

Protezione dei dati personali e pluralità dei poteri pubblici: il coordinamento tra tutela inibitoria, sanzioni amministrative e responsabilità civile nel GDPR

di Gianluca Bellomo

Title: Personal data protection and the plurality of public powers: coordinating injunctive relief, administrative sanctions and civil liability under the GDPR

Keywords: Regulation (EU) 2016/679; Non-material damage; Data protection authorities

1. – La pronuncia qui in commento si colloca nel cuore del dibattito, ormai maturo, sul modo in cui il diritto fondamentale alla protezione dei dati personali – sancito dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea e dall'art. 16 del Trattato sul Funzionamento dell'Unione europea – viene reso effettivo attraverso un sistema di rimedi che intreccia, in modo strutturale, poteri delle autorità amministrative indipendenti e tutela giurisdizionale decentrata. In dottrina è stato da tempo rilevato come la protezione dei dati non si esaurisca in una rilettura “aggiornata” della tradizionale privacy, ma configuri un vero e proprio diritto fondamentale della persona dotato di una propria architettura di garanzie, nella quale il controllo di un'autorità indipendente costituisce componente intrinseca del contenuto del diritto, accanto alle azioni esperibili dinanzi ai giudici nazionali (cfr. M. Gambini, *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *Esp. Jurídico*, 2013, 149-155; in senso conforme, anche con specifico riferimento al ruolo delle Autorità di controllo quali garanti di un interesse pubblico europeo alla protezione dei dati personali, F. Pizzetti, *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni*, in *MediaLaws*, 2018, n. 1, 107-112; più di recente, sul nesso tra autonomia del diritto alla protezione dei dati personali e tutela della dignità umana, A. Vertuccio, *Diritto alla protezione dei dati personali e dignità umana: “profili di una pregnante correlazione”*, in *Riv. dir. media*, 2025, n. 1, 116-120).

In questa chiave, il *Manual on European Data Protection Law* elaborato dall'Agenzia dell'Unione europea per i diritti fondamentali, dal Consiglio d'Europa e dal Garante europeo per la protezione dei dati sottolinea come il sistema delineato dal «Regolamento (UE) 2016/679» (di seguito, “GDPR” dall'acronimo inglese) si articoli lungo un doppio binario: da un lato, il reclamo all'autorità di controllo e i suoi poteri correttivi e sanzionatori; dall'altro, il diritto ad un ricorso effettivo dinanzi ai giudici, in attuazione dell'art. 47 della Carta dei diritti fondamentali dell'Unione europea, con particolare riguardo alle azioni contro i titolari del trattamento e contro le stesse autorità (cfr. EU Agency for

Fundamental Rights – Council of Europe – European Data Protection Supervisor, *Manual on European Data Protection Law*, Luxembourg, Publications Office of the European Union, 2018, 238 ss.). È su questo sfondo che la dimensione giuspubblicistica della protezione dei dati viene letta non come mero corollario organizzativo, ma come elemento strutturale del diritto stesso, che implica un'amministrazione indipendente, dotata di poteri tecnici e discrezionali, inserita in una rete europea di cooperazione (artt. 51-63 GDPR).

In dottrina è stato efficacemente proposto di parlare, in tale contesto, di una vera e propria “proceduralizzazione” dei rimedi in materia di *data protection*, nella quale il contenuto sostanziale del diritto è inseparabile dai meccanismi di tutela amministrativi e giurisdizionali che lo sorreggono. È stato osservato, in particolare, che il sistema dei rimedi si sviluppa su tre livelli: i diritti esercitabili direttamente nei confronti del titolare o del responsabile del trattamento; il controllo assegnato alle autorità di protezione dei dati, dotate di poteri quasi-giurisdizionali; il sindacato dei giudici nazionali e della Corte di giustizia, chiamati a garantire l'effettività dell'intero assetto (cfr. A. Galetta, P. De Hert, *The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-oriented Remedial System?*, in 8 *Rev. Eur. Admin. L.* 125 (2015). Più di recente, una ricostruzione sistematica dei rimedi amministrativi e giurisdizionali previsti dagli artt. 77-82 GDPR è offerta da C.T. Ungureanu, *Legal Remedies for Personal Data Protection in European Union*, in 14 *Acta Univers. Danub. Jur.* 32 (2018). La protezione dei dati personali si presenta, così, come laboratorio privilegiato di un più ampio “diritto amministrativo europeo dei rimedi”, nel quale le tecniche di tutela non sono solo private, ma costruite, anzitutto, come poteri e procedimenti delle autorità indipendenti.

