GIURETA
Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente
Vol. XXIII
2025

La giurisprudenza europea in materia di dati personali: continuità, innovazione e prospettive dopo la sentenza *Mousse*

Donatella Del Vescovo [*]

SOMMARIO: 1. Introduzione – 2. L'evoluzione del principio di minimizzazione dei dati nel contesto del diritto alla privacy – 3. Quadro normativo di riferimento – 4. Il principio di minimizzazione dei dati tra diritto italiano e ordinamenti esteri: prospettive a confronto e criticità emergenti – 5. La sentenza *Mousse*. I fatti e la questione pregiudiziale – 5.1. I principi di diritto enunciati dalla Corte – 5.2. Lo sviluppo giurisprudenziale pre-2025 in materia di protezione dei dati – 5.3. La sentenza *Mousse* vs. i *leading cases*: un confronto continuo su necessità e minimizzazione – 5.4. Il consolidamento di un paradigma restrittivo nel diritto europeo dei dati - 6. Considerazioni critiche, implicazioni sistemiche e prospettive - 7. Conclusioni.

1. – La protezione dei dati personali rappresenta uno degli ambiti più dinamici e complessi del diritto dell'Unione europea, in cui il costante avanzamento tecnologico e le esigenze pratiche dei diversi attori sociali ed economici si confrontano con la necessità di garantire il pieno rispetto dei diritti fondamentali [1]. Tra i principi cardine del Regolamento (UE) 2016/679, meglio noto come Regolamento Generale sulla Protezione dei Dati (RGPD) [2], quello di minimizza-

[*] Professore associato in Diritto dell'Unione Europea, Università di Bari

[1] Si v. tra i tanti Stefano Rodotà, *La privacy tra individuo e collettività*, in *Pol. dir.*, Bologna, 1974; G. D'Acquisto, M. Naldi, *Big Data e privacy by design*, Torino, 2017, 5; L. Chieffi, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee*, in *Federalismi.it*, 14 febbraio 2018, 6; V. Cuffaro, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e impresa* n. 3/2018, 1102; S. Sica, *La tutela dei dati personali*, in *Manuale di diritto dell'informatica*, Napoli, 2016, 97; G. La Rocca, *Appunti sul Regolamento UE n.679/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (parte 1*), in *Il Caso.it*, 9 settembre 2017, 5; G. Finocchiaro, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Bologna, 2017, 5; L. Bolognini, E. Pelino, C. Bistolfi, *Il Regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 104; E. Morozov, *Il mercato dei dati*, in *Internazionale*, 6 settembre 2013; Stefano Rodotà, *Intervista su privacy e libertà*, a cura di Paolo Conti, Roma-Bari, 2005, 8.

[2] Reg. 2016/679, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al

ISSN 1724-7322

zione dei dati (art. 5, par. 1, lett. c) si pone come parametro essenziale di proporzionalità: i dati personali devono essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati». Tale regola, sebbene apparentemente chiara, si presta a tensioni interpretative significative, specie quando il trattamento si inserisce in contesti quotidiani, apparentemente innocui, ma che possono rivelare profili discriminatori o sproporzionati.

La recente sentenza *Mousse* (C-394/23), pronunciata dalla Corte di giustizia dell'Unione europea il 9 gennaio 2025 [3], si colloca esattamente in questo crocevia. Il caso, relativo alla necessità per gli utenti di piattaforme di vendita online di titoli di trasporto, di scegliere obbligatoriamente tra gli appellativi "Signore" e "Signora", ha offerto alla Corte l'occasione di chiarire la portata del principio di minimizzazione in relazione alla base giuridica del legittimo interesse del titolare del trattamento (art. 6, par. 1, lett. f, RGPD). Secondo la Corte, la raccolta di tali dati non era giustificata da una necessità oggettiva, poiché esistevano modalità alternative di gestione della comunicazione con il cliente, meno invasive e più inclusive.

L'importanza della sentenza risiede non soltanto nell'oggetto specifico della controversia, ma soprattutto nella portata dei principi affermati. La Corte ha stabilito che il trattamento di dati personali, anche se apparentemente "banali" o "di cortesia", non può essere giustificato se non strettamente indispensabile per il perseguimento della finalità dichiarata. Inoltre, ha chiarito che il diritto di opposizione (art. 21 RGPD) non può essere invocato per sanare ex post un trattamento sproporzionato: l'analisi della necessità deve precedere la raccolta dei dati e non può essere sostituita dalla possibilità per l'interessato di opporsi successivamente [4].

trattamento dei dati personali, in g.u.u.e., L 119, 4.5.2016.

[3] Ceg., 9 gennaio 2025, C-394/23, *Mousse c. CNIL, SNCF Connect*, ECLI:EU:C:2025:2, punti 36-40.

[4] L'articolo 21 del RGPD riconosce all'interessato il diritto di opporsi, in qualsiasi momento, al trattamento dei propri dati personali quando questo si fonda sull'interesse pubblico, sull'esercizio di pubblici poteri o sul legittimo interesse del titolare o di terzi. In tali casi il titolare deve interrompere il trattamento, a meno che non dimostri motivi legittimi prevalenti o esigenze connesse alla tutela in sede giudiziaria. Un ambito particolare è quello del marketing diretto: qui l'opposizione è sempre possibile, senza condizioni, e riguarda anche le attività di profilazione connesse a finalità promozionali; una volta esercitato, il titolare non può più utilizzare i dati per tali scopi. L'interessato può inoltre opporsi ai trattamenti effettuati per fini di ricerca scientifica, storica o statistica, salvo che essi siano necessari per l'esecuzione di un compito di interesse pubblico. Infine, il regolamento impone al titolare l'obbligo di

La tesi centrale di questo saggio è che la sentenza *Mousse* rappresenti una svolta significativa nell'applicazione del principio di minimizzazione dei dati, consolidandone la funzione di parametro sostanziale e vincolante per la liceità dei trattamenti. Essa restringe i margini di discrezionalità delle imprese nell'invocare il "legittimo interesse" e rafforza il ruolo del giudice e delle autorità di controllo nell'assicurare che la protezione dei dati personali non sia sacrificata a favore di esigenze organizzative o consuetudinarie. In tal modo, la pronuncia contribuisce a delineare un nuovo equilibrio tra innovazione tecnologica, efficienza operativa e salvaguardia dei diritti fondamentali.

Il presente contributo si propone di sviluppare un'analisi critica della sentenza resa nel 2025, ponendola a confronto con i principali orientamenti giurisprudenziali che l'hanno preceduta e mettendone in evidenza le implicazioni di ordine sistemico.

L'indagine sarà articolata lungo quattro direttrici principali. In primo luogo, si procederà a una ricostruzione dell'evoluzione storica e concettuale del principio di minimizzazione dei dati, mettendo in luce il suo percorso di trasformazione: da canone etico-sociale, volto alla salvaguardia della dignità e della libertà individuale, a regola giuridica formalizzata, progressivamente adattata alle nuove sfide poste dall'innovazione tecnologica e dall'economia digitale.

In secondo luogo, si analizzerà il contesto normativo e giurisprudenziale che ha costituito il presupposto della decisione, con attenzione alle fonti del diritto europeo e alle principali linee interpretative che hanno preparato il terreno all'intervento della Corte.

In terzo luogo, l'attenzione sarà rivolta alla causa *Mousse* (C-394/23), esaminandone i contenuti innovativi e i principi affermati dalla Corte, nonché le eventuali discontinuità rispetto alla tradizione interpretativa consolidata.

Infine, si discuteranno le ricadute teoriche e applicative della pronuncia, valutandone l'impatto tanto per gli operatori economici quanto per il dibattito dottrinale e giuridico. In questa prospettiva, l'obiettivo sarà quello di verificare se e in quale misura la sentenza contribuisca a ridefinire la portata sistemica del principio di minimizzazione e la sua effettiva capacità di fungere da parametro di bilanciamento tra tutela dei diritti fondamentali e interessi economici e tecnologici di crescente rilievo.

informare chiaramente l'interessato, fin dal primo contatto, dell'esistenza di questo diritto di opposizione.

2. – Il principio di minimizzazione dei dati costituisce oggi uno dei cardini della disciplina giuridica in materia di protezione dei dati personali. Tuttavia, per comprendere appieno la portata e la funzione di tale principio, è necessario ripercorrerne le origini e l'evoluzione storica, che si collocano nel più ampio processo di consolidamento del diritto alla riservatezza e alla protezione dei dati personali.

Le prime manifestazioni di una consapevolezza giuridica rispetto alla necessità di limitare la raccolta e la conservazione dei dati personali si fanno strada negli anni Settanta del Novecento, con l'avvento e la progressiva diffusione dei sistemi informatici centralizzati. In tale contesto, soprattutto nei Paesi occidentali, cresce la preoccupazione per l'accresciuto potere delle amministrazioni pubbliche e delle grandi imprese di raccogliere, elaborare e conservare informazioni sugli individui in modo massivo, potenzialmente senza limiti né controlli [5]. Tali pratiche rischiavano di compromettere in modo irreversibile il diritto alla privacy, favorendo fenomeni di sorveglianza sistematica, profilazione indebita e discriminazione.

