Giacalone P, 'L'effettività della tutela nel diritto alla riservatezza' (2025) Special Issue 2 EJPLT.
DOI: https://doi.org/10.57230/EJPLTSIBPG

EJPLT
ISSN 2704-8012

L'effettività della tutela nel diritto alla riservatezza

The effectiveness of the protection of the right to privacy

PAOLA GIACALONE
Avv., Ph.D. and Senior Researcher of the Research Centre in European Private Law (ReCEPL)
Università degli studi Suor Orsola Benincasa

Abstract

Il contributo esamina l'evoluzione del principio di effettività nella tutela del diritto alla riservatezza, ricostruendo il passaggio dal tradizionale modello giurisprudenziale a una concezione pienamente autonoma del diritto fondamentale alla protezione dei dati personali. L'analisi prende avvio dalla fase antecedente alla disciplina organica, per poi soffermarsi sul progressivo consolidamento del formante europeo. Particolare rilievo è attribuito al ruolo della giurisprudenza sovranazionale nel rafforzamento degli standard di tutela effettiva. In tale prospettiva, il Regolamento (UE) 2016/679 segna una svolta sistemica. Il GDPR introduce un approccio proattivo e preventivo fondato sul principio di accountability. L'effettività viene così declinata in termini di responsabilità, prevenzione e deterrenza. Il contributo si conclude esaminando le criticità emergenti connesse all'impiego dell'intelligenza artificiale e ai processi decisionali automatizzati.

The article analyses the evolution of the principle of effectiveness in the protection of the right to privacy, tracing the shift from traditional jurisprudential models to the autonomous fundamental right to personal data protection. The analysis starts from the pre-codification phase and examines the progressive consolidation of the European legal framework. Particular emphasis is placed on the role of supranational case law in strengthening effective safeguards. From this perspective, Regulation (EU) 2016/679 represents a systemic turning point. The GDPR introduces a proactive and preventive approach based on the principle of accountability. Effectiveness is thus framed in terms of responsibility, prevention, and deterrence. The article concludes by addressing the challenges posed by artificial intelligence and automated decision-making systems.

© The author(s) 2026, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Diritto alla riservatezza; effettività della tutela; privacy; accountability; DPIA.

Summary: 1. Introduzione: dal diritto alla riservatezza al diritto alla protezione dei dati. – 2. Gli albori della tutela in Italia: dalla giurisprudenza alla legge 675/96. – 3. L'influenza del formante europeo e il conseguente rafforzamento della tutela. – 4. Le radicali innovazioni del GDPR e il principio di *accountability*. – 5. Il contributo della giurisprudenza unionale ed italiana - 6. Conclusioni: Le sfide future e il consolidamento del diritto.

1. Introduzione: dal diritto alla riservatezza al diritto alla protezione dei dati

La nozione di *privacy*, considerata in origine nel suo significato classica di "diritto a essere lasciati soli"[1], è stata oggetto di un radicale cambiamento con l'insorgere ed il diffondersi dell'innovazione digitale, sviluppandosi in un più vasto "diritto alla protezione dei dati personali". In tale contesto, il fulcro della tutela si è evoluto dalla mera protezione contro le intrusioni illecite nella sfera più intima alla concreta garanzia del potere di controllo del singolo sulla circolazione delle proprie informazioni.

Contestualmente a tale sviluppo del concetto, si è avuto un incremento esponenziale del bisogno di garantire l'effettività della tutela, di modo che i diritti, pur se riconosciuti, non rimanessero semplici declamazioni di principio, ma fossero in concreto azionabili e atti a produrre un risultato tangibile.

L'effettività, così intesa, finisce per essere la cartina di tornasole della piena e concreta operatività dell'ordinamento giuridico, che tende a realizzare un