Sul versante italiano, è stato messo in luce come la tutela del diritto alla protezione dei dati personali si collochi stabilmente all'incrocio tra autorità indipendenti e giudici nazionali, secondo un modello di alternatività solo parziale tra reclamo al Garante e azione giurisdizionale, che riflette il doppio volto – soggettivo e oggettivo – del diritto in questione: da un lato, come posizione individuale azionabile in giudizio, anche ai sensi dell'art. 82 GDPR; dall'altro, come interesse pubblico alla corretta regolazione dei flussi informativi, affidato alla vigilanza del Garante per la tutela dei dati personali e del Comitato europeo (cfr. F. Parodo, *La tutela del diritto alla protezione dei dati personali: l'effettività dei rimedi e il ruolo nomofilattico del Comitato europeo per la protezione dei dati personali*, in *federalismi.it*, n. 2021, n. 21, 112-115). Da questa prospettiva, il GDPR appare come un terreno in cui si sperimenta una forma di “amministrazione composita” europea, in cui le autorità nazionali cooperano tra loro e con il livello sovranazionale nella definizione e nell'applicazione dei rimedi.

Parallelamente, sul piano del *private enforcement*, è stato rilevato come l'azione di responsabilità *ex art. 82 GDPR* tenda ad assumere una portata sempre più generale, destinata a confrontarsi con dinamiche di contenzioso seriale e con strumenti di tutela collettiva, in parziale analogia con quanto accade nel diritto antitrust. In questa direzione si muove, ad esempio, l'analisi della dimensione transnazionale del contenzioso in materia di dati personali, che mette in luce il ruolo centrale delle azioni civili, anche collettive, nella costruzione di un *enforcement* effettivo accanto all'intervento delle autorità (cfr. F. Ragno, *Il diritto fondamentale alla tutela dei dati personali e la dimensione transnazionale del private enforcement del GDPR*, in *Ord. internaz. dir. umani*, 2020, 824 ss.). In prospettiva comparata, è stato altresì sottolineato il parallelismo – e le differenze – tra l'evoluzione del *private enforcement* nel settore della concorrenza e in quello della protezione dei dati, con particolare riguardo al rapporto tra azioni risarcitorie individuali, azioni collettive e sanzioni amministrative (cfr. W. Wurmnest, M. Gömann, *Comparing Private Enforcement of EU Competition and Data Protection*

Law, in 13 *J. Eur. Tort L.* 176 (2022); nonché M. Federico, *European Collective Redress and Data Protection. Challenges and Opportunities*, in *Riv. dir. media*, 2023, n. 1, 90 ss.).

È in questo quadro teorico – segnato da una crescente integrazione tra rimedi amministrativi e rimedi civili, e da una forte attenzione al ruolo delle autorità indipendenti come garanti di un diritto fondamentale “procedimentalizzato” – che si inserisce la sentenza *IP c. Quirin Privatbank AG*. La pronuncia è chiamata a chiarire, in particolare, (i) se dal GDPR derivi un vero e proprio diritto soggettivo all’ingiunzione inibitoria in capo all’interessato, distinto dal diritto al risarcimento del danno; (ii) quale rapporto sistematico si stabilisca tra tale eventuale azione inibitoria, i poteri correttivi delle autorità di controllo e l’azione risarcitoria ex art. 82; (iii) in che misura la funzione del risarcimento sia esclusivamente compensativa o possa assolvere anche a compiti deterrenti, in concorso con il sistema delle sanzioni amministrative. La risposta che la Corte offre a tali interrogativi incide direttamente sull’equilibrio tra *public enforcement* (affidato alle autorità di controllo) e *private enforcement* (fondato sulle azioni individuali e collettive), e dunque sul modo in cui si configura, in concreto, un vero e proprio “diritto amministrativo europeo dei rimedi” in materia di protezione dei dati personali.

