ai loro diritti e la poca propensione degli stessi ad investire tempo e denaro per avviare procedimenti giudiziari; tutti fattori che generano una diffusa apatia di iniziativa processuale del singolo[78]. Di certo l'individuo non è incentivato a chiedere ristoro, sobbarcandosi l'onere (e i costi) del giudizio, specie qualora si parli di lesioni modeste, le cui gravità e serietà non possono essere comprese se non nella loro dimensione "collettiva"[79]. Infatti, la produzione di effetti dannosi non si sostanzia soltanto nella moltiplicazione (quantitativa) di danni individuali, ma si manifesta altresì nella produzione (qualitativa) di danni seriali e massivi, che investono cioè sistematicamente «folle di danneggiati e serie indefinite di persone, peraltro nemmeno sempre catalogabili attraverso categorie predefinite»[80].

La responsabilità ordinaria di una condotta strutturalmente presente su vasta scala e rivolta verso numero indefiniti di soggetti mostra tutta la sua inefficienza, qualora rimanesse ancorata in un'ottica individualistica e volontaristica. Anche se i danni individuali fossero eventualmente riconosciuti al singolo, la dimensione globale della circolazione dei dati determinerebbe comunque un danno sociale, senza che il risarcimento del danno sia «minimamente in grado di creare un baluardo o quantomeno una deterrenza efficace»[81]. In altri termini, le regole della responsabilità per danni e la tutela offerta dal risarcimento per equivalente si mostrano inefficaci nell'allocazione dei costi tra i principali attori dei mercati digitali.

privata. Diversamente, laddove l'operatore professionale aderisse volontariamente ad un certo codice di condotta e ne prevedesse pattiziamente la deroga *in peius*, quest'ultima potrebbe dirsi comunque valida, qualora vengano garantiti livelli "minimi" di protezione conformi al GDPR.

77 *Amplius*, Gambini, M.: *Principio di responsabilità e tutela aquiliana dei dati personali*, Esi, Napoli, 2018, p. 9 ss.

78 Irti, C.: *Consenso "negoziato" e circolazione dei dati personali*, cit., p. 192. Sulla limitata litigiosità processuale, vedi D'Ambrosio, M.: *Progresso tecnologico, "responsabilizzazione" dell'impresa*, cit., p. 110.

79 Gambini, M.: *Principio di responsabilità e tutela aquiliana dei dati personali*, cit., p. 11.

80 Camardi, C.: "Note critiche in tema di danno", cit., p. 810. Potrebbero essere gli utenti di un *social network*, categorie di consumatori individuati in base ad un criterio geografico, o in forza di un criterio di profilazione, e via dicendo.

81 Ancora Camardi, C.: "Note critiche in tema di danno", cit., p. 810, la quale afferma che l'impostazione dei rimedi contro l'offensività strutturale dell'economia digitale richiede l'utilizzazione di strumenti altri, di natura preventiva e forse non soltanto di diritto privato.

Nella prospettiva da ultimo ricordata, meglio se ad attivarsi non è l'individuo, ma un organismo di tutela dei diritti degli utenti dei servizi digitali attraverso lo strumento delle azioni "collettive": in questo senso si esprime, da ultimo, la Direttiva 2020/1828/UE relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori, applicabile, peraltro, anche nel caso di violazioni del GDPR[82].

La vera novità introdotta dalla nuova Direttiva consiste nella previsione di un complesso di "provvedimenti risarcitori" (art. 9), imposti dall'autorità giudiziaria (o amministrativa) competente ai professionisti convenuti con l'azione rappresentativa, laddove tra i possibili rimedi offerti ai consumatori, oltre allo strumento (inibitorio e) risarcitorio per equivalente, vi è anche l'esplicita indicazione di ulteriori meccanismi di tutela, quali indennizzo, riparazione, sostituzione, riduzione del prezzo, risoluzione del contratto e altri eventualmente stabiliti dal legislatore nazionale. Sicché attraverso le azioni rappresentative sarà possibile far valere non soltanto le pretese creditorie, di natura risarcitoria e/o restitutoria – attualmente contemplate, nel nostro ordinamento, dall'art. 840 *bis*, comma 2, c.p.c. e un tempo previste dall'art. 140 *bis* c. cons. – ma anche altre pretese creditorie: non vi è motivo per escludere, infatti, che possano e debbano considerarsi ricomprese tutte le ipotesi in cui una disposizione di diritto dell'Unione o di diritto interno attribuisca a consumatori un diritto all'"esatto adempimento" del contratto la cui stipulazione sia stata preceduta, accompagnata o seguita dalla violazione di una delle disposizioni di tutela dei consumatori riportate nell'Allegato alla Direttiva[83].