[1] È generalmente riconosciuto che la concezione moderna della tutela della sfera privata affondi le proprie radici nella pubblicazione, sulla Harvard Law Review del 1890, del celebre saggio di Warren e Brandeis dedicato al "right to privacy". Gli autori individuarono tale prerogativa nel diritto dell'individuo a non essere disturbato, ossia nel potere di escludere ogni indebita ingerenza nella propria vita personale. Muovendo da una visione ispirata al modello proprietario, all'epoca dominante nella tradizione giuridica, la borghesia, cui inizialmente era circoscritta la titolarità di questa forma di protezione, rivendicava un ambito interiore riservato, destinato a rimanere accessibile solo al soggetto e a coloro con cui egli intendesse volontariamente condividerlo. Per una maggiore analisi, cfr. WARREN, BRANDEIS, *Right to Privacy*, *Harvard Law Review*, 1890,4.
Successivamente, la protezione della vita privata venne progressivamente associata ai diritti di libertà, individuali e collettivi, fino ad acquisire una dimensione sociale più ampia. In tale prospettiva, essa rappresentò una condizione essenziale affinché ciascuno potesse esercitare, senza timore di ripercussioni o discriminazioni, scelte rilevanti sul piano politico, religioso o ideale: aderire a un partito, iscriversi a un sindacato, professare una fede o esprimere opinioni personali. La privacy iniziò così ad essere percepita come garanzia della libertà personale e come strumento attraverso il quale l'individuo può sviluppare pienamente la propria identità, venendo definita sempre più chiaramente quale diritto alla protezione delle informazioni che lo riguardano. Per un'analisi più accurata, si veda S. RODOTÀ, *Intervista su Privacy e Libertà,* a cura di CONTI, 2005.
L'avvento delle tecnologie digitali ha segnato un ulteriore momento di svolta. L'informatizzazione dei processi di raccolta, elaborazione e circolazione dei dati, unita alla radicale trasformazione delle modalità di comunicazione interpersonale, ha infatti eliminato i limiti imposti dalla distanza fisica e temporale, determinando una completa ridefinizione degli spazi relazionali. Tale mutamento ha condotto alla configurazione della dimensione telematica come un "non luogo", distinto dalle categorie tradizionali di terra, mare e aria. Parallelamente, la crescente rilevanza economica delle informazioni generate dagli utenti – raccolte e analizzate dalle imprese operanti nel settore del cosiddetto *cybermarketing* – ha posto in evidenza la necessità di un approccio organico alla protezione dei dati in rete, come illustrato nei documenti elaborati in sede europea sin dagli anni Novanta. V. ZENO-ZENCOVICH, A. ZOPPINI, *La disciplina dei servizi telematici nel quadro delle proposte comunitarie di tutela dei dati personali,* in Dir. Inf., 1992, p. 773 s.

idoneo equilibrio tra le libertà individuali e le mutevoli dinamiche di un contesto informativo e tecnologico in costante e velocissima evoluzione[2]

Questa analisi vuole passare rapidamente in rassegna i punti chiave di come è cambiato il principio: inizialmente si accennerà alla tutela, anche se frammentata, che la giurisprudenza italiana ha accordato allo stesso; quindi, si esaminerà il suo consolidamento a livello europeo; infine, si considererà la svolta operata dal GDPR, che ha ridefinito l'effettività, esigendo maggiore proattività, nonché più consistenti responsabilità e prevenzione.

2. Gli albori della tutela in Italia: dalla giurisprudenza alla legge 675/96

Anteriormente all'introduzione di un contesto regolatorio organico, il diritto alla riservatezza in Italia non disponeva di un riconoscimento esplicito e generale nel testo di norme di legge, ma riveniva il suo fondamento nella giurisprudenza e in alcuni principi costituzionali, specie nell'art. 2 Cost., che tutela i diritti inviolabili dell'uomo e la dignità umana, e nell'art. 15 Cost., che garantisce la libertà e la segretezza della corrispondenza. Una tutela di tal fatta, tuttavia, si presentava settoriale e frammentata, essendo affidata prevalentemente all'interpretazione giurisprudenziale, che ricorreva per lo più ad analogie e a principi generali per sanzionare le violazioni della sfera più intima della persona[3].

Una tappa determinante, in questo stadio dell'evoluzione del concetto in esame,, fu costituito dalla celebre sentenza della Corte di Cassazione del 27 maggio 1975, n. 2199, che ha riconosciuto per la prima volta un vero e proprio "diritto alla riservatezza", come diritto della personalità, in un'ipotesi relativa alla pubblicazione non autorizzata di fotografie[4].

La dottrina, da lungo tempo concentrata sulla questione, aveva lamentato la lacuna di una disciplina specifica, e la giurisprudenza cercava di far fronte a tale mancanza[5].

Ciò nonostante, la tutela rimaneva settoriale e tendente prevalentemente alla salvaguardia della reputazione, dell'onore o dell'immagine, non tanto a un controllo intrinseco e autonomo sul trattamento dei dati personali.

Il primo vero punto di svolta si è avuto con l'emanazione della legge n. 675 del 31 dicembre 1996, la cosiddetta "legge sulla privacy". Tale normativa, adottata per recepire la Direttiva europea n. 95/46/CE, ha posto in essere una disciplina organica sul trattamento dei dati personali, mutando il diritto alla riservatezza da una mera protezione da intrusioni illecite in un diritto al controllo sui propri dati, indipendentemente dalla loro lesività. La legge n.

---

[2] AA.VV., *La protezione dei dati personali. Commentario al D. lgs. 30 giugno 2003, n.196* («Codice della Privacy»), a cura di C.M. BIANCA, F.D. BUSNELLI, Padova, 2007.