2. – La vicenda concreta in cui tali nodi sistematici vengono al pettine è, in apparenza, di ordinaria amministrazione. IP manifesta interesse, tramite un *social network professionale*, per un posto presso la *Quirin Privatbank*. Una dipendente dell’istituto avvia le trattative utilizzando il sistema di messaggistica interna e gli indirizza un messaggio con il quale respinge le pretese retributive formulate e avanza una controproposta salariale più bassa. Per un errore di instradamento, tuttavia, il messaggio non giunge al candidato, bensì a un terzo: un collega del medesimo settore, che conosce personalmente IP e che, stupito dal contenuto, glielo inoltra chiedendogli se sia in cerca di una nuova occupazione.

È su questo incidente, solo in apparenza banale – ma potenzialmente lesivo per la reputazione e la posizione concorrenziale dell’interessato nella propria cerchia professionale – che si innesta l’interrogativo, ben più generale e di immediato interesse pubblicistico, sull’architettura dei rimedi e sul riparto di funzioni tra giudici ordinari e autorità di controllo nel sistema del GDPR. Dinanzi al *Landgericht Darmstadt* (tribunale regionale di primo grado), IP chiede, da un lato, un’ingiunzione a che la banca si astenga da qualsiasi futura divulgazione illecita dei dati relativi alla candidatura; dall’altro, il risarcimento del danno non patrimoniale ex art. 82 GDPR, lamentando l’ansia per ulteriori possibili diffusioni, il pregiudizio concorrenziale nel mercato del lavoro qualificato e l’umiliazione connessa alla circolazione, presso terzi, dell’esito delle trattative e del livello retributivo negoziato. Il giudice di primo grado accoglie entrambe le domande; l’*Oberlandesgericht* (corte d’appello regionale), in appello, conferma la tutela inibitoria ma nega il risarcimento, ritenendo non dimostrato un pregiudizio immateriale «serio» e giuridicamente apprezzabile.

Investito dei ricorsi di entrambe le parti, il *Bundesgerichtshof* (Corte federale di giustizia) sospende il giudizio e sottopone alla Corte di giustizia sei questioni pregiudiziali, che – se considerate nella prospettiva del disegno complessivo di tutela e dell’assetto dei poteri pubblici coinvolti – si lasciano raggruppare attorno a tre direttrici principali.

In primo luogo, viene in rilievo la configurabilità, nel diritto dell’Unione, di un autonomo diritto soggettivo all’ingiunzione ad astenersi da future violazioni, desumibile o meno dagli artt. 17, 18, 79 e 84 GDPR, nonché le condizioni del suo esercizio (in particolare il requisito, o la presunzione, del rischio di reiterazione) e

il margine lasciato agli ordinamenti nazionali nel predisporre rimedi inibitori ulteriori: è il profilo che interroga più direttamente il sistema multilivello di tutela giurisdizionale dei diritti fondamentali alla protezione dei dati.

In secondo luogo, il giudice del rinvio chiede quale relazione debba instaurarsi tra tale eventuale azione inibitoria davanti al giudice ordinario, i poteri correttivi delle autorità indipendenti di controllo e l'azione risarcitoria *ex art. 82*: qui il problema è il coordinamento, in chiave di effettività ed equivalenza, tra *enforcement* amministrativo e tutela giurisdizionale individuale, nonché la delimitazione funzionale delle rispettive sfere di intervento.

In terzo luogo, le questioni attengono alla fisionomia del danno non patrimoniale e alla sua funzione nel sistema: se rientrano nell'ambito dell'art. 82 anche i meri sentimenti negativi (rabbia, inquietudine, paura) o sia richiesta una soglia minima di gravità ulteriore rispetto al normale disagio esistenziale; quale rilievo assuma il grado di colpa del titolare o del responsabile, tanto ai fini dell'*an* quanto della quantificazione; e se, infine, il riconoscimento di un'ingiunzione ad astenersi possa incidere in diminuzione sul *quantum* del risarcimento, così da modulare – in combinazione con le sanzioni amministrative – la complessiva funzione anche deterrente del rimedio civilistico.