Con il futuro esperimento delle azioni rappresentative, dunque, la possibile comminatoria di "provvedimenti risarcitori" *diversi* rispetto al risarcimento per equivalente potrà seguire pure al caso di mancata adozione di (altre) misure tecniche e organizzative (più) adeguate, tecnicamente possibili e proporzionate alla valutazione del rischio dell'attività svolta, alla stregua di una violazione del GDPR (e non per forza produttive di danno).

Per esemplificare, si pensi in proposito al noto *social network TikTok* (e delle tragiche morti di minori impegnati in pericolosissime *challenge*), per il quale il Garante *privacy* italiano ha rilevato, nel gennaio 2021, che nello impostare in via predefinita il profilo dell'utente come pubblico, è ravvisabile una violazione del principio di *data protection by default*; nell'indeterminatezza dei tempi di

82 L'art. 2 definisce l'ambito di applicazione della Direttiva, individuandolo nelle azioni rappresentative intentate nei confronti di professionisti per violazioni delle disposizioni del diritto dell'Unione di cui all'allegato I. Per un primo commento, Casarosa, F.: "Transnational collective actions for cross-border data protection violations", *Internet Policy Review*, 2020, 9(3), p. 1 ss.

83 Così De Cristofaro, G.: "Azioni 'rappresentative' e tutela degli interessi collettivi dei consumatori. La 'lunga marcia' che ha condotto all'approvazione della dir. 2020/1828/UE e i profili problematici del suo recepimento nel diritto italiano", *Nuove leggi. civ. comm.*, 2022, p. 1033, il quale aggiunge, appunto, anche le obbligazioni di *dare* o *facere* funzionali alla correzione di inesattezze o difetti che abbiano connotato l'adempimento contrattuale da parte del professionista.

conservazione, una violazione del principio di *storage limitation*; nella assenza di meccanismi di verifica dell'età "reale" per il consenso prestato da minori, una violazione dell'art. 8 GDPR sul trattamento dei dati dei minorenni[84]. Così, l'Autorità ha provvisoriamente disposto un blocco del trattamento per i dati di minori per i quali non fosse stata accertata l'età anagrafica. Successivamente, *TikTok* ha cambiato non solo le sue *policies*, ma anche adottato nuove misure tecniche per la *age verification*, ivi compresi sistemi di *AI*[85]. Rileggendo il caso in chiave privatistica – anziché di *public enforcement* – le violazioni rilevate dall'autorità di controllo parrebbero integrare oggi un'ottima opportunità per l'esperimento delle azioni rappresentative. In particolare, alla inadeguata adozione di misure opportune per la protezione dei dati personali e, di conseguenza, alla tutela dei diritti degli interessati, si potrebbe pensare non tanto all'esperimento della «protezione minima e indefettibile»[86] rappresentata dalla tutela per equivalente, bensì ricorrendo alla tecnica rimediale in forma specifica, che ben si concretizza nel rimedio del ripristino della conformità, ascrivibile ai nuovi "provvedimenti risarcitori" richiamati dalla Direttiva 1828/2020. Con una conseguenza non da poco, dal momento che poi anche tutti i *social* simili dovrebbero aggiornare le proprie impostazioni, dal momento che gli utenti potrebbero *ragionevolmente* aspettarsi i medesimi *standard* di sicurezza, per non ricorrere gli altri titolari del trattamento, a loro volta, in un difetto di conformità. Come a dire che anche l'incremento di interventi di stampo "pro-attivo", determinerebbe, sia pur indirettamente, l'innalzamento del livello di diligenza professionale richiesta agli operatori nelle attività di trattamento dei dati personali. Detti *standard*, laddove resi vincolanti, promuoverebbero il costante miglioramento delle tecnologie a beneficio della collettività e svolgerebbero un ruolo attivo nella tutela dei diritti e delle libertà degli individui[87].