[3] C.M. BIANCA, *Diritto civile* I, *La norma giuridica. I soggetti*, Milano, 2002 rileva come nel linguaggio comune i termini *privacy*, *riservatezza personale* e *protezione dei dati personali* fossero spesso impiegati come sinonimi, sebbene si riferiscano a diritti distinti. Tali diritti erano tutelati dal previgente art. 2 del Codice Privacy e lo sono oggi dal GDPR, oltre che dall'art. 2 della Costituzione.

[4] Si v. tra i tanti autori, P. RESCIGNO, *I diritti della personalità, in Trattato di diritto privato diretto da Iudica–Zatti*, Giuffrè.

[5] Si pensi ai contributi di A. DE CUPIS, *I Diritti della personalità,* Milano, 1982; A. DE CUPIS, *Il diritto alla riservatezza esiste*, in *Il Foro Italiano*, 1954, 77, 4; A. DE CUPIS, *I diritti della personalità*, in *Trattato di diritto civile e commerciale*, diretto da A. CICU, F. MESSINEO, 1959, 4. L'autore individuava nel diritto all'immagine il fondamento della tutela

675/96 non definiva soltanto i principi generali, ma introduceva già meccanismi di tutela effettiva. Tra questi, destava grande interesse l'istituzione del Garante per la protezione dei dati personali, un'autorità amministrativa indipendente, dotata di poteri di vigilanza e di poteri sanzionatori, alla quale i soggetti interessati potessero rivolgersi, attraverso un reclamo, per ottenere tutela in tempi rapidi.

La legge introduceva pure sanzioni penali ed amministrative per le violazioni, delineando un insieme di garanzie, con l'intento di porre rimedio all'inefficacia della sola tutela civile e ad introdurre un meccanismo di controllo preventivo e successivo, fondamentale per garantire l'effettività della "novella".

La disciplina italiana, pur con i limiti dovuti all'epoca della sua introduzione ed alla limitata prassi del settore, contribuì, comunque, a gettare le basi di una cultura della protezione dei dati personali che sarebbe stata via via sviluppata negli anni successivi[6].

3. L'influenza del formante europeo e il conseguente rafforzamento della tutela

Lo sviluppo della salvaguardia della *privacy*, e, con essa, del principio di effettività della medesima, è stata grandemente influenzata dalla sempre crescente integrazione del diritto europeo negli ordinamenti giuridici degli Stati membri.

Siffatto adattamento dei sistemi interni al formante europeo ha fornito un quadro di riferimento sempre più solido ed armonizzato, che ha consentito di colmare le lacune e le frammentazioni delle regolamentazioni nazionali.

Uno snodo di carattere determinante è la Convenzione n. 108 del Consiglio d'Europa (1981), la quale, pur costituendo uno strumento sovranazionale e non direttamente vincolante, ha fissato i principi fondamentali sulla protezione dei dati, fungendo, così, da modello e da ispirazione per le normative successive.

Una spinta decisiva, verso la tutela effettiva nella materia, si è avuta, quindi, con l'introduzione della Carta dei Diritti Fondamentali dell'Unione Europea (2000), la quale, all'articolo 8, riconosce espressamente il diritto alla protezione dei dati personali quale diritto fondamentale, distinto ed autonomo rispetto al diritto alla vita privata (tutelato, invece, all'art. 7).

Si tratta di una differenza di carattere sostanziale, poiché ha spostato il baricentro dalla protezione contro le ingerenze altrui alla necessità di un controllo attivo da parte dell'interessato sui propri dati, indipendentemente dalla loro natura intrusiva. Il ruolo assunto della giurisprudenza, sia di quella della Corte di Giustizia dell'Unione Europea (CGUE) che della Corte europea dei diritti dell'uomo (CEDU), si è rivelato determinante per delineare e rafforzare l'effettività di tale diritto. La CGUE, in particolare, ha assunto una vera e propria posizione di "custode" della tutela dei dati personali, anzitutto in relazione al regime statunitense di trasferimento dei dati.

Sentenze che hanno finito per essere considerate come delle pietre miliari, quali quella del caso *Schrems I* (C-362/14), che ha annullato la decisione della

[6] G. ALPA, G. RESTA, Le persone fisiche e i diritti della personalità, I, in Trattato di Diritto Civile, diretto da R. Sacco, Torino 2006; S. Rodotà, Intervista su privacy e libertà, Bari, 2005.

Commissione relativa al "safe harbor" tra l'UE e gli USA, e del successivo caso *Schrems II* (C-311/18)[7], che ha posto nel nulla il "Privacy Shield", hanno affermato con toni inequivocabili che il trasferimento di dati verso paesi terzi non può compromettere il livello di tutela accordato dal diritto europeo.

Queste sentenze hanno sottolineato l'esigenza di apprestare una tutela forte ed effettiva in materia di dati personali, anche in presenza dei rapidi sviluppi tecnologici e della globalizzazione dei trattamenti.