3. – Sul primo raggruppamento di questioni pregiudiziali, la Corte costruisce una risposta solo in apparenza “modesta”, che in realtà ridisegna l'intera architettura dei rimedi. Il *Bundesgerichtshof* domanda se dal GDPR emerga, per l'interessato che non chieda la cancellazione o la limitazione, un autonomo diritto ad ottenere in giudizio un'ingiunzione preventiva che vieti la reiterazione del trattamento illecito e, in caso negativo, se il regolamento osti alla previsione, nel diritto interno, di un'azione inibitoria fondata su norme nazionali di responsabilità (punto 36). Il percorso argomentativo è scandito da due passaggi chiave. Anzitutto, la Corte ribadisce che il GDPR si fonda sul riconoscimento di un diritto fondamentale alla protezione dei dati personali, che deve essere garantito ad un livello elevato e omogeneo in tutti gli Stati membri (punto 38), e che gli obblighi posti dal capo II in capo al titolare del trattamento trovano il loro contraltare in diritti soggettivi delle persone interessate. Ne deriva, in termini espliciti, un vero e proprio “diritto ad un trattamento lecito” dei dati personali, quale corollario dell'obbligo generale di non trattare i dati in modo non conforme al regolamento (punto 40), in linea con la ricostruzione proposta dall'Avvocato generale, che deduce questo diritto direttamente dai principi di liceità e correttezza degli artt. 5, par. 1, lett. a), e 6, par. 1, GDPR letti alla luce dell'art. 8 della Carta dei diritti fondamentali dell'Unione europea (parr. 35-40, conclusioni).

Su questo sfondo, entra in gioco il secondo pilastro del ragionamento: la Corte richiama la propria giurisprudenza secondo cui il diritto dell'Unione, di regola, non impone agli Stati membri di istituire rimedi nuovi rispetto a quelli esistenti, salvo che dall'economia dell'ordinamento interno emerga l'assenza di qualunque mezzo idoneo ad assicurare, anche solo in via incidentale, la tutela dei diritti conferiti dall'Unione (punto 41). È in questa chiave che viene letta la domanda tedesca: la situazione non concerne misure cautelari, ma la possibilità di una azione di merito a carattere preventivo volta ad ottenere un'ingiunzione di non reiterazione del trattamento illecito (punto 42). La Corte constata che il GDPR non contiene alcuna disposizione che riconosca, esplicitamente o implicitamente, un diritto dell'interessato ad ottenere in via preventiva un ordine giudiziale che imponga al titolare di astenersi, in futuro, dal violare il regolamento, e nega che un tale diritto possa essere ricavato dagli artt. 17 e 18 GDPR, nonostante la lettura estensiva proposta dall'Avvocato generale (punto 43; parr. 54-69, conclusioni). Analoga è la conclusione quanto al capo VIII: né la struttura sistematica, né il tenore letterale dell'art. 79, par. 1 – che garantisce un

“ricorso giurisdizionale effettivo” ma non tipizza la forma della tutela – obbligano gli Stati a prevedere una specifica azione inibitoria preventiva (punti 44-45). Tuttavia, proprio il rinvio “fatto salvo” ad ogni altro ricorso amministrativo o extragiudiziale e l’assenza di una clausola di chiusura nel capo VIII sono letti come indice del fatto che agli Stati membri non è precluso introdurre, accanto ai rimedi armonizzati, ulteriori azioni, incluso un ricorso preventivo volto ad ottenere un’ingiunzione di astensione, purché nel rispetto dei principi di equivalenza ed effettività (punti 46-48, con richiamo a *Lindenapotheke*, C-21/23). In prospettiva comparata, la soluzione della Corte legittima la tradizione tedesca, in cui l’azione inibitoria si radica nell’analogia con i §§ 823 e 1004 BGB per la tutela dei diritti della personalità, ma è perfettamente compatibile anche con modelli – come quello italiano – nei quali la protezione preventiva passa per la combinazione fra diritti sostanziali di fonte unionale, rimedi processuali generali (art. 700 c.p.c., responsabilità aquiliana *ex* art. 2043 c.c.) e poteri correttivi e interdittivi dell’autorità indipendente (art. 58 GDPR, art. 152 Codice privacy). Ne risulta accentuata la dimensione pubblicistica del sistema: più che cristallizzare un catalogo uniforme di azioni soggettive, il diritto dell’Unione prefigura una trama di poteri e procedimenti – giudiziali e amministrativi – entro la quale gli ordinamenti nazionali restano chiamati a modellare, secondo le proprie tecniche di tutela inibitoria, l’effettività del diritto fondamentale ad un trattamento lecito dei dati personali (punto 49).