In risposta a tali istanze, la Comunità internazionale inizia a elaborare strumenti normativi volti a garantire un quadro di protezione dei dati personali. Un primo tentativo di regolamentazione sovranazionale si concretizza con l'adozione delle *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* nel 1980 [6], le quali rappresentano uno dei primi documenti internazionali volti a codificare principi fondamentali in materia di trattamento dei dati personali. Tra questi, il *Collection Limitation Principle* sancisce espressamente che «la raccolta dei dati personali deve essere limitata e deve avvenire mediante mezzi leciti e corretti, con il consenso dell'interessato o in base ad altro fondamento legittimo» [7]. Ana-

[5] G. Buttarelli, *Privacy e protezione dei dati personali: la dignità della persona nell'era digitale*, in *Federalismi.it*, 2017, 98.

[6] *OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Parigi, 23 settembre 1980, disponibile su: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[7] Il *Collection Limitation Principle*, principio di limitazione della raccolta, richiede che la raccolta di dati personali sia limitata a quanto necessario per lo scopo specificato e ottenuta con mezzi leciti e corretti, idealmente con la conoscenza o il consenso dell'interessato. Questo principio enfatizza la raccolta di dati solo in quantità adeguata e pertinente, evitando l'eccesso e conservando i dati solo per il tempo necessario..

logamente, il principio venne incluso nei principali strumenti normativi di protezione dei dati a livello globale, come il *Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)* [8] e l'*APEC Privacy Framework* [9].

Parallelamente, a livello europeo, le prime tracce giuridiche della tutela della privacy si rinvengono già nel XVIII secolo, con la filosofia dei diritti naturali in Germania [10] e con lo sviluppo del concetto di libertà negativa [11], che si lega all'idea di autodeterminazione e protezione da interferenze esterne. Nel corso del XIX e XX secolo, con l'affermazione dell'individualismo moderno, la privacy si emancipa dalla sua originaria connotazione legata alla proprietà per assumere un valore spirituale e personale, riconosciuto anche in ambito giuridico, come dimostrato dalla legislazione francese e dalle prime pronunce giurisprudenziali europee [12].

L'importanza del principio di minimizzazione trova una prima formalizzazione giuridica nella Convenzione n. 108 del Consiglio d'Europa del 1981

[8] La Legge canadese sulla protezione delle informazioni personali e dei documenti elettronici (*PIPEDA*) è una legge federale che disciplina le modalità di raccolta, utilizzo e divulgazione delle informazioni personali da parte delle organizzazioni del settore privato durante le attività commerciali. Mira a bilanciare il diritto alla privacy degli individui con le legittime esigenze delle organizzazioni di utilizzare le informazioni personali in modo responsabile.

[9] L'*APEC Privacy Framework* è un insieme di principi guida non vincolanti sviluppati dall'Asia-Pacifico Cooperazione Economica (APEC) per promuovere una protezione coerente della privacy dei dati personali tra le economie della regione Asia-Pacifico. Il *Framework* mira a bilanciare la tutela della privacy degli individui con gli interessi economici, evitando barriere inutili al flusso di informazioni e favorendo la crescita del commercio e dell'economia digitale nella regione.

[10] La filosofia dei diritti naturali è la dottrina secondo cui esiste un diritto fondato sulla natura dell'uomo o sulla ragione umana, che è precedente o superiore al diritto creato dallo Stato (diritto positivo). Questo diritto naturale non dipende necessariamente da leggi scritte: può valere anche se non formalizzato, perché è ritenuto universale, immutabile, valido per tutti gli uomini semplicemente per ragione o natura. Spesso si usa come criterio morale: le leggi dello Stato devono essere conformi a quei principi di giustizia, altrimenti possono essere considerate ingiuste o non autenticamente "legittime".

[11] Per "libertà negativa" si intende la condizione in cui un individuo è libero da interferenze esterne: libertà "da" vincoli, ostacoli o costrizioni, soprattutto da parte dello Stato o di altri soggetti. È diversa dalla "libertà positiva", che riguarda invece la capacità di autodeterminarsi, di essere padroni di sé o partecipare attivamente al governo di sé stessi e della comunità.

[12] M. Surace, *Analisi socio-giuridica del rapporto tra sorveglianza e diritto alla riservatezza nell'era di*

per la protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale [13]. L'articolo 5 della Convenzione infatti stabilisce che i dati devono essere «raccolti per finalità determinate e legittime e non utilizzati in modo incompatibile con tali finalità; ossia adeguati, pertinenti e non eccedenti rispetto alle finalità per cui sono conservati». Tale disposizione introduce in modo esplicito il criterio di "proporzionalità e necessità" che caratterizza in sostanza la nozione moderna di minimizzazione.

L'evoluzione normativa di fatto ha progressivamente trasformato questo diritto da semplice concetto etico e sociale a vera e propria situazione giuridica soggettiva protetta, oggi riconosciuta come diritto fondamentale sia a livello europeo – all'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea [14] – sia a livello internazionale – all'articolo 17 del Patto internazionale sui diritti civili e politici (1966) [15]. All'interno di questa cornice giuridica, il principio di minimizzazione rappresenta in sostanza uno strumento essenziale per garantire la proporzionalità del trattamento e la limitazione del potere informativo dei soggetti pubblici e privati nei confronti degli individui, fungendo da baluardo contro gli eccessi del trattamento automatizzato in epoca digitale. La sua applicazione effettiva ha richiesto dunque un approccio integrato e multidisciplinare, in cui le competenze giuridiche si affianchino a quelle tecnologiche e organizzative, in modo da assicurare un equilibrio concreto tra innovazione e tutela dei diritti fondamentali della persona [16].

L'affermazione del principio risulta in seguito ulteriormente rafforzata

Internet, in *Adir, L'altro diritto*, 2005, disponibile su https://www.adir.unifi.it/rivista/2005/surace/.

[13] Convenzione per la protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione n. 108 del Consiglio d'Europa), Strasburgo, 28 gennaio 1981.

[14] Carta dei diritti fondamentali dell'Unione Europea, proclamata a Nizza il 7 dicembre 2000, art. 8 – "Protezione dei dati di carattere personale": Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

[15] Patto internazionale relativo ai diritti civili e politici, adottato dall'Assemblea Generale delle Nazioni Unite con risoluzione 2200 A (XXI), 16 dicembre 1966.

[16] Si v. S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, XI; F. Fabris, *Il diritto alla privacy tra passato, presente e futuro*, in *Tigor: rivista di scienze della comunicazione* – A.I (2009) n.2 (luglio-dicembre), 95; P. Rescigno, *Diritti della persona-*

con l'adozione della Direttiva 95/46/CE [17], che per lungo tempo ha rappresentato il quadro normativo di riferimento per gli Stati membri dell'Unione europea in materia di protezione dei dati. Anche in questo testo normativo, il principio di minimizzazione, che è chiaramente espresso all'articolo 6, impone agli Stati membri di garantire che i dati personali siano «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità» e che siano «adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti».

Con l'entrata in vigore del RGPD [18], il principio di minimizzazione riceve una sistematizzazione ancora più chiara e vincolante, elevandosi a criterio fondamentale della liceità del trattamento dei dati, la cui violazione può determinare conseguenze significative in termini di responsabilità giuridica per il titolare del trattamento. Il Regolamento infatti non si limita a riaffermare la centralità del principio, ma lo integra all'interno dell'architettura generale della "responsabilizzazione" (*accountability*, art. 5, par. 2) e della "protezione dei dati fin dalla progettazione" (*privacy by design*, art. 25), imponendo un'analisi preventiva e continua circa la necessità e proporzionalità dei dati trattati rispetto alle finalità dichiarate.

3. – A livello europeo il fondamento normativo del principio di minimizzazione dei dati viene rinvenuto nell'articolo 5, paragrafo 1, lettera c) del RGPD, secondo il quale i dati personali devono essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati» [19].

lità, Enc. Giur. Treccani, Roma, 1994; M. Timiani, *Un contributo allo studio sul diritto alla riservatezza*, in *Rivista di studi parlamentari e di politica costituzionale*, n.176, 2012; V. Cuffaro, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e impresa* n.3/2018, 1101; A. R. Popoli, *Social Network e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, in *Diritto dell'Informazione e dell'Informatica* (III), fasc.6, 2014, 981. G. M. Riccio, *Social networks e responsabilità civile*, in *Il Diritto dell'informazione e dell'informatica*, Milano, 2010, 850. Sul punto, cfr. anche C. Perlingieri, *Profili civilistici dei social networks*, Napoli, 2014. L. Picotti, *I diritti fondamentali nell'uso e abuso dei social network: aspetti penali*, in *Giurisprudenza di Merito*, 2012, 2523.

[17] Dir. 95/46/CE, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali.

[18] Cfr. articoli 5 e 25 GDPR.

[19] Sul GDPR si veda tra i tanti E. Belisario, G.M. Riccio, G. Scorza, *GDPR e normativa privacy. Commentario*, Milano, 2020; F. Pizzetti (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, 2019.