La CEDU, da parte sua, ha incrementato in senso evolutivo la propria giurisprudenza sull'articolo 8 della Convenzione, interpretandolo fino a considerarlo comprensivo anche della protezione dei dati personali, attraverso un approccio multilivello, che interagisce con le norme e la giurisprudenza dell'UE. La dottrina maggioritaria ha considerato questo dinamismo come la realizzazione di un vero e proprio "modello europeo" di protezione dei dati[8], tendente aa accordare un medesimo livello di protezione per tutti i cittadini dell'Unione, a prescindere dal luogo in cui i dati vengano trattati.

Il descritto approccio giurisprudenziale ha finito per rappresentare un terreno fecondo per il successivo sviluppo del contesto regolatorio, facendo da apripista verso un sistema di protezione dei dati ancor più uniforme e rigoroso, quale quello introdotto dal GDPR.

4. Le radicali innovazioni del GDPR e il principio di accountability

Il vero e proprio salto di qualità verso una tutela esaurientemente "effettiva" si è avuto, però, con l'entrata in vigore del Regolamento UE n. 2016/679 (GDPR) [9] . Questo ha colmato la frammentazione e superato l'approccio reattivo della precedente disciplina, mettendo in opera una filosofia olistica e rafforzando in modo determinante i diritti degli interessati.

La svolta è imperniata sul principio di *accountability* (responsabilizzazione), una nozione che ha modificato, in termini rivoluzionari, il paradigma di conformità. Non è più sufficiente l'osservanza formale delle norme, ma il titolare del trattamento è chiamato a dimostrare attivamente, e in ogni momento, di aver adottato le misure idonee per garantire la conformità al regolamento.

Questa modifica dell'onere della prova e della responsabilità ha trasformato il titolare da soggetto passivo di obblighi aa attivo protagonista di una strategia di conformità, basata sulla scrupolosa documentazione delle misure tecniche ed organizzative adottate. In tal modo, l'effettività si manifesta attraverso la progettualità (*privacy by design*), la precauzione (valutazione d'impatto), la deterrenza (sanzioni) e il controllo (autorità di garanzia).

---

[7] O. POLLICINO, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato, in Medialaws, 2018;* F. Rossi Dal Pozzo, La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della *persona (dal Safe Harbour al Privacy Shield)*, in Diritto internazionale, 2016, 690-724; S. CRESPI, *La tutela dei dati personali UE a seguito della sentenza Schrems*, in *Eurojus*, 2015.

[8] G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi, Bologna, 2012; C.* COLAPIETRO, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa italiana sulla privacy*, Napoli, 2018

[9] L. CALIFANO, C. COLAPIETRO, *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2018.

Il GDPR ha rafforzato la tutela dell'interessato su plurimi piani, conglobando sia le azioni preventive sia quelle successive a una violazione, garantendo così che la protezione dei dati sia intrinseca e non episodica.

1) In fase preventiva, in base al criterio *Privacy by Design* e *by Default*, il titolare del trattamento è tenuto a integrare e ad assicurare la protezione dei dati fin dal momento della progettazione dei sistemi e dei processi (Privacy by Design) e a fare sì che, per impostazione predefinita, siano trattati solo i dati personali strettamente necessari (Privacy by Default).

Si tratta di un'impostazione che si basa sul rovesciamento della logica dapprima accolta, apprestando la protezione ancor prima che si verifichi un rischio. L'effettività si concreta, quindi, attraverso l'obbligo di un approccio strutturale e procedurale, che fa diventare la protezione dei dati parte integrante di qualsiasi operazione di trattamento, minimizzando i rischi di violazione *ex ante*.

2) Attraverso il livello amministrativo e giurisdizionale, l'effettività della tutela si estrinseca nella facoltà, per l'interessato, di disporre di rimedi efficaci in caso di violazione. Il GDPR incrementa i meccanismi di tutela attraverso una pluralità di canali: 2.a. reclamo all'Autorità di controllo (Garante): il cittadino può presentare un reclamo all'autorità di controllo nazionale (in Italia, il Garante per la protezione dei dati personali), la quale è dotata di poteri investigativi, correttivi e sanzionatori. L'effettività è assicurata dalla rapidità e dall'indipendenza di tali autorità; 2.b. ricorso all'autorità giudiziaria: l'interessato può rivolgersi ai tribunali, per ottenere il risarcimento dei danni, sia materiali che immateriali, secondo quanto stabilito dall'art. 82 GDPR. La giurisprudenza della Corte di Cassazione ha sottolineato e consolidato lil rilievo di tale tutela giurisdizionale effettiva, pure se il GDPR ha ampliato in maniera significativa le possibilità risarcitorie[10].