4. – Il secondo raggruppamento di questioni pregiudiziali ruota attorno alla nozione di «danno immateriale» *ex* art. 82, par. 1, GDPR e al problema, tipicamente “civilistico-costituzionale”, dell’eventuale soglia minima di gravità del pregiudizio risarcibile. La Corte, muovendo dalla tecnica ormai consolidata dell’“autonomia concettuale” del diritto dell’Unione, afferma anzitutto che la nozione di danno immateriale deve ricevere una definizione uniforme a livello europeo, non rinviando l’art. 82, par. 1, a categorie nazionali (punto 55). A partire dalla propria giurisprudenza recente (*Österreichische Post, Agentsia po vpisvaniyata, PS*), la Corte ribadisce poi il tritico dei presupposti cumulativi: esistenza di un danno, materiale o immateriale, violazione del regolamento e nesso causale tra i due (punto 56). Ne discende, in negativo, il rigetto di ogni tentativo di introdurre, per via legislativa o giurisprudenziale, una “soglia di rilevanza” al di sotto della quale il danno immateriale non sarebbe risarcibile (punto 58): l’art. 82 non consente di subordinare il ristoro alla prova di un pregiudizio «serio» o «grave», come ipotizzato dal giudice del rinvio sulla base del diritto tedesco. In positivo, la Corte valorizza l’elenco esemplificativo dei considerando 75 e 85, includendo espressamente, tra i possibili danni, la “perdita di controllo” sui dati e il timore di un loro uso abusivo o di un pregiudizio reputazionale (punti 59-61); ciò che rileva è che l’interessato dimostri di provare *concretamente* quei sentimenti negativi – timore, insoddisfazione, umiliazione – e che tali stati d’animo siano causalmente ricollegabili alla violazione del GDPR (punti 62-63), come nel caso di una trasmissione non autorizzata a un terzo attivo nello stesso settore professionale. La risposta alla quarta questione consacra così un modello “estensivo ma non automatico”: da un lato, qualunque pregiudizio non patrimoniale, anche minimo, può integrare un danno immateriale risarcibile; dall’altro, non basta allegare la violazione, ma occorre dimostrare l’effettività, sia pure modesta, delle conseguenze negative sul piano psichico o relazionale (punto 64).

Questo approdo dialoga in modo serrato con il dibattito dottrinale, italiano e comparato, sulla natura del danno da illecito trattamento dei dati. Nella prospettiva internazionale-comparata, una parte rilevante della dottrina vede nell’art. 82 GDPR la codificazione di un modello di responsabilità per violazione di diritti fondamentali, nel quale l’idea stessa di *danno non patrimoniale* mal si