In stretta connessione con la regola di minimizzazione, il RGPD individua anche le basi giuridiche che legittimano il trattamento dei dati personali (art. 6). Particolare rilievo, nella prospettiva qui considerata, assume l'art. 6, par. 1, lett. f), che consente il trattamento qualora «sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi», a condizione che non prevalgano «gli interessi o i diritti e le libertà fondamentali dell'interessato». Il trattamento dei dati personali dunque può essere effettuato solo se il "legittimo interesse" del titolare (cioè di chi raccoglie o usa i dati) è più forte o comunque non in contrasto con i diritti della persona cui i dati appartengono. Tale clausola aperta ha suscitato sin dall'origine ampi dibattiti dottrinali e giurisprudenziali [20], proprio perché rischia di fungere da "valvola di sfogo" attraverso cui giustificare prassi di trattamento non pienamente coerenti con i principi di necessità e proporzionalità.

Un ulteriore punto di riferimento normativo è l'art. 21 RGPD, che riconosce all'interessato il diritto di opposizione al trattamento basato sul legittimo interesse del titolare. La sua portata, tuttavia, è stata oggetto di controversie interpretative: può il diritto di opposizione fungere da meccanismo correttivo *ex post* rispetto a un trattamento che non soddisfa in origine i requisiti di necessità? La dottrina maggioritaria e la giurisprudenza più recente tendono a escludere tale possibilità, riaffermando che la valutazione della necessità deve essere preventiva e non delegata alla capacità di reazione dell'interessato [21].

Tuttavia vediamo come questo quadro normativo riveli in realtà una tensione strutturale: da un lato, infatti il RGPD enuncia una serie di principi stringenti e garantisti, destinati a rafforzare la tutela del diritto fondamentale alla protezione dei dati personali (art. 8 della Carta dei diritti fondamentali dell'U.E.); dall'altro, invece introduce margini di discrezionalità, soprattutto attraverso il ricorso al "legittimo interesse", che rischiano di indebolire l'effettività delle garanzie.

[20] Cfr. R. Polčák, *Legitimate Interests as a Legal Basis for Data Processing: Between Flexibility and Uncertainty*, in *Computer Law & Security Review*, vol. 38, 2020, 105–118; G. Butti, M.R. Perugini, *GDPR: la privacy nella pratica quotidiana. Tutte le domande a cui un DPO deve sapere rispondere*, Milano, 2021; R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della privacy e data protection*, Milano, 2019; A. Alongi, F. Pompei, *Diritto della privacy e protezione dei dati personali: il GDPR alla prova della data driven economy*, Roma, 2021; Commentario al codice della privacy, Pisa, 2020; G. Martorana (a cura di), *La privacy al passo con il Regolamento UE 2016/679. Esperienze applicative dei principi del GDPR nella governance aziendale*, Santarcangelo di Romagna, 2021.

[21] Cfr. G. Buttarelli, *Il diritto di opposizione nel sistema del RGPD: profili di effettività*, in *Rivista italiana di informatica e diritto*, n. 2, 2019, 45–67.

Tale ambivalenza ha reso necessario un costante intervento interpretativo della Corte di giustizia europea[22], la quale, con un approccio progressivamente più rigoroso, ha chiarito che la minimizzazione non costituisce un mero criterio formale, bensì un parametro sostanziale idoneo a limitare l'estensione delle basi giuridiche invocate dai titolari.

In questo contesto, la sentenza *Mousse* assume rilievo sistemico: essa infatti interviene proprio nel punto di frizione tra la discrezionalità operativa degli operatori economici e la natura vincolante dei principi generali del trattamento, riaffermando la centralità della minimizzazione come strumento di garanzia effettiva dei diritti fondamentali.

4. – In Italia, tale principio ha conosciuto una prima formalizzazione con il D.Lgs. 196/2003 (Codice Privacy) [23], dove veniva delineata la necessità del trattamento e il rispetto della pertinenza e non eccessività dei dati.

La sua formulazione normativa più recente e stringente è stata tuttavia recepita con il D.Lgs 101/2018, che ha adeguato il Codice Privacy al RGPD, sancendo in modo più esplicito e rigoroso il principio di minimizzazione [24].

Con questo intervento legislativo, il principio di minimizzazione ha assunto un rilievo ancora più marcato, passando da criterio implicito di correttezza e proporzionalità a parametro espressamente sancito tra i principi generali del trattamento.

Il recepimento italiano, attraverso il D.Lgs. 101/2018, ha quindi rafforzato il quadro normativo, imponendo a pubbliche amministrazioni, imprese e professionisti di adottare un approccio maggiormente consapevole e seletti-

[22] Cfr. Ceg., 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland*; 21 dicembre 2016, C-203/15 e C-698/15, *Tele2 Sverige*; 16 luglio 2020, C-311/18, *Schrems II*.

[23] Il d.lgs. 196/2003, noto come "Codice in materia di protezione dei dati personali" o più brevemente "Codice Privacy", è la principale normativa italiana che disciplina il trattamento dei dati personali. Esso è stato emanato per disciplinare in modo organico e coordinare la protezione dei dati personali nel rispetto dei diritti e delle libertà fondamentali degli individui, con particolare attenzione alla riservatezza e dignità dell'interessato.

[24] Il d.lgs. 101/2018 rappresenta l'atto normativo con cui l'Italia ha adeguato il proprio quadro legislativo nazionale, in particolare il Codice Privacy (d.lgs. 196/2003), alle disposizioni del Reg. 2016/679 noto come GDPR. Pubblicato in .u.u.e. il 4 settembre 2018 ed entrato in vigore il 19 settembre 2018, questo decreto ha modificato e integrato il Codice Privacy per armonizzarlo con i nuovi standard europei in materia di protezione dei dati personali.

vo nella gestione delle informazioni personali.

La giurisprudenza più significativa in materia si è espressa con la Corte di Cassazione, che ha ribadito tale principio in diverse occasioni, definendolo inderogabile e collegandolo strettamente al concetto di liceità e pertinenza del trattamento [25].

Un caso emblematico è stato l'ordinanza n. 34113 del 19 dicembre 2019 della Corte di Cassazione (Sez. I Civile) [26], la quale ha stabilito che il trattamento dei dati personali deve essere limitato ai dati indispensabili e pertinenti per il perseguimento delle finalità per cui sono raccolti, come illustrato nel contesto della cessione di crediti da parte di una banca a privati [27]. La Corte ha confermato che non costituisce violazione la comunicazione di dati strettamente funzionali alla finalità (ad esempio situazione debitoria, ubica-

[25] Si v. a tal proposito F. Sarzana, *Corte di Cassazione e privacy: il principio di minimizzazione dei dati del GDPR*, in *Il Sole24Ore*, dicembre 2019; *La Cassazione pronuncia in tema di privacy e trattamento dei dati personali ponendo in evidenza il principio di necessità e minimizzazione dei dati ex art. 5 GDPR*, su *Diritti Fondamentali*, gennaio 2020; S. Aterno, *Il principio di minimizzazione nell'uso di dati personali in Cassazione*, in *Diritto di Internet*, 22 gennaio 2020 (Nota alla Cass., ord. 21-10-2019, n. 26778); N. Pisanu, *Recupero crediti, rispettare il principio della minimizzazione dei dati: ecco la sentenza della Cassazione*, in *Cybersecurity360* (sezione *Norme e adeguamenti*), 24 dicembre 2019; V. Colarocco, *La Corte di Cassazione interviene sulla data minimization*, Previti, novembre 2019; *Corte di Cassazione e Privacy: il principio di minimizzazione dei dati alla luce del GDPR*, Legal-Team, gennaio 2020; G. D'Ascola, A. Manna, *Sanzioni privacy e poteri del giudice: i principi affermati dalla Corte di cassazione*, in *Giustizia Insieme*, 7 novembre 2023.

[26] Cass. 19-12-2019, ord. n. 34113.

[27] Questa ordinanza affronta il tema della cessione di crediti bancari e, nello specifico, delle conseguenze che tale operazione comporta in relazione al trattamento dei dati personali del debitore ceduto. Il caso nasce dalla contestazione di un debitore che si era opposto alla diffusione dei propri dati personali a soggetti privati (cessionari), sostenendo che la banca cedente avesse trasferito informazioni non strettamente necessarie al perseguimento delle finalità della cessione. La Corte di Cassazione ha colto l'occasione per ribadire un principio fondamentale della disciplina sulla privacy: i dati personali possono essere comunicati e trattati solo nella misura in cui siano indispensabili, pertinenti e non eccedenti rispetto allo scopo legittimo per cui vengono raccolti. Applicando tale regola al caso concreto, la Corte ha precisato che, nel contesto della cessione di crediti, la banca è certamente autorizzata a trasferire al cessionario le informazioni necessarie per l'identificazione del debitore e per l'esercizio dei diritti derivanti dal credito stesso. Tuttavia, non è lecito includere nel pacchetto informativo dati ulteriori o irrilevanti, che non siano indispensabili alla gestione del credito ceduto. In questo modo la Cassazione ha confermato che il principio di minimizzazione dei dati opera come limite sostanziale alle pratiche bancarie, bilanciando la legittima circolazione dei crediti con la tutela della riservatezza del debitore.

zione immobile di garanzia), ma ha ribadito che qualsiasi dato in eccesso o non necessario configuri una violazione del principio di minimizzazione.