Tutto ciò senza contare il significativo ruolo rivestito nella materia della Corte di Giustizia UE.: le sue sentenze, come quelle citate nei casi *Schrems*, continuano a porre l'accento sulla rilevanza di una tutela effettiva in materia di dati personali, facendo onere agli Stati membri ed ai titolari del trattamento del rispetto rigoroso degli standard europei[11].

3. Sul piano della responsabilità, il principio di responsabilizzazione (*accountability*) costituisce il pilastro su cui si regge la tutela effettiva del diritto alla *privacy* nel quadro regolatorio attuale.

Tale principio non si esaurisce nella semplice osservanza delle disposizioni, ma presuppone la necessità di un approccio proattivo, vale a dire sostanziale e preventivo, oltre che dimostrabile, teso a salvaguardare la protezione dei dati. L'effettività si sostanzia attraverso:

- la valutazione d'impatto sulla protezione dei dati (DPIA): rispetto ai trattamenti che o un rischio elevato, l'obbligo di preventiva valutazione dei rischi per i diritti e le libertà dei soggetti interessati impone una riflessione strutturata e documentata.

[10] Corte di Cass., Sez. Un. 26972/2008,

[11] Per un'analisi complessiva dell'impatto della sentenza Schrems si veda: Gruppo di lavoro "Articolo 29", Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 13 aprile 2016.

- il Registro dei trattamenti: è previsto l'obbligo di tenere un registro delle attività di trattamento, che fornisce una traccia documentale, la quale contribuisce alla possibilità di dimostrare la conformità dei trattamenti alle regole

- la deterrenza anche attraverso sanzioni: l'incremento decisivo dell'entità delle sanzioni amministrative pecuniarie (fino a 20 milioni di euro o al 4% del fatturato annuo mondiale) dimostra l'intento di disporre di un forte deterrente, rafforzando l'effettività d'insieme del sistema tra gli obblighi di responsabilizzazione

La descrizione di tali elementi testimonia della stretta connessione causale tra gli obblighi di responsabilizzazione del titolare del trattamento e la concreta protezione dell'interessato: nel sistema del GDPR, l'effettività della tutela non si colloca solo nel momento patologico e successivo della sanzione, ma caratterizza tutto il ciclo dinamico dell'esistenza del dato personale attraverso un approccio basato sul rischio. Il fulcro della tutela si sposta dalla conformità formale alle regole alla responsabilità in senso sostanziale: il titolare del trattamento non deve solo rispettare le norme, ma si deve mettere in grado di dimostrare di averlo fatto.

Pertanto, l'effettività della tutela nel contesto del GDPR non si esaurisce in una dimensione esclusivamente sanzionatoria, ma si sostanzia attraverso un'evoluzione del sistema della responsabilità civile verso logiche di *regulatory private law* (o diritto privato regolatorio)[12]. In questo concetto, che si colloca a cavallo tra il diritto privato e la regolamentazione pubblicistica, tra l'*hard* ed *il soft law*, il risarcimento del danno ex art. 82 GDPR non svolge solo una funzione compensativa, ma diventa uno strumento di tutela preventiva, volto a salvaguardare l'operatività effettiva del mercato unico digitale attraverso una responsabilizzazione sostanziale e in via preventiva del titolare.

La concreta attuazione della tutela dei dati personali sul versante normativo si manifesta, così, attraverso un regime probatorio particolarmente severo: come statuito dalla giurisprudenza di legittimità più recente, una volta che l'interessato abbia allegato la violazione e il danno, spetta al titolare fornire la prova rigorosa – secondo la dottrina, una vera e propria *probatio diabolica* - di aver adottato le misure tecniche e organizzative adeguate ai sensi degli artt. 24 e 32 del Regolamento.

L'onere della prova non è limitato, dunque, alla dimostrazione della mancanza di colpa, ma impone la dimostrazione che l'evento dannoso non sia in alcun modo imputabile al titolare, nonostante l'adozione di *standards* di sicurezza d'avanguardia[13].

Sulla base dei descritti elementi, il GDPR non può essere considerato come un semplice aggiornamento normativo, ma come una radicale trasformazione di prospettiva, che non enfatizza più solo l'originaria funzione risarcitoria della responsabilità civile, per accreditare un modello di precauzione e di cura sostanziale e preventiva. Tale modello si basa sull'analisi dei rischi, sulla

[12] Per un inquadramento sistematico dell'evoluzione descritta nel testo, si veda: ALONZO, "Il risarcimento del danno per violazione del GDPR (art. 82 Reg. UE 2016/679). La tutela della persona nelle logiche del diritto privato regolatorio?", in *Nuove leggi civ. comm.*, 2024, 601 ss.; nonché TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Milano, 2019.