concilia con soglie rigide di rilevanza, perché i pregiudizi “minori” fanno strutturalmente parte del rischio digitale cui il regolamento mira a rimediare (cfr. G. Navone, *La costruzione dello statuto eurounitario del “danno immateriale”: la prima pietra della Corte di giustizia*, in *Ordines*, 2024, n. 1, 187 ss.; J. Knetsch, *The compensation of non-pecuniary loss in GDPR infringement cases*, in *Eur. J. Privacy L. & Tech.*, SI, 63 (2020)). In chiave più specificamente civilistica, lavori recenti dedicati al risarcimento del danno non patrimoniale da violazione della privacy (anche in ambito italiano) hanno criticato la tradizionale insistenza su “gravità della lesione” e “serietà del danno” come filtri di accesso alla tutela, sottolineando come, a fronte di un diritto fondamentale alla protezione dei dati, tali filtri rischino di produrre una sotto-compensazione sistematica dei pregiudizi emotivi e reputazionali (cfr. A. Lottini, *Risarcimento del danno immateriale a seguito della violazione del regolamento (UE) 2016/679: la sentenza Österreichische Post determina un cambio di paradigma?*, in *Quad. AISDUE*, 2023, n. 2, 6; G. Navone, *La costruzione dello statuto eurounitario del “danno immateriale”: la prima pietra della Corte di giustizia*, cit., 179-184). La linea tracciata dalla Corte in C-655/23 si colloca chiaramente su questo versante: la perdita di controllo informazionale e il timore di futura utilizzazione abusiva diventano figure-chiave del danno immateriale “digitale”, a condizione che siano provate nelle loro ricadute concrete. In tal senso, si comprende anche la crescente attenzione della dottrina europea ai profili probatori e valutativi del danno immateriale – dalla questione dell’eventuale *de minimis* alla frammentazione delle prassi nazionali – che mette in luce come la scelta della Corte di escludere soglie di gravità, pur coerente con la logica dei diritti fondamentali, accentui la tensione tra uniformità del concetto di danno e persistenza di metodi nazionali di quantificazione molto diversi. In prospettiva più prettamente pubblicistica, il messaggio è altrettanto chiaro: il diritto fondamentale alla protezione dei dati non si esaurisce nella reazione “amministrativa” del sistema sanzionatorio, ma genera una pretesa di ristoro individuale anche per quei pregiudizi che, nelle categorie tradizionali del danno non patrimoniale, sarebbero forse qualificati come “micro-offese” (cfr. A. Palumbo, *La tutela inibitoria*, Napoli, Jovene, 2010, 139-145).

5. – Il terzo raggruppamento di questioni investe, da un lato, il ruolo della gravità dell’illecito e della colpevolezza del titolare nella quantificazione del risarcimento, dall’altro, il rapporto tra risarcimento *ex art. 82* e ingiunzione di astensione, quando quest’ultima sia stata ottenuta in base al diritto nazionale. Sul primo versante (quinta questione), la Corte prende nettamente le distanze dalla tradizione – ben radicata, ad esempio, nel § 253 BGB e nella giurisprudenza tedesca – che assegna al risarcimento del danno immateriale una funzione anche satisfattivo-punitiva, collegando l’“ammontare” dell’indennizzo al grado di colpa dell’autore (punto 67). Dopo aver ricordato che, in mancanza di regole europee sulla *quantificazione* del danno, spetta al diritto nazionale disciplinarne le modalità nel rispetto dei principi di equivalenza ed effettività (punto 66), la Corte richiama la propria giurisprudenza per ribadire che il diritto al risarcimento *ex art. 82* ha una funzione esclusivamente compensativa: esso esige un ristoro «pieno ed effettivo» del pregiudizio concretamente subito, ma non mira ad infliggere “danni punitivi” né ad assumere una funzione deterrente general-preventiva (punti 69-70). Di qui la conseguenza decisiva: la gravità e l’eventuale carattere intenzionale della violazione, così come l’atteggiamento soggettivo del titolare, non possono essere presi in considerazione per ridurre o modulare l’importo del risarcimento dovuto (punti 71-73). In altri termini, l’illecito è presupposto di responsabilità; una volta accertata la violazione e dimostrato il danno, l’indennizzo deve misurarsi solo sul pregiudizio subito, non sul “merito” o “demerito” dell’autore. La

dimensione sanzionatoria e dissuasiva viene “spostata” sul terreno delle sanzioni amministrative *ex art. 83 GDPR*, che prevedono espressamente – e soltanto in quel contesto – la rilevanza del grado di gravità e della colpa.