In un altro orientamento, sempre la giurisprudenza italiana ha sancito che l'istituto bancario non può subordinare l'operatività di un conto corrente al consenso per trattare dati personali non strettamente necessari, in particolare dati sensibili, in ragione dell'inderogabilità del principio di minimizzazione (Cass. Sez. I, 21-10-2019, n. 26778) [28]. Ciò evidenzia come il principio assuma anche valenza di strumento di tutela dei diritti fondamentali degli interessati, limitando il potere contrattuale delle parti in materia di privacy.

Operando un confronto con altri ordinamenti europei, come quello francese, si trovano analogie non solo nel ricevimento ma anche nell'applicazione rigorosa del principio di minimizzazione. L'ultima sentenza della Corte di Cassazione civile francese in materia (novembre 2024) [29], infatti, impone restrizioni stringenti sull'uso dei dati personali nei procedimenti giudiziari, obbligando a limitare la richiesta di documenti solo a ciò che è strettamente necessario e proteggendo i dati di terzi non coinvolti. Questo approccio è utile per evitare un uso eccessivo dei dati che rischia di compromettere la privacy e la responsabilità nella gestione delle informazioni.

In una prospettiva comparata, notiamo come invece taluni ordinamenti extraeuropei – si pensi agli Stati Uniti – non attribuiscano analoga centralità al principio di minimizzazione, preferendo un approccio di tipo settoriale e meno vincolante [30]. Ciò si traduce spesso in una più ampia libertà nella raccolta dei dati personali e in una ridotta delimitazione dei trattamenti, con conseguenze significative sul piano della protezione della sfera privata [31].

Sul piano critico dunque, pur riconoscendo che il RGPD e la legislazione

[28] Cass. 21-10-2019, ord. n. 26778, sul divieto di condizionare condizioni contrattuali al consenso per dati non necessari. In merito si v. il commento di S. Aterno, *Il principio di minimizzazione nell'uso di dati personali in Cassazione*, su *Diritto di Internet*.

[29] Sentenza Corte di Cassazione civile francese, 4 novembre 2024, applicazione rigorosa del principio di minimizzazione nei procedimenti giudiziari.

[30] In merito al principio di minimizzazione nell'ordinamento statunitense si v. G. Sacerdoti Mariani, A. Reposo e M. Patrono, *Guida alla Costituzione degli Stati Uniti d'America*, Milano, 1999, 8-9; N. Lugaresi, *Internet, Privacy e Pubblici Poteri negli Stati Uniti*, Milano, 2000, 47; F.D. Shoeman, *Privacy and Social Freedom*, New York, 1992, 11 e ss; J.J. Patrick, *The Young Oxford Companion to the Supreme Court of the United States*, New York, 1994, 194-195; T.K. Clancy, *What does the Fourth Amendament Protect? Property, Privacy, or Security?*, in *Wake Forest Law Review*, vol. 33, 1998, 344 e ss.

[31] D.J. Solove, W. Hartzog, *The FTC and the New Common Law of Privacy*, in *Columbia Law Re-*

italiana forniscono un solido quadro normativo di tutela attraverso l'affermazione del principio di minimizzazione dei dati, le maggiori difficoltà si manifestano nella fase della sua concreta attuazione. In particolare, l'applicazione pratica del principio richiede un delicato bilanciamento con altre esigenze di pari rilievo, quali la sicurezza nazionale, la prevenzione e la repressione della criminalità, nonché l'adempimento di obblighi di *compliance* aziendale.

Ulteriori criticità inoltre si riscontrano con riferimento ai settori maggiormente esposti ai processi di digitalizzazione e all'uso dell'intelligenza artificiale, nei quali la logica dei *big data* presuppone l'accumulo di ingenti quantità di informazioni. Tale paradigma può entrare in evidente tensione con l'obbligo di limitare i dati trattati a quanto strettamente necessario, sollevando questioni interpretative di non poco rilievo. In particolare, la definizione di ciò che debba intendersi per dato "necessario" o "pertinente" resta spesso vaga e suscettibile di differenti letture, esponendo così operatori e giudici al rischio di incertezze applicative e di contenziosi.

Non meno rilevante, nell'analisi del principio di minimizzazione e più in generale della disciplina europea in materia di protezione dei dati personali, è la constatazione che, nonostante il carattere direttamente applicabile del RGPD, permangano divergenze interpretative e applicative tra gli Stati membri. La funzione armonizzatrice del Regolamento incontra infatti dei limiti nella prassi: le autorità nazionali di controllo e gli organi giurisdizionali non sempre forniscono letture convergenti, generando un quadro che si traduce in incertezza giuridica e difficoltà operative per i titolari del trattamento che agiscono in più giurisdizioni.

Gli esempi sono numerosi. In Italia, il Garante per la protezione dei dati personali ha assunto spesso un approccio particolarmente attento al principio di minimizzazione, imponendo limiti stringenti alla conservazione dei dati nei rapporti di lavoro e nella videosorveglianza, ribadendo la necessità

view, 114 (2014), 583-676; O. Tene, J. Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, in *Northwestern Journal of Technology & Intellectual Property*, 11 (2013), 239-273; J. Polonetsky, O. Tene, *Privacy and Big Data: Making Ends Meet*, in *Stanford Law Review Online*, 66 (2013), 25-33; I.S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, in *International Data Privacy Law*, 3(2) (2013), 74-87; I.S. Rubinstein, W. Hartzog, *Anonymization and Risk*, in *Washington Law Review*, 91(2) (2016), 703-760; W. Hartzog, *Privacy's Constitutional Moment and the Limits of Data Protection*, saggio/working paper, 2020; A.E. Waldman, *The New Privacy Law*, in *UC Davis Law Review Online*, 57 (2024), 1-22; N. M. Richards, W. Hartzog, J. Francis, *A Concrete Proposal for Data Loyalty*, in *Harvard Journal of Law & Technology* (Symposium), 2023.

che i dati raccolti siano sempre strettamente funzionali alle finalità dichiarate [32]. Diversa è stata, in alcune circostanze, la posizione della CNIL francese, che si è mostrata più rigorosa nel richiedere ai titolari del trattamento di predisporre misure tecniche concrete – quali pseudonimizzazione o anonimizzazione – per garantire il rispetto del principio [33]. Ancora più marcato è l'orientamento di alcune autorità tedesche, le quali, in virtù della tradizione federale, hanno adottato prassi tra loro non sempre uniformi: in alcuni Länder si è privilegiato un controllo sostanziale sul rischio effettivo di eccedenza dei dati, in altri si è dato maggiore rilievo all'adozione preventiva di strumenti organizzativi di *accountability* [34].

Queste differenze dimostrano come un principio cardine, pur chiaramente formulato all'art. 5, par. 1, lett. c) del GDPR, possa assumere connotati diversi nella sua attuazione pratica. La conseguenza è duplice: da un lato, si indebolisce la certezza del diritto, poiché le imprese e le pubbliche amministrazioni non hanno sempre la garanzia che un determinato comportamento sia considerato lecito allo stesso modo in tutta l'Unione; dall'altro, si accrescono i costi di *compliance* per i titolari del trattamento che operano in più Paesi, i quali devono conformarsi a standard non pienamente allineati.

Ne risulta evidente l'importanza del ruolo del Comitato europeo per la protezione dei dati (EDPB) [35], chiamato a garantire coerenza attraverso linee guida e pareri, e un dialogo costante tra le autorità nazionali. Solo attraverso un rafforzamento di questi strumenti di coordinamento si potrà giungere a un'applicazione realmente uniforme del principio di minimizzazione e, più in generale, di tutto il quadro normativo europeo in materia di protezione

[32] Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati*, 2007; nonché provvedimento in materia di videosorveglianza dell' 8 aprile 2010.

[33] CNIL, *Recommandation relative aux mots de passe*, 2017; v. anche *Rapport d'activité 2021*, 52 ss., dove si insiste sulla necessità di tecniche di minimizzazione come l'anonimizzazione.

[34] Si v. ad es. Autorità garante per la protezione dei dati del Land Baviera, *Annual Report 2019*, 34 ss.; e Autorità del Land Baden-Württemberg, *Tätigkeitsbericht 2020*, 41, con differenze negli standard applicativi del principio di minimizzazione.

[35] Il Comitato europeo per la protezione dei dati (*European Data Protection Board – EDPB*) è un organismo indipendente dell'Unione europea, con il compito di garantire l'applicazione uniforme della normativa in materia di protezione dei dati personali, in particolare del Regolamento generale sulla protezione dei dati (RGPD). La sua istituzione, la composizione, i compiti, i poteri e le regole di funzionamento sono disciplinati dagli articoli 68-76 del RGPD.

dei dati personali.

5. – La vicenda che ha dato origine al procedimento oggetto del presente lavoro prende le mosse da una controversia sorta in Germania tra un consumatore e un'impresa commerciale operante nel settore dell'*e-commerce*.