[13] In merito all'onere probatorio e alla sua gravosità per il titolare, si veda Cass. Civ., Sez. I, 8 luglio 2025, n. 18583 (con riferimento ai termini procedurali innanzi al Garante).

trasparenza delle strutture decisionali e sulla tracciabilità dei processi, con l'intento di portare a compimento lo sviluppo del diritto alla *privacy* da semplice tutela contro le ingerenze altrui a diritto strutturalmente proattivo, realizzabile come garanzia in via sostanziale e preventiva.

Ne risulta, indubbiamente, un potenziamento dei rimedi a disposizione degli interessati. All'approccio principalmente formale e centrato su adempimenti minimi, il GDPR sostituisce un modello sostanziale, imperniato sul principio di *accountability* e su quello della dimostrabilità delle cautele adottate. Il mutamento di prospettiva del Regolamento tende a superare la frammentazione delle discipline nazionali, attraverso un'armonizzazione con ricorso diretto e rimedi uniformi. L'ambito delle sanzioni applicabili non è più solo simbolico e poco dissuasivo sul piano economico, ma contempla sanzioni maggiormente effettive.

5. Il contributo della giurisprudenza unionale e italiana.

Il significato intrinseco dell'effettività della tutela dei dati personali ha trovato ampia e autorevole conferma nelle più recenti pronunce della Corte di Giustizia dell'Unione Europea, che hanno cercato di fronteggiare e di rimuovere la frammentazione dei sistemi nazionali, nella misura in cui essi rappresentavano veri e propri ostacoli alla risarcibilità dei danni bagatellari.

A tale riguardo, la sentenza Österreichische Post (C-300/21) del 4 maggio 2023[14] ha rappresentato un traguardo fondamentale, avendo affermato che l'art. 82 GDPR osta a qualsiasi normativa o prassi nazionale che subordini il risarcimento del danno immateriale al superamento di una determinata "soglia di gravità". Questa interpretazione ha alimentato un acceso dibattito dottrinale, spesso definito come una specie di "guerra tra le corti", in merito alla persistenza dei filtri selettivi basati sulla limitatezza o futilità del danno[15].

Il sistema europeo, tendente alla massima effettività, riconosce che anche la sola perdita di controllo sul dato o il timore di un futuro utilizzo abusivo a seguito di un determinata violazione dei dati personali (perdita, intrusione o fuga), come affermato da CGUE C-340/21, possono integrare un danno immateriale risarcibile, purché ne venga dimostrata l'esistenza in concreto, sia pure minima.

Un tale approccio è stato ulteriormente consolidato dalla sentenza nella causa C-200/23 del 4 ottobre 2024, che ha ribadito la funzione autonomamente compensativa del risarcimento, impedendo che l'ottenimento di rimedi correttivi o inibitori possa essere considerato dal giudice per ridurre l'entità del ristoro pecuniario dovuto all'interessato[16].

Anche nel sistema italiano si può considerare convintamente recepito il criterio dell'effettività della tutela anche in questo settore. Si è assistito, sul

[14] V. sentenza CGUE, 4 maggio 2023, causa C-300/21, *UI c. Österreichische Post AG*.

[15] In dottrina, sul superamento della soglia di gravità, PAGLIANTINI, "Un altro palcoscenico della 'guerra' tra le corti: il danno (immateriale) bagatellare dell'art. 82 Gdpr", in *Foro it.*, 2023, 288 ss.; PATTI, "Il risarcimento del danno immateriale secondo la Corte di giustizia", in *Nuove leggi civ. comm.*, 2023, 1112 ss.

[16] Nel senso dell'estensione del concetto di responsabilità al danno da "timore" e a quello da perdita di controllo,si vedano le sentenze citate nel testo: CGUE, 14 dicembre 2023, causa C-340/21, *Natsionalna agentsia za prihodite* e CGUE, 4 ottobre 2024, causa C-200/23, *Agentsia po vpisvaniyata*

piano del “diritto vivente”, all’evoluzione da una concezione restrittiva del danno non patrimoniale ad un modello di tutela tendenzialmente più piena.

Se ancora nel 2021 la Corte di Cassazione (ordinanza n. 16402/2021) ha richiamato il principio di solidarietà, di cui all'art. 2 Cost., per porre un filtro i danni bagatellari o "futili" e richiedere una "gravità della lesione", l’evoluzione decisiva si è avuta in tempi più recenti. Con l'ordinanza n. 13073 del 12 maggio 2023, la Suprema Corte ha chiarito che l'effettività della protezione esige il risarcimento di ogni lesione concreta alla portata del diritto fondamentale, abbandonando la logica dei filtri minimi, pur mantenendo ferma la necessità di provare il pregiudizio almeno attraverso presunzioni semplici, in relazione alla tipologia del dato e al contesto della violazione[17]. La S.C., allineandosi alla CGUE, ha affermato: 1) la tutela dei dati è un diritto fondamentale protetto a livello costituzionale (Artt. 2 e 21 Cost.) e sovranazionale (Art. 8 CEDU); 2) il danno va risarcito anche se la lesione è marginale, poiché l'effettività del diritto alla protezione dei dati esige che ogni offesa concreta alla portata effettiva del diritto trovi una risposta sanzionatoria; 3) pur dovendosi negare la configurabilità di un danno *in re ipsa*, è ammissibile il ricorso alla prova presuntiva, basata sulla tipologia del dato (es. dati sanitari) e sul contesto della violazione.