La sesta questione consente di completare il quadro, affrontando la tentazione – anch’essa ben nota al diritto tedesco (cfr. T.U. Amelung, *Damage Awards for Infringement of Privacy – The German Approach*, in 14 *Tul. Eur. & Civ. L. Forum* 19 (1999)) – di considerare l’ingiunzione di astensione come fattore di riduzione, o addirittura come «equivalente funzionale», del risarcimento del danno immateriale. La Corte ricostruisce con cura il problema: secondo il giudice del rinvio, il fatto che la vittima abbia ottenuto un’ingiunzione a non reiterare l’illecito potrebbe giustificare, nel diritto interno, una diminuzione del *quantum* o persino l’esclusione dell’indennizzo (punto 75). Chiamata a verificare se un simile criterio sia compatibile con l’art. 82 GDPR, la Corte torna a insistere sul principio della piena ed effettiva riparazione: le forme di ristoro riconosciute dal diritto nazionale, ivi comprese quelle “non pecuniarie”, sono ammissibili solo se garantiscono in concreto la compensazione integrale del pregiudizio subito (punti 78-81). Da qui il passaggio chiave: un risarcimento dovuto ai sensi dell’art. 82 non può essere concesso, in tutto o in parte, sotto forma di ingiunzione di astensione, perché tale misura ha una funzione esclusivamente preventiva, volta ad evitare nuovi danni, e non risarcisce quelli già verificatisi (punto 82). Nello stesso senso si muove l’Avvocato generale, che sottolinea come l’azione inibitoria presupponga un rischio di recidiva e miri a scongiurare ulteriori lesioni, mentre il danno immateriale riferibile al timore di reiterazione deve essere ristorato *a posteriori* e non “assorbito” dal successo dell’azione inibitoria stessa (parr. 86-88, conclusioni). Di conseguenza, la Corte afferma che l’ottenimento, in base al diritto nazionale, di un’ingiunzione di astensione non può essere utilizzato né per ridurre il risarcimento pecuniario né, *a fortiori*, per sostituirlo (punto 83).

Anche su questo terreno si innesta un ricco dialogo con la dottrina. In prospettiva comparata, vari autori hanno sottolineato come l’architettura del GDPR separi nettamente – almeno sul piano delle funzioni – il circuito compensativo (art. 82) da quello sanzionatorio-dissuasivo (art. 83) e da quello inibitorio/correttivo, affidato principalmente alle autorità di controllo (art. 58), con il rischio però di affidare quasi interamente la deterrenza al versante amministrativo, in un contesto di *enforcement* transnazionale spesso ineffettivo (cfr. H.C.H. Hofmann, L. Mustert, *Data protection*, in M. Scholten (cur.), *Research Handbook on the Enforcement of EU Law*, Cheltenham, 2023, 462-466 e 469-471). Sul versante del danno, la dottrina europea più recente ha evidenziato come l’insistenza della Corte sulla “purezza” compensativa dell’art. 82 rafforzi la centralità del pregiudizio individuale – materiale o immateriale – ma renda anche più difficile utilizzare il risarcimento come leva strutturale di conformazione dei comportamenti dei titolari (cfr. G. Gentile, O. Lynskey, «*Deficient by Design? The Transnational Enforcement of the GDPR*», in 71 *Intern. & Comp. L. Quart’y* 799 (2022)). In ambito italiano, dove il danno da illecito trattamento di dati personali è stato a lungo ricondotto, anche simbolicamente, alle categorie del danno non patrimoniale *ex art. 2059 c.c.* e della lesione della riservatezza (G. Sica, “*Responsabilità e “danno” da illecito trattamento dei dati personali. Il modello europeo all’indomani del caso VB c. NAP*”, in *Dir. Merc. Tec.*, 15 dicembre 2023, 1-17, reperibile in www.dimt.it), la linea giurisprudenziale rinvenibile nella sentenza C-655/23 impone di distinguere più nettamente tra funzioni di prevenzione (rimesse alle autorità indipendenti e alle azioni inibitorie nazionali) e funzione compensativa del risarcimento, pena la violazione dell’effetto utile dell’art. 82. In chiave pubblicistica, ciò significa che la tutela del diritto fondamentale alla protezione dei dati – così come ridisegnata dal combinato disposto delle sentenze *Österreichische Post*, *Agentsia po vprisvaniyata*, *Patērētāju tiesību aizsardzības centrs* e