La retorica del diritto alla protezione dei dati personali come diritto fondamentale non può allora impedire di valutare l'idoneità dei meccanismi giuridici di tutela nel mutato scenario politico, economico, sociale e tecnologico attuale[88]. Così, anche le "mobili frontiere" della responsabilità civile e il suo maccanismo principale di riparazione del danno subiscono delle ibridazioni che consentono di individuare dei rimedi utili non solo in chiave compensativa[89]. In questo senso, il rispristino della conformità in caso di violazione delle regole e dei principi stabiliti dal GDPR

84 Garante per la Protezione dei Dati Personali, provv. del 22 gennaio 2021, reperibile all'indirizzo *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9524194*. In argomento, vedi Senigaglia, R.: "Il dovere di educare i figli nell'era digitale", *Persona e mercato*, 2021, p. 524.

85 Vedi, ancora, il comunicato stampa del Garante all'indirizzo *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9533424*.

86 Carapezza Figlia, G., Sajeva, S.: "Responsabilità civile e tutela ragionevole ed effettiva degli interessi", *Arch. giur.*, 2017, 2, p. 336.

87 Così Gambini, M.: "Algoritmi e sicurezza", cit., p. 1740.

88 Di questo avviso Perlingieri, P.: "Il «giusto rimedio» nel diritto civile", *Il giusto processo civile*, 2011, p. 1 ss.

89 Una prospettiva, questa, già segnalata da Di Majo, A.: "La responsabilità civile nella prospettiva dei rimedi: la funzione deterrente", *Eur. dir. priv.*, 2008, p. 305.

pare un rimedio utile non solo per il consumatore-interessato al trattamento, ma anche in funzione della (efficace) regolazione dei mercati digitali.

BIBLIOGRAFIA

Alessi, R.: "Il difficile percorso della «responsabilità civile europea»", *Danno resp.*, 1999, p. 377 ss.

Alpa G., Conte G. (a cura di): *La responsabilità dell'impresa*, Giuffré, Milano, 2015

Bellisario, E: "La responsabilità sociale delle imprese fra autonomia e autorità privata", *Danno e resp.*, 2013, p. 809 ss.

Bernes, A.: Enhancing Transparency of Data Processing and Data Subject's Rights through Technical Tools: the PIMS and PDS Solution", in *Privacy and Data Protection in Software Services* (edited by R. Senigaglia, C. Irti e A. Bernes), Springer, Singapore, 2022, p. 197 ss.

Bertelli, F.: *Le dichiarazioni di sostenibilità nella fornitura dei beni di consumo*, Giappichelli, Torino, p. 20 ss.

Bevivino, G.: "La responsabilità sociale delle imprese fra autonomia privata, nuovi obblighi di legge e prospettiva rimediale", in *Analisi giur. ec.*, 2018, p. 107 ss.

Bevivino, G.: *La responsabilità sociale delle imprese. Strumenti attuativi e rimedi*, Esi, Napoli, 2018, p. 65 ss.

Bilotta, F.: "La responsabilità civile nel trattamento dei dati personali", in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato* (a cura di R. Panetta), Giuffré, Milano, 2019, p. 452 ss.

Bravo, F.: "Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali", in *Persona e mercato dei dati. Riflessioni sul GDPR* (a cura di N. Zorzi-Galgano), Cedam-Wolters Kluwer, Padova-Milano, 2019, p. 402 ss.

Califano, L.: "Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali", in *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679* (a cura di L. Califano e C. Colapietro), Editoriale Scientifica, Napoli, p. 34 ss.

Camardi, C.: "Liability and Accountability in the "Digital" Relationships", in *Privacy and Data Protection in Software Services* (edited by R. Senigaglia, C. Irti e A. Bernes), Springer, Singapore, 2022, p. 25 ss.

Camardi, C.: "Note critiche in tema di danno da illecito trattamento dei dati personali", *Jus Civile*, 2020, p. 796 ss.

Camardi, C.: "Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali", *Giust. civ.*, 2019, p. 514 ss.

Carapezza Figlia, G., Sajeva, S.: "Responsabilità civile e tutela ragionevole ed effettiva degli interessi", *Arch. giur.*, 2017, 2, p. 336 ss.

Casarosa, F.: "Transnational collective actions for cross-border data protection violations", *Internet Policy Review*, 2020, 9(3), p. 1 ss.

Cocuccio, M.: "Dimensione "patrimoniale" del dato personale e tutele risarcitorie", *Dir. fam. pers.*, 2022, p. 252 ss.

D'Ambrosio, M.: *Progresso tecnologico, "responsabilizzazione" dell'impresa ed educazione dell'utente*, Esi, Napoli, 2017, p. 118 ss.

De Cristofaro, G.: "Azioni 'rappresentative' e tutela degli interessi collettivi dei consumatori. La 'lunga marcia' che ha condotto all'approvazione della dir. 2020/1828/UE e i profili problematici del suo recepimento nel diritto italiano", *Nuove leggi. civ. comm.*, 2022, p. 1033 ss.