Questo approccio assicura concreta ed efficiente tutela, semplificando l'onere probatorio per il danneggiato, che può fondare la propria pretesa su ragionamenti logico-inferenziali, senza dover fornire prove dirette di ingenti sofferenze psicologiche.

Un esempio emblematico e significativo di come questo concetto di effettività possa operare nel mercato digitale è costituito dall'ordinanza n. 6433 del 18 marzo 2026[18] in tema di diritto all'oblio, con la quale la S.C. ha stabilito che la tardiva deindicizzazione, da parte di un diffusissimo motore di ricerca, lede per sua natura la dignità sociale dell'individuo, rendendo il risarcimento uno strumento indispensabile per restituire l’effettività al controllo informativo del soggetto interessato, indipendentemente dalla rimozione tardiva del link, la quale non estingue il danno già maturato. Questa decisione dimostra che l'effettività si realizza anche attraverso la responsabilizzazione dei custodi dell'informazione digitale *(gate keeper)*, imponendo loro tempi certi e risposte concrete alle istanze degli interessati.

[17] In ordine all’evoluzione giurisprudenziale delineata nel testo, si veda Cass. Civ., Sez. VI, ord. 10 giugno 2021, n. 16402, per la tesi oggi superata, e Cass. Civ., Sez. I, ord. 12 maggio 2023, n. 13073, sulla più recente e coerente impostazione, secondo cui, in tema di illecito trattamento dei dati personali, l'esclusione del principio del danno "in re ipsa" presuppone la prova della serietà della lesione conseguente al trattamento; ne consegue che può non determinare il danno la mera violazione delle prescrizioni formali in tema di trattamento del dato, mentre induce sempre al risarcimento quella violazione che, concretamente, offenda la portata effettiva del diritto alla riservatezza.

[18] Per l'applicazione al diritto all'oblio e ai motori di ricerca, Cass. Civ., Sez. I, ord. 18 marzo 2026, n. 6433, con commento di PUCCI, "Diritto all'oblio: Cassazione su danno e motori di ricerca", in *GiuriCivile*, 2026. Secondo tale decisione, Ii giudice di merito deve valutare se la permanenza *online* di dati non più pertinenti leda per sua natura la dignità sociale; il danno può essere desunto dalla diffusione dello scritto, dalla rilevanza dell'offesa e dalla posizione sociale della vittima.

6 Conclusioni: Le sfide future e il consolidamento del diritto.

Il percorso storico fin qui tratteggiato lascia intravedere un progressivo ed inarrestabile potenziamento del principio di effettività nella tutela della *privacy*, evolvendo da una visione semplicemente reattiva e risarcitoria, operante a posteriori, verso un approccio proattivo, più concreto e preventivo, che ha trovato nel GDPR il suo momento di massima espressione.

Tuttavia, le sfide e gli ostacoli verso una tutela efficace non appaiono affatto superati, ma si convertono in tensioni verso nuovi traguardi, che richiedono un costante adattamento del quadro regolatorio ed una continua attenzione verso il raggiungimento di un idoneo equilibrio tra le esigenze del crescente sviluppo dell'innovazione tecnologica e quelle di tutela dei diritti fondamentali dei singoli.

Il bilanciamento tra l'effettività della tutela e la libera circolazione dei dati, la gestione dei dati in contesti transnazionali e l'adattamento delle norme alle nuove tecnologie (prima fra tutte, l'intelligenza artificiale) rappresentano, invero, i fronti su cui si misurerà, fin da oggi, la capacità del diritto alla riservatezza di offrire una tutela dei dati davvero effettiva.

Infatti, in primo luogo, il delicato bilanciamento tra l'effettività della tutela e la libera circolazione dei dati continua a rappresentare un nodo cruciale da sciogliere, specialmente in un'economia di carattere globale, basata sulla circolazione e sulla monetizzazione delle informazioni.

La gestione dei dati in ambiti transnazionali, resa sempre più complessa dalla divergenza e dalla frammentazione tra i quadri normativi nazionali (si pensi alla richiamata giurisprudenza della CGUE sui trasferimenti di dati verso gli USA), continua a rappresentare un terreno di scontro in continua evoluzione.