In occasione della registrazione necessaria per l'acquisto di prodotti e servizi online, all'utente veniva richiesto in via obbligatoria di selezionare un titolo di cortesia ("Signore"/"Signora"). Tale requisito, apparentemente marginale e legato a consuetudini commerciali diffuse, è stato oggetto di contestazione da parte del consumatore, il quale sosteneva che esso costituisse un trattamento di dati personali sproporzionato e non necessario rispetto alle finalità del contratto, in violazione del principio di minimizzazione di cui all'art. 5, par. 1, lett. c) del RGPD.

L'interessato ha altresì sottolineato come tale prassi non fosse neutrale sotto il profilo dei diritti fondamentali, in quanto idonea a determinare un rischio di discriminazione nei confronti delle persone la cui identità di genere non si riconduce a categorie binarie. In questo senso, il dato richiesto, pur qualificabile come "formale" o "di cortesia", si rivelava potenzialmente lesivo non soltanto della protezione dei dati personali, ma anche del principio di parità di trattamento sancito dagli artt. 20 e 21 della Carta dei diritti fondamentali dell'UE e dalla Direttiva 2004/113/CE.

Il giudice nazionale, investito della controversia, ha pertanto sospeso il procedimento e adito la Corte di giustizia ai sensi dell'art. 267 TFUE, sottoponendo una questione pregiudiziale di particolare rilievo sistemico. In particolare, è stato chiesto se il principio di minimizzazione dei dati, unitamente all'art. 6, par. 1, lett. b) e f) del RGPD, consenta a un'impresa di raccogliere e trattare in via obbligatoria il titolo di cortesia di un cliente nell'ambito di una prestazione contrattuale.

La questione, così formulata, ha sollevato due interrogativi centrali: da un lato, se il conferimento di tali dati possa rientrare nella nozione di necessità contrattuale ai sensi dell'art. 6, par. 1, lett. b); dall'altro, se l'eventuale ricorso alla base del legittimo interesse (art. 6, par. 1, lett. f)) sia compatibile con il principio di proporzionalità, tenuto conto del rischio discriminatorio insito nella raccolta obbligatoria di dati legati all'identità di genere.

5.1. – Con la sentenza *Mousse*, la Corte non si è limitata a confermare gli orientamenti già affermati in precedenza, ma ha scelto di accentuarli in senso più restrittivo.

L'oggetto del giudizio – la raccolta obbligatoria di un titolo di cortesia – costituisce infatti un terreno solo in apparenza marginale, poiché è stato assunto come occasione per rafforzare la centralità del principio di minimizzazione e per integrare, nel test di liceità del trattamento, anche la valutazione del rischio di discriminazione. In questo modo, una prassi commerciale di routine è stata trasformata in un vero e proprio banco di prova per estendere l'applicazione del principio di proporzionalità e di necessità anche ai dettagli più minuti delle relazioni tra imprese e consumatori.

In primo luogo, la Corte ha escluso che tale trattamento possa essere giustificato sulla base della necessità contrattuale (art. 6, par. 1, lett. b)). Secondo i giudici di Lussemburgo infatti, il dato richiesto non risulta in alcun modo indispensabile all'esecuzione del contratto di vendita o di prestazione di servizi, potendo quest'ultimo essere concluso senza alcuna indicazione di genere [36]. Tale impostazione si inserisce nel solco di una giurisprudenza ormai consolidata, che interpreta in maniera restrittiva il concetto di "necessità contrattuale" per evitare che esso diventi un espediente per eludere il consenso dell'interessato [37].

In secondo luogo, la Corte ha escluso la possibilità di fondare la liceità del trattamento sul legittimo interesse del titolare (art. 6, par. 1, lett. f) [38], in assenza di una dimostrazione rigorosa della proporzionalità e della non invasività del trattamento. I giudici infatti hanno osservato che l'obiettivo della personalizzazione mediante titoli di cortesia non soddisfa il requisito della necessità oggettiva, potendo essere agevolmente sostituito da formule neutre [39].

Questo orientamento era stato già espresso dalla Corte nelle sentenze *Meta Platforms* e *Koninklijke Nederlandse Lawn Tennisbond*, anche se in quest'ultima è stato accentuato il carattere eccezionale e restrittivo delle basi

[36] Ceg. *Mousse,* cit. punti 36-40.

[37] Cfr. O. Pollicino, *La Corte di giustizia e i limiti della necessità contrattuale nel trattamento dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 2022, 521 ss.

[38] Ceg. *Mousse*, cit. punti 36-40.

[39] Ceg. *Mousse*, cit. punti 41-44.

alternative al consenso [40]. La Corte ha infatti richiamato il criterio delle alternative meno intrusive, osservando che l'utilizzo di formule di cortesia neutrali o del solo nome dell'utente rappresenta una soluzione equivalente e meno invasiva [41]. Tale affermazione rafforza l'idea che la nozione di "necessità" vada intesa in senso stretto e che la presenza di strumenti meno pregiudizievoli comporti automaticamente l'illegittimità del trattamento.

Il passaggio più innovativo risiede però nell'aver riconosciuto espressamente il rischio discriminatorio derivante dalla raccolta di dati relativi al genere [42]. La Corte ha sottolineato che l'obbligo di indicare un titolo binario può determinare discriminazioni dirette e indirette, in violazione degli artt. 20 e 21 della Carta dei diritti fondamentali e della Direttiva 2004/113/CE [43]. In tal modo, il giudice di Lussemburgo ha integrato la logica antidiscriminatoria all'interno del test di liceità del trattamento, ampliando la portata del principio di minimizzazione.

In questo senso vediamo come la pronuncia compie un passo ulteriore rispetto alla giurisprudenza precedente, trasformando di fatto la dimensione antidiscriminatoria da parametro autonomo del diritto dell'Unione a criterio integrato nella logica del RGPD [44].

La Corte di giustizia, con questa sentenza ha operato in sostanza una significativa restrizione nell'interpretazione delle basi di liceità del trattamento, trasformando una prassi commerciale apparentemente innocua – la richiesta obbligatoria del titolo di cortesia – in un banco di prova per consolidare e al tempo stesso innovare la propria giurisprudenza.

Anzitutto, essa ha dichiarato illegittima l'obbligatorietà di tale raccolta, rilevando che il dato relativo al genere non è strettamente necessario all'ese-

[40] V. Ceg. 4 luglio 2023, C-252/21, *Meta Platforms Inc. v Bundeskartellamt*, ECLI:EU:C:2023:537; 4 ottobre 2024, C-621/22, *Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens*, ECLI:EU:C:2024:857. Sul punto, v. anche G. Malgieri, *The Concept of Legitimate Interest in GDPR: From Flexibility to Restriction?*, in *Computer Law e Security Review*, 2021, 1054.

[41] Ivi, punti 41-44. Cfr. anche Ceg. 22 giugno 2021, C-439/19, *Latvijas Republikas Saeima*, ECLI:EU:C:2021:504, sul rilievo delle misure alternative meno invasive.

[42] Sul collegamento tra protezione dati e non discriminazione v. L. Daniele, *Il principio di non discriminazione nell'ordinamento dell'Unione europea*, Torino, 2019, 233 ss.

[43] Ceg. *Mousse,* cit., punti 60-63. Dir. 2004/113/CE, del 13 dicembre 2004 in g.u.u.e., L 373 del 21.12.2004, 37-43.

[44] Ceg. *Mousse,* cit., punti 60-63. In dottrina, cfr. G. Sartor, *The Right to Data Protection: Logic, Evolution and Interpretation*, in *European Data Protection Law Review*, 2020, 289 ss.

cuzione del contratto ai sensi dell'art. 6, par. 1, lett. b) RGPD, né può essere giustificato come proporzionato rispetto a un legittimo interesse del titolare ex art. 6, par. 1, lett. f)[45]. Il fatto che il contratto possa essere agevolmente concluso senza tale informazione evidenzia l'assenza di un nesso di necessità oggettiva.

Infine, la Corte ha riaffermato la centralità della trasparenza: l'impresa, per legittimare il trattamento, non solo deve informare in modo chiaro sulle finalità perseguite, ma deve anche dimostrare che il proprio interesse legittimo prevale sugli interessi e sui diritti degli interessati. Nel caso di specie, tale condizione non risultava soddisfatta [46].

Da queste premesse la sentenza ricava tre principi di rilievo sistemico: (i) il principio di minimizzazione non tollera eccezioni neppure per dati apparentemente "innocui", qualora non siano strettamente indispensabili all'esecuzione del contratto; (ii) l'art. 6, par. 1, lett. b) e f) RGPD deve essere interpretato in senso restrittivo, imponendo una dimostrazione rigorosa della necessità, non riducibile a convenzioni sociali o preferenze commerciali; (iii) la valutazione di liceità del trattamento deve integrare anche la dimensione antidiscriminatoria, trasformando la protezione dei dati in uno strumento di tutela trasversale dei diritti fondamentali.

Da un punto di vista critico, la decisione dunque segna un passo ulteriore rispetto alle pronunce precedenti: la Corte non si limita più a delimitare lo spazio applicativo delle basi giuridiche, ma introduce un vero e proprio paradigma integrato, nel quale la logica della minimizzazione si coniuga con quella della parità di trattamento. In tal senso, la *Mousse* può essere letta come la tappa più recente di un percorso che conduce verso un ordine pubblico europeo dei dati personali, nel quale anche i dettagli più minuti delle pratiche commerciali vengono sottoposti al vaglio dei principi fondamentali [47].