Di Ciommo, F.: "Civiltà tecnologica e, mercato e insicurezza: la responsabilità del diritto", *Riv. crit. dir. priv.*, 2010, p. 590 ss.

Di Majo, A.: "La responsabilità civile nella prospettiva dei rimedi: la funzione deterrente",

Eur. dir. priv., 2008, p. 305 ss.

Finocchiaro, G.: "Il principio di accountability", *Giur. it.*, 2019, p. 2778 ss.

Finocchiaro, G.: "Introduzione al Regolamento europeo sulla protezione dei dati", *Nuove leggi civ. comm.*, 2017, p. 10 ss.

Franzoni, M.: "Responsabilità derivante da trattamento di dati personali", in *Diritto dell'informatica* (a cura di G. Finocchiaro e F. Delfini), Wolters Kluwer, Milano, 2014, p. 829 ss.

Gambini, M.: "Algoritmi e sicurezza", *Giur. it.*, 2019, p. 1737 ss.

Gambini, M.: "Responsabilità e risarcimento nel trattamento di dati personali, in *I dati personali nel diritto europeo* (V. Cuffaro, R. D'Orazio e V. Ricciuto), Giappichelli, Torino, 2019, p. 1057 ss.

Gambini, M.: *Principio di responsabilità e tutela aquiliana dei dati personali*, Esi, Napoli, 2018, p. 9 ss.

Hijmans, H.; Raab, C.: "Ethical Dimensions of the GDPR, AI Regulation, and Beyond", *Direito Público*, 2022, 18(100), p. 68 ss.

Irti, C.: *Consenso "negoziato" e circolazione dei dati personali*, Giappichelli, Torino, 2021, p. 119 ss.

Lipari, N.: *Le categorie del diritto civile*, Giuffré, Milano, 2013, p. 199 ss.

Mazzamuto, S.: "La prospettiva dei rimedi in un sistema di *civil law*: il caso italiano", *Contr. e impr.*, 2019, p. 841 ss.

Perlingieri, P.: "Il «giusto rimedio» nel diritto civile", *Il giusto processo civile*, 2011, p. 1 ss.

Perlingieri, P.: "*Privacy* digitale e protezione dei dati personali tra persona e mercato", *Foro nap.*, 2018, p. 482 ss.

Piraino, F.: "Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato", *Nuove leggi civ. comm.*, 2017, p. 389 ss.

Poletti, D., Causarano, M. C.: "Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione", in Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy* (a cura di E. Tosi)*,* Giuffré, Milano, 2019, *p.* 369 ss.

Quelle, C.: "Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach", *Eur. Journal of Risk Regulation*, 2018, 9, p. 502 ss.

Ratti, M.: "La responsabilità da illecito trattamento di dati personali nel nuovo Regolamento", in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (a cura di G. Finaocchiaro), Zanichelli, Bologna, 2017, p. 615 ss.

Ricciuto, V.: *L'equivoco della privacy. Persona vs. dato personale*, Esi, Napoli, 2022

Rodotà, S.: *Tecnologie e diritti*, Il Mulino, Bologna, 1995, p. 51 ss.

ROMEO, F.: "Il governo giuridico delle tecniche dell'informazione e della comunicazione", in *I dati personali nel diritto europeo* (a cura di V. CUFFARO, R. D'ORAZIO e V. RICCIUTO), Giappichelli, Torino, p. 1270 ss.

SCOTTI, A.: *I codici di condotta tra mercato, impresa e contratto*, Giuffré, Milano, 2019, p. 17 ss-

SENIGAGLIA, R.: "La vincolatività dei codici etici: ossimoro o sineddoche?", *Riv. crit. dir. priv.*, 2011, p. 580 ss.

THOBANI, S.: "Commento all'art. 82", in *Commentario al Codice civile* (diretto da E. GABRIELLI), *Delle persone* (a cura di A. BARBA e S. PAGLIANTINI), *Leggi collegate*, II, Utet- Wolters Kluwer, Milano, 2019, p. 1238 ss.

TOSI, E.: *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Giuffrè, Milano, 2019, p. 125 ss.

VETTORI, G.: *Effettività fra legge e diritto*, Giuffré, Milano, 2020

ZOPPINI, A.: *Il diritto privato e i suoi confini*, Il Mulino, Bologna, 2020, p. 201 ss.