Infine, l'adattamento delle norme alle nuove tecnologie, con l'intelligenza artificiale (IA) *in primis*, pone rilevanti interrogativi sull'effettività del controllo sui dati, in presenza di algoritmi opachi e di possibili decisioni automatizzate[19]. L'intelligenza artificiale, attraverso la sua capacità di rendere nuovamente identificabili dati anonimi e di dedurre informazioni riservate tramite l'analisi automatizzata, rischia di svuotare di significato molti dei principi su cui si fonda l'attuale regolamentazione della materia qui esaminata, trasformando l'effettività della tutela - oggi come e ancor più che in passato – in un'incessante corsa contro il tempo. Le sfide sull'effettività della tutela nei dati personali sono, perciò, strettamente connesse ai concetti di trasparenza algoritmica e della sua spiegabilità (*explainability*).

L'effettività della tutela rispetto ai processi decisionali automatizzati (Art. 22 GDPR) si realizza garantendo all'interessato il diritto di conoscere in anticipo la logica del trattamento e di contestare la decisione. In assenza di questi basilari elementi di trasparenza[20], il diritto alla protezione dei dati rischierebbe di rimanere senza efficace garanzia rispetto alla complessità computazionale

[19] AA.VV., *Privacy and Consent. A Legal and UX&HMI Approach*, a cura di L. GATT, R. MONTANARI, I.A. CAGGIANO Napoli, 2021; L. GATT, The contradictions of the privacy law, in EJPLT, 2020, Special Issue; L. GATT, I.A. CAGGIANO, *Consumers and Digital Environments as a Structural Vulnerability Relationship*, EJPLT, 2022, 2, 8-16; V. RICCIUTO, *L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022.

[20] In ordine alla trasparenza algoritmica, oltre all'articolo 22 del GDPR, assumono gli articoli 13, 14 e 22 del medesimo regolamento, realizzando che l'informativa includa "informazioni significative sulla logica utilizzata".

degli algoritmi opachi. La messa in opera del *Data Governance Act* [21] e l'integrazione di nuove piattaforme di condivisione di dati richiedano una gestione comune del rischio per mantenere inalterata l'effettività della protezione.

In contesti caratterizzati dalla sempre maggiore diffusione dell'intelligenza artificiale, l'effettività della tutela potrà essere meglio garantita da un'evoluzione della figura del Responsabile della Protezione dei Dati (RPD), prevista come obbligatorio per enti pubblici, soggetti che monitorano dati su larga scala o gestiscono dati sensibili, che non agisca più solo come semplice supervisore tecnico o garante formale, ma assuma il ruolo di "catalizzatore di visioni". In questa nuova veste, il RPD potrà divenire il soggetto incaricato di assicurare che l'innovazione tecnologica non possa ledere né limitare la dignità umana, fungendo da efficiente ed adeguato raccordo tra le esigenze della produttività e la conformità della protezione dati fin dalla progettazione dei sistemi di IA più complessi.

Di fronte a tutte queste sfide, il ruolo delle autorità di controllo e della giurisprudenza europea e nazionale continuerà ad essere decisivo per assicurare che il diritto alla protezione dei dati personali rimanga un pilastro fondamentale delle libertà civili nel XXI secolo.

L'approccio proattivo dell'*accountability*, con i propri strumenti di progettazione (*privacy by design*) e di valutazione preventiva (DPIA), rappresenta soltanto l'inizio di un percorso che richiederà impegno ed ideazione costanti, per far sì che la tutela effettiva non sia solo un'utopia, ma una realtà tangibile e difendibile per ogni individuo nell'era dei *big data*.

[21] La dottrina ha analizzato l'interconnessione tra il GDPR e il Regolamento (UE) 2022/868 (DGA), evidenziando la necessità di una gestione integrata del rischio nelle piattaforme di condivisione o di scambi di dati: G. FINOCCHIARO, in *Intelligenza artificiale. Quali regole*?, Bologna,, 2024, ha evidenziato come il DGA non sostituisca il GDPR, ma vi si sovrapponga, rendendo necessario un bilanciamento tra la libera circolazione dei dati e la tutela dei diritti fondamentali, mediante il ricorso a modelli evoluti di responsabilità e gestione del rischio; F. BRAVO, *"Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act"*, in *Contratto e impresa Europa*, 1/2021, analizza specificamente il passaggio normativo e l'integrazione tra i due regolamenti nel contesto dei servizi di scambio dati; secondo M.C. POLLICINO, in Gli effetti della 'sommatoria' tra il GDPR e il nuovo Regolamento sulle intelligenze artificiali nell'ambito dell'attività amministrativa", *Rivista italiana di informatica e diritto*, 7(1), pp. 231–256, il nuovo approccio europeo (DGA, Data Act, AI Act) richieda di superare la visione "a silos" della conformità. Il rischio non riguarda più solo l'interessato, come profilo di privacy, ma anche la sicurezza industriale, la neutralità degli intermediari e la competitività del mercato.