In sostanza da un punto di vista critico, la sentenza mostra la volontà della Corte di espandere la portata del principio di minimizzazione ben oltre la

[45] Ceg. *Mousse,* cit., punti 36-40.

[46] Ceg. 4 luglio 2023, C-252/21, *Meta Platforms Inc. v Bundeskartellamt*, ECLI:EU:C:2023:537, sulla trasparenza come condizione imprescindibile per l'invocazione del legittimo interesse.

[47] In dottrina, cfr. G. Sartor, *The Right to Data Protection: Logic, Evolution and Interpretation*, in *European Data Protection Law Review*, 2020, 289 ss.; E. Spiller, *La sentenza Tele2 Sverige: verso una Digital Rule of Law europea?*, in *IANUS*, 2017, 279 ss., sul progressivo consolidarsi di un ordine pubblico europeo dei diritti nella società digitale.

mera quantità di dati raccolti: ciò che conta non è soltanto ridurre il dato al minimo necessario, ma anche evitare che la sua raccolta, per quanto formalmente marginale, generi conseguenze pregiudizievoli per la dignità e l'eguaglianza della persona. In tal senso, la *Mousse* segna una svolta paradigmatica, avvicinando la disciplina della protezione dei dati a quella della non discriminazione e rafforzando l'idea di un ordine pubblico europeo dei diritti fondamentali che permea anche le pratiche commerciali quotidiane.

5.2. – Per valutare appieno la portata innovativa della sentenza del 2025, è necessario inquadrarla nell'evoluzione giurisprudenziale della Corte di giustizia dell'Unione europea. Solo attraverso tale prospettiva è infatti possibile cogliere la continuità e le rotture che essa introduce rispetto al percorso già tracciato a livello europeo.

La Corte, in particolare, ha progressivamente trasformato il diritto alla protezione dei dati personali da principio generale e astratto a parametro sostanziale di legittimità degli atti normativi e amministrativi, riconoscendogli un ruolo sempre più centrale nell'architettura dei diritti fondamentali dell'Unione. Questa progressiva valorizzazione non è tuttavia priva di criticità: il passaggio da diritto meramente dichiarativo a criterio vincolante per le legislazioni nazionali ha posto questioni di ordine esegetico e attuativo, alimentando, talora, divergenze tra gli ordinamenti degli Stati membri.

La sentenza del 2025, pur consolidando la centralità del dato personale, rappresenta non solo un punto di approdo, ma anche un'occasione per rileggere criticamente i limiti e le ambiguità accumulate lungo il percorso giurisprudenziale, mettendo in luce le sfide ancora aperte nella concreta armonizzazione tra tutela dei diritti e flessibilità normativa.

Prima della sentenza *Mousse* del 2025, la Corte aveva già tracciato un percorso rigoroso, sviluppando una giurisprudenza che metteva al centro i principi di necessità, proporzionalità e minimizzazione. Tuttavia, fino ad allora, l'attenzione della giurisprudenza si era concentrata prevalentemente su scenari di portata "macro" — quali la sorveglianza statale, i trasferimenti transfrontalieri di dati e l'impiego delle informazioni da parte di grandi piattaforme digitali — trascurando quasi sistematicamente le dinamiche "micro" che caratterizzano la vita quotidiana e le interazioni contrattuali tra imprese e consumatori. Questa focalizzazione privilegiata sugli ambiti di grande im-

patto ha finito per marginalizzare contesti altrettanto rilevanti sotto il profilo della tutela effettiva dei diritti, evidenziando una lacuna interpretativa nella costruzione di un paradigma giuridico realmente centrato sull'individuo.

La linea giurisprudenziale in materia di protezione dei dati personali è stata inaugurata con le note sentenze *Digital Rights Ireland* [48] e *Tele2 Sverige* [49], nelle quali il giudice di Lussemburgo ha dettato i primi limiti stringenti al ricorso a misure di sorveglianza e raccolta dei dati su larga scala, sancendo un principio di indisponibilità dei diritti fondamentali destinato in realtà a riecheggiare anche nelle successive decisioni.

In tali sentenze, la Corte ha dichiarato incompatibile con il diritto dell'Unione la conservazione generalizzata e indifferenziata dei dati relativi al traffico e alla localizzazione, ritenendola non conforme ai principi di proporzionalità e minimizzazione sanciti dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'UE.

Come osservato in dottrina, la giurisprudenza in questo caso non si è limitata a una valutazione di carattere tecnico, ma ha individuato nella indisponibilità dei diritti fondamentali un limite invalicabile all'azione normativa e amministrativa degli Stati membri, sottraendo tali diritti a logiche meramente utilitaristiche o securitarie [50].

[48] Ceg. 8 aprile 2014, Cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, et al.*; *Kärntner Landesregierung, et al.*, ECLI:EU:C:2014:238.

[49] Ceg. 21 dicembre 2016, Cause riunite C-203/15 e C-698/15, T*ele2 Sverige AB v Post-och telestyrelsen* e *Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis,* ECLI:EU:C:2016:970.

[50] Cfr. C. Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford, 2017, 145 ss. Le sentenze sono state ampiamente commentate in dottrina si vedano alcuni esempi in M. Pierre Granger & K. Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, in *European Law Review*, 2014, 835 ss.; O. Lynskey, *The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland*, in *Common Market Law Review*, 2014, vol. 51, 1789 –1811; M. M. F. Villarica, *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice, and Geoffrey Lewis (C.J.E.U.)*, in *International Legal Materials*, Vol. 57, Issue 1, 2018, 125 – 154; *The Political and Judicial Life of Metadata: Digital Rights Ireland and Trail Data Retention*, paper del CEPS (Centre for European Policy Studies), 2014; Riguardo alle fonti italiane invece si citano E. Spiller, *La sentenza Tele2 Sverige: verso una Digital Rule of Law europea?*, in *IANUS*, n. 15-16, giugno-dicembre 2017, 279 ss.: G. Caggiano, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di*

Il filo conduttore di queste pronunce in sostanza risiede nell'affermazione che le esigenze di sicurezza pubblica, pur costituendo un interesse primario, non possono giustificare misure che incidano in maniera sproporzionata sulla sfera privata degli individui, fino a comprometterne l'essenza [51]. Ne consegue che la Corte, lungi dal porsi come arbitro di un bilanciamento contingente, ha riaffermato la struttura assiologica dell'ordinamento europeo, nella quale i diritti fondamentali si configurano come parametri inderogabili di legittimità.

Tale orientamento è stato ulteriormente consolidato con la sentenza *Facebook Schrems* (C-311/18, 2020) [52], che ha invalidato il regime del *Privacy Shield* disciplinante i trasferimenti di dati personali tra UE e Stati Uniti [53]. In questa occasione, la Corte ha esteso il proprio scrutinio oltre i confini interni

servizi di comunicazione, in *Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno* (atti del convegno, Messina, 26-27 maggio 2017), 64 ss.; O. Pollicino, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto Penale Contemporaneo*, 2017.

[51] V. anche L. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Dordrecht, Springer, 2014, 201 ss.

[52] Ceg. 16 luglio 2020, C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, ECLI:EU:C:2020:559.

[53] Il *Privacy Shield* era il quadro UE-USA (2016) che permetteva il trasferimento di dati personali verso aziende USA autocertificate al rispetto di 7 principi di tutela. I principi erano: *Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, Recourse/Enforcement/Liability*. Nel 2020 la Corte di giustizia (*Schrems II*, C-311/18) ha invalidato il *Privacy Shield* per insufficienza delle garanzie contro la sorveglianza USA e l'assenza di rimedi efficaci. Nel 2023 la Commissione europea ha adottato l'EU-U.S. *Data Privacy Framework* (DPF), che ricalca quei principi con nuove salvaguardie; è il meccanismo oggi in vigore per i trasferimenti verso le imprese partecipanti. v. https://ec.europa.eu/commission/presscorner/api/files/attachment/ 875613/EU.

A inizio settembre 2025 il Tribunale UE ha confermato la validità del DPF nel caso T-553/23 (*Latombe v. Commissione*). Il Tribunale dell'Unione europea in questo caso ha respinto il ricorso di annullamento proposto contro la decisione di adeguatezza sul *Data Privacy Framework* UE-USA, schierandosi con la Commissione. Secondo i giudici, alla data della sua adozione (10 luglio 2023) l'ordinamento statunitense garantiva un livello adeguato di protezione dei dati personali trasferiti dall'UE alle organizzazioni statunitensi aderenti. In particolare, le preoccupazioni relative alla sorveglianza sono state ritenute compensate dall'esistenza di un controllo giurisdizionale "ex post" affidato alla *Data Protection Review Court* (DPRC), considerato sufficiente a soddisfare le esigenze di tutela individuate dalla giurisprudenza *Schrems II*. Ne deriva che i trasferimenti verso i soggetti certificati nell'ambito del DPF restano coperti dall'adeguatezza. Resta comunque aperta la via dell'impugnazione dinanzi alla Corte di giustizia, limitatamente alle questioni di diritto. Sul piano del dibattito pubblico, Max Schrems ha espresso persistenti riserve, sostenendo che una verifica più ampia della legislazione statunitense avrebbe potuto condurre a un esito diverso. Cfr. M. Schrems, *Kämpf um deine Daten*, Wien, 2014.

del mercato digitale europeo, imponendo che anche i rapporti transatlantici rispettino il requisito di un livello di tutela "sostanzialmente equivalente" a quello garantito dal diritto dell'Unione. Come osservato dalla dottrina, questo passaggio esprime l'apertura dell'ordine pubblico europeo dei diritti fondamentali verso l'esterno, impedendo compromessi che si basino soltanto su interessi economici o geopolitici [54].

