Piattaforme e trattamento dei dati personali: l'approccio europeo

Aurora Saija

Piattaforme digitali e protezione dei dati personali: tra privacy, concorrenza e tutela dei consumatori.
Il contributo analizza il ruolo centrale dei dati personali nei modelli di business delle piattaforme digitali e le connesse criticità in materia di privacy, profilazione e decisioni automatizzate. Alla luce dell'interazione tra Regolamento (UE) 2016/679 (GDPR), Digital Services Act, Digital Markets Act e AI Act, il saggio esamina le sfide di regolazione ed enforcement e il ruolo del Garante per la protezione dei dati personali nel garantire un equilibrio tra innovazione, tutela dei diritti fondamentali e fiducia dei consumatori.

1. Piattaforme e trattamento dei dati personali: l'approccio europeo

Le piattaforme online sono ambienti in cui si instaurano relazioni personali e professionali, si realizzano transazioni, si diffondono idee e si acquisiscono informazioni. Ciò è reso possibile da una struttura che consente di facilitare l'interazione a distanza, anche su scala globale, tra due o più gruppi diversi di soggetti (*multi-sided nature*). In via di estrema semplificazione, tenuto conto della prospettiva rilevante ai fini di questo Rapporto, su un versante si trovano le imprese, intenzionate a rafforzare la propria immagine o espandere la propria presenza sul mercato rendendo più visibili e fruibili i propri prodotti