ora C-655/23 – non è il prodotto di un unico “super-rimedio” europeo, ma il risultato di una trama complessa di strumenti: azioni risarcitorie ad alto tasso di individualizzazione del pregiudizio, poteri correttivi e sanzionatori delle autorità di controllo, azioni inibitorie di fonte nazionale. Il compito, per il legislatore e per la giurisprudenza nazionali – e qui i profili amministrativistici si riaffermano con forza – è quello di assicurare che questi tre piani restino tra loro coordinati, senza che né l’azione inibitoria né le sanzioni amministrative finiscano per comprimere, in fatto, la pienezza del ristoro garantito dall’art. 82 GDPR.

6. – In conclusione, la sentenza C-655/23 ha il merito non secondario di riportare il dibattito sul terreno che le è proprio: non quello – un po’ illusorio – della ricerca del “super-rimedio” europeo capace da solo di assicurare l’effettività del diritto alla protezione dei dati, ma quello, più realistico, della costruzione di un sistema multilivello di tutele, nel quale il diritto dell’Unione definisce le coordinate essenziali e gli ordinamenti nazionali restano responsabili dell’ingegneria dei rimedi. La Corte, da un lato, riconosce con chiarezza l’esistenza di un diritto ad un trattamento lecito dei dati personali (punto 40), ponendo così un tassello importante nella costituzionalizzazione sostanziale del GDPR; dall’altro, rifiuta di tradurre immediatamente tale diritto in un’azione inibitoria uniforme (punti 43-45), preferendo mantenere uno spazio, vigilato ma reale, per le tecniche domestiche – civilistiche e amministrative – di tutela preventiva. Il punto di forza della pronuncia sta proprio in questo equilibrio: mentre l’Avvocato generale spinge verso una massima “giuridificazione” del diritto all’astensione, la Corte preserva la flessibilità degli strumenti, ma al prezzo di una forte responsabilizzazione del legislatore e della giurisprudenza nazionali, vincolati dai principi di equivalenza ed effettività (punti 48-49).

Al tempo stesso, sul versante della responsabilità, la decisione consolida due assi portanti della giurisprudenza recente: l’assenza di qualsiasi soglia minima di gravità per il danno immateriale (punto 58) e la natura esclusivamente compensativa del risarcimento *ex* art. 82, separata tanto dalla funzione sanzionatoria-dissuasiva del sistema di *enforcement* amministrativo (art. 83) quanto dalla logica, anche simbolica, dei “danni punitivi” (punti 69-73, 82-83). Per gli ordinamenti europei – e per quello italiano in particolare – ciò implica, da un lato, la necessità di affinare gli strumenti probatori e valutativi del danno non patrimoniale “digitale”, superando approcci eccessivamente restrittivi; dall’altro, l’obbligo di ricalibrare il rapporto tra azioni inibitorie di fonte interna, poteri delle autorità indipendenti e rimedi risarcitori, evitando che l’una o l’altra forma di tutela venga utilizzata per comprimere, in fatto, il ristoro integrale garantito dall’art. 82. In prospettiva internazionale, la sentenza offre infine un modello interessante: un sistema che, pur respingendo la tentazione di trasformare il risarcimento in uno strumento di regolazione “punitiva” del mercato dei dati, eleva il danno immateriale – perdita di controllo, timore di uso abusivo, lesione reputazionale – a indicatore centrale di effettività, delineando un paradigma europeo che si colloca a metà strada fra la tradizione continentale di *civil liability* e l’esperienza, più spiccatamente deterrente, dei sistemi di *privacy litigation* di matrice statunitense (su cui cfr. L. Miglietti, *Profili storico-comparativi del diritto alla privacy*, in *Dir. comp.*, 4 dicembre 2014, reperibile in www.diritticomparati.it).

Gianluca Bellomo

Dipartimento di Scienze Giuridiche e Sociali

Università degli Studi “G. d’Annunzio” – Chieti/Pescara

gianluca.bellomo@unich.it