In tale prospettiva, la CGUE non appare dunque soltanto come custode della proporzionalità delle misure nazionali o sovranazionali, ma anche come garante di un "diritto fondamentale alla protezione dei dati" inteso quale nucleo identitario dell'ordinamento europeo [55]. La riaffermazione dell'indisponibilità dei diritti implica che essi non possano essere oggetto di contrattazione né all'interno dell'Unione, né nei rapporti esterni, ma debbano costituire il criterio ultimo di legittimità dell'azione normativa e amministrativa.

5.3. – Il percorso giurisprudenziale della Corte di giustizia in materia di protezione dei dati personali si è dunque progressivamente consolidato con un orientamento sempre più restrittivo nella lettura delle basi di liceità del trattamento.

Con la più recente sentenza *Schrems* (C-446/21, 2024) [56] infatti, la Corte ha ribadito che la tutela della privacy e dei dati personali deve essere garantita in tutte le fasi del trattamento, con particolare riguardo ai trasferimenti internazionali. L'accento è posto sul principio di equivalenza delle garanzie anche al di fuori dell'Unione, nella linea già tracciata da *Facebook Schrems* (C-311/18, 2020).

Su questa stessa traiettoria si colloca la sentenza *Mousse*, che sposta l'attenzione dalla dimensione esterna alla stretta interpretazione delle basi giuridiche interne, imponendo un'applicazione severa del principio di necessità anche a dati apparentemente marginali, come quelli relativi all'identità di genere. La differenza è evidente: *Schrems* tutela la circolazione sicura dei dati oltre confine, mentre *Mousse* rafforza la protezione *in loco*, nei rapporti quotidiani tra operatori economici e utenti.

[54] O. Lynskey, *The Schrems II judgment: EU fundamental rights and the territorial scope of EU law*, in *Common Market Law Review*, 58(6), 2021, 1765 ss.

[55] G. Sartor, *The Right to Data Protection: Logic, Evolution and Interpretation*, in *European Data Protection Law Review*, 6(3), 2020, 289 ss.

[56] Ceg. 4 ottobre 2024, C-446/21, *Schrems*, ECLI:EU:C:2024:834.

In continuità con questo orientamento, la sentenza *Koninklijke Nederlandse Lawn Tennisbond* (C-621/22, 2024) [57] ha introdotto un test rigoroso per valutare i trattamenti fondati su basi alternative al consenso, richiedendo una verifica puntuale della necessità oggettiva e dell'assenza di soluzioni meno intrusive. La pronuncia *Mousse* invece non solo conferma tale impostazione, ma la radicalizza, chiarendo in sostanza che la personalizzazione mediante titoli di cortesia non soddisfa il requisito della necessità e può perfino generare rischi discriminatori legati all'identità di genere.

Analogamente, con *Meta Platforms* (C-252/21, 2023) [58], la Corte ha ribadito che le basi alternative al consenso devono essere interpretate restrittivamente e che l'informazione trasparente agli interessati costituisce presupposto essenziale di liceità. La *Mousse* si colloca sulla stessa linea, sottolineando, a differenza della *Meta Platforms,* che l'invocazione del legittimo interesse non è ammissibile senza un'adeguata informativa e senza una reale dimostrazione di proporzionalità. L'innovazione principale risiede dunque nell'aver connesso tale analisi al rischio di discriminazione di genere, richiamando espressamente la Direttiva 2004/113/CE [59].

In realtà già in *Latvijas Republikas Saeima* (C-439/19, 2021) [60] la Corte aveva riaffermato che il principio di proporzionalità esige la ricerca di misure alternative meno invasive. Seguendo questa linea interpretativa, la *Mousse* ribadisce che solo l'uso di formule di cortesia neutre costituisce una soluzione equivalente, meno invasiva e quindi preferibile (punti 39-40).

Infine, un collegamento significativo si può tracciare con la più risalente *Richards* (C-423/04, 2006) [61], che, pur in un contesto anteriore al RGPD, aveva interpretato la Direttiva 2004/113/CE in senso ampio, includendo nella tutela le discriminazioni connesse al mutamento dell'identità di genere. La *Mousse* infatti riprende e aggiorna tale orientamento, traslandolo nel quadro del RGPD e chiarendo che il rischio di discriminazione deve entrare a

[57] Ceg. 4 ottobre 2024, C-621/22, *Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens*, ECLI:EU:C:2024:857.

[58] Ceg. 4 luglio 2023, C-252/21, *Meta Platforms Inc. v Bundeskartellamt*, ECLI:EU:C:2023:537.

[59] Dir. 2004/113/CE, del 13 dicembre 2004, che attua il principio della parità di trattamento tra uomini e donne per quanto riguarda l'accesso a beni e servizi e la loro fornitura, in g.u.u.e., L 373 del 21.12.2004, 37–43.

[60] Ceg. 6 ottobre 2021, C-439/19, *Latvijas Republikas Saeima*, ECLI:EU:C:2021:504.

[61] Ceg. 27 aprile 2006, C-423/04, *Richards,* ECLI:EU:C:2006:256.

pieno titolo nella valutazione di liceità anche dei trattamenti dei dati a fini commerciali (punti 60-63).

5.4. – Dall'analisi della traiettoria giurisprudenziale della Corte di giustizia emergono in sostanza tre profili di rilievo sistematico.

In primo luogo si registra, come abbiamo già anticipato, un consolidamento progressivo del rigore interpretativo: la Corte ha progressivamente inasprito il controllo sull'applicazione del principio di minimizzazione dei dati, spostando il proprio scrutinio dai grandi scenari di sorveglianza di massa e di trasferimenti internazionali (si pensi a *Digital Rights Ireland*, *Tele2 Sverige* e *Facebook Schrems*) verso le pratiche commerciali quotidiane. Tale evoluzione evidenzia un passaggio da una protezione "macro", volta a contenere le interferenze statali di ampia portata, a una protezione "micro", centrata sulle relazioni ordinarie tra imprese e utenti.

In secondo luogo, le pronunce del triennio 2021-2024 (*Latvijas Republikas Saeima*, *Meta Platforms*, *Koninklijke Nederlandse Lawn Tennisbond*) hanno chiarito i limiti del legittimo interesse quale base giuridica autonoma del trattamento ai sensi dell'art. 6, par. 1, lett. f) GDPR. L'orientamento della Corte infatti, si è mosso nella direzione di una progressiva riduzione dello spazio per un'interpretazione elastica di tale disposizione, esigendo una verifica stringente della necessità oggettiva e dell'assenza di soluzioni meno intrusive. Questa traiettoria ha preparato il terreno alla radicalizzazione operata dalla sentenza *Mousse*, che ha escluso la possibilità di fondare sul legittimo interesse trattamenti non strettamente necessari, come la personalizzazione di titoli di cortesia.

In terzo luogo, la novità di maggior rilievo risiede nell'inclusione della dimensione antidiscriminatoria nel cuore stesso del test di liceità dei trattamenti. La sentenza *Mousse* ha difatti integrato espressamente i principi di parità e non discriminazione (artt. 20 e 21 della Carta dei diritti fondamentali dell'UE; Direttiva 2004/113/CE) nella valutazione di liceità, affermando che anche il rischio di discriminazione deve essere considerato come criterio autonomo di legittimità accanto alla proporzionalità e alla minimizzazione. Si tratta di un ampliamento della logica tradizionale di minimizzazione: non solo quantità e necessità dei dati, ma anche qualità e impatto discriminatorio del trattamento.

Queste tre considerazioni ci mostrano come la *Mousse* in realtà non si limiti a recepire gli orientamenti precedenti, ma li sintetizza e li potenzia, raf-

forzando ulteriormente la centralità del principio di minimizzazione e contemporaneamente traslandolo nel terreno delle interazioni quotidiane tra cittadini e imprese.

6. – La sentenza in oggetto segna come abbiamo visto un passaggio decisivo nella giurisprudenza europea in materia di protezione dei dati personali. Per la prima volta, la Corte di giustizia ha spostato il baricentro del proprio scrutinio dai grandi flussi di dati – sorveglianza di massa, trasferimenti internazionali, attività delle piattaforme digitali – alle pratiche quotidiane delle imprese commerciali. In tal modo, il giudice di Lussemburgo ha affermato che anche le raccolte di dati apparentemente marginali devono superare un test stringente di necessità e proporzionalità, non potendo essere giustificate da mere convenzioni sociali o preferenze di marketing [62].

Tuttavia, non mancano criticità. Da un lato, la sentenza rischia di alimentare incertezza interpretativa circa la qualificazione dei dati come "strettamente necessari": nei settori in cui la personalizzazione costituisce componente essenziale della strategia commerciale, la linea di demarcazione tra dato superfluo e dato funzionale potrebbe risultare ambigua [63]. Dall'altro lato, la valorizzazione del rischio discriminatorio, sebbene coerente con l'evoluzione del diritto europeo, apre potenzialmente a conflitti con la libertà d'impresa garantita dall'art. 16 della Carta dei diritti fondamentali [64]. L'integrazione tra principi di protezione dei dati e principi antidiscriminatori, infatti, potrebbe comportare restrizioni ulteriori alla discrezionalità imprenditoriale, imponendo un ripensamento radicale delle pratiche di raccolta e gestione delle informazioni personali.

In definitiva, la *Mousse* non rappresenta solo un'evoluzione del diritto dei dati personali, ma una vera e propria svolta di sistema, in cui l'equilibrio tra mercato e diritti fondamentali viene ridefinito a favore di questi ultimi. La Corte delinea un nuovo paradigma: la personalizzazione, lungi dall'essere un

[62] Punti 36-44. Si v. M. P. Granger – K. Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland*, in *European Law Review*, 2014, 723 ss.; O. Pollicino, *La Corte di giustizia e i limiti della necessità contrattuale nel trattamento dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 2022, 521 ss.; G. Malgieri, *The Concept of Legitimate Interest in GDPR: From Flexibility to Restriction?*, in *Computer Law e Security Review*, 2021, 105452.

[63] O. Lynskey, *The Foundations of EU Data Protection Law*, Oxford, 2015, 141 ss.

[64] Sul rapporto tra libertà d'impresa e protezione dei dati, cfr. C. Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford, 2017, 201 ss.

automatismo, deve risultare facoltativa, proporzionata e trasparente; mai obbligatoria né invasiva [65].

La sentenza produce un impatto dirompente sul sistema della protezione dei dati, poiché consolida il principio di minimizzazione come criterio inderogabile per ogni trattamento, a prescindere dalla rilevanza economica o dalla natura "apparentemente innocua" dei dati raccolti. Se in passato l'attenzione della Corte si era concentrata solo sui trattamenti massivi, sulla sorveglianza e sui trasferimenti transfrontalieri, ora invece il controllo viene esteso anche alle pratiche ordinarie delle imprese, trasformando il RGPD in uno strumento di tutela capillare e non meramente reattivo [66].

L'innovazione più rilevante quindi consiste nell'integrazione tra protezione dei dati e diritto antidiscriminatorio: la Corte afferma infatti che la liceità del trattamento non può prescindere dalla valutazione dei rischi di discriminazione, anche indiretta, in applicazione degli artt. 20 e 21 della Carta e della Direttiva 2004/113/CE [67].

Si delinea così un modello multilivello di protezione, in cui la logica della minimizzazione viene arricchita da una prospettiva di eguaglianza sostanziale, con ricadute potenzialmente decisive anche per i settori emergenti dell'intelligenza artificiale, della profilazione e dell'uso degli algoritmi [68].

La pronuncia in sostanza contribuisce a ridefinire il rapporto tra mercato e diritti fondamentali: la personalizzazione, un tempo percepita come valore aggiunto imprescindibile per le strategie commerciali, è ora subordinata a un rigoroso test di necessità, ridimensionando il margine di autonomia delle imprese e rafforzando la prevalenza dei diritti fondamentali rispetto alla libertà d'impresa (art. 16 Carta) [69]. Ciò comporta conseguenze operative rilevanti: le imprese devono rivedere le procedure di raccolta dati, valutando la stretta indispensabilità delle informazioni richieste, predisponendo alternati-

[65] G. Sartor, *The Right to Data Protection: Logic, Evolution and Interpretation*, in *European Data Protection Law Review*, 2020, 289 ss.

[66] Punti 36-44; v. anche O. Lynskey, *The Foundations of EU Data Protection Law*, Oxford, 2015, 141 ss.

[67] Punti 60-63; L. Daniele, *Il principio di non discriminazione nell'ordinamento dell'Unione europea*, Torino, 2019, 233 ss.

[68] Cfr. G. Malgieri, *Bias and Discrimination in Algorithmic Decision-Making: A Challenge for Data Protection Law*, in *Computer Law e Security Review*, 2020, 1053.

[69] Sul rapporto tra libertà d'impresa e tutela dei dati v. C. Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford, 2017, 201 ss.

ve meno invasive e includendo il rischio discriminatorio nelle valutazioni di impatto (ex art. 35 RGPD), mentre le autorità di controllo sono chiamate a vigilare non solo sulla proporzionalità, ma anche sull'assenza di effetti discriminatori [70].

7. – L'itinerario giurisprudenziale tracciato dalla Corte di giustizia tra il 2014 e il 2025 mostra una progressiva radicalizzazione del controllo sulla liceità dei trattamenti di dati personali. Dalle prime decisioni in materia di sorveglianza di massa (*Digital Rights Ireland*, *Tele2 Sverige*), passando per il livello transfrontaliero dei trasferimenti internazionali (*Facebook Schrems*), fino alle pronunce più recenti sulle basi giuridiche interne (*Meta Platforms*, *Koninklijke Nederlandse Lawn Tennisbond*), la Corte ha sviluppato un paradigma restrittivo volto a garantire che i diritti sanciti dagli artt. 7, 8, 20 e 21 della Carta mantengano carattere di indisponibilità [71].

La sentenza *Mousse* rappresenta l'esito di questo percorso: essa trasla l'attenzione dai grandi scenari di sicurezza e trasferimento dati alle pratiche ordinarie delle imprese, affermando che anche la raccolta di dati apparentemente marginali debba superare un test rigoroso di necessità, proporzionalità e assenza di discriminazione [72]. In tal modo, la Corte non solo consolida il principio di minimizzazione, ma ne amplia la portata, connettendolo alla tutela contro le discriminazioni e delineando un modello integrato di protezione dei diritti.

Sul piano sistemico, ciò comporta almeno tre conseguenze. In primo luogo, un riequilibrio tra mercato e diritti fondamentali: la libertà d'impresa ex art. 16 Carta deve oggi confrontarsi con limiti più stringenti derivanti dalla centralità della dignità digitale [73]. In secondo luogo, un rafforzamento del ruolo delle autorità di controllo, chiamate non solo a valutare la proporzio-

[70] Si v. M.P. Granger – K. Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland*, in *European Law Review*, 2014, 723 ss.

[71] Si v. A. Mantelero, *AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment*, in *Computer Law & Security Review*, 2018, 754 ss.

[72] S. Wachter – B. Mittelstadt – L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, 76 ss.

[73] L. Floridi, *The Ethics of Information*, Oxford, 2013, spec. cap. 7; F. Celeste, *La protezione dei dati personali nell'era digitale: verso la dignità digitale*, Napoli, 2021, 45 ss.

nalità dei trattamenti, ma anche a vigilare sull'assenza di effetti discriminatori. In terzo luogo, un orizzonte evolutivo che proietta questo approccio verso i settori emergenti dell'intelligenza artificiale e della profilazione algoritmica, in cui i rischi di discriminazione sono particolarmente accentuati [74].

In prospettiva, si delinea un modello europeo di dignità digitale, nel quale la protezione dei dati personali non si esaurisce nella riservatezza ma diventa strumento di eguaglianza sostanziale e di legittimazione dell'innovazione tecnologica.

La sfida per la giurisprudenza e il legislatore sarà dunque armonizzare questo paradigma con gli obiettivi di competitività e sviluppo del mercato digitale, affinché la tutela dei diritti non rappresenti un ostacolo, bensì una condizione di fiducia e sostenibilità [75].

[74] P. Hacker, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination under EU Law*, in *Common Market Law Review*, 2021, 1147 ss.

[75] S. Rodotà, *Il diritto alla dignità digitale*, in *Politica del diritto*, 2017, p. 11 ss.; J. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford, 2019, 233 ss.

Abstract

La tutela dei dati personali rappresenta un tema centrale nell'ordinamento europeo, caratterizzato da un continuo confronto tra esigenze investigative e diritti fondamentali. Questo saggio analizza le principali pronunce giurisprudenziali in materia, mettendole a confronto critico con la sentenza C-394/23 del 2025 (*Mousse*), per tracciare l'evoluzione del quadro normativo e giurisprudenziale riguardante la protezione dei dati personali. L'indagine approfondisce le implicazioni di tale evoluzione sia in termini di salvaguardia della privacy sia nel bilanciamento con l'innovazione tecnologica, offrendo un contributo al dibattito accademico e giuridico sulle modalità di interpretazione e applicazione del Regolamento Generale sulla Protezione dei Dati (RGPR) nei contesti commerciali e tecnologici.

The protection of personal data is a central issue in the European legal system, characterised by a constant clash between investigative needs and fundamental rights. This essay analyses the main case law decisions on the matter, critically comparing them with the 2025 ruling C-394/23 (*Mousse*), to trace the evolution of the regulatory and case law framework regarding the protection of personal data. The study delves into the implications of this evolution both in terms of privacy protection and in balancing it with technological innovation, offering a contribution to the academic and legal debate on the interpretation and application of the General Data Protection Regulation (GDPR) in commercial and technological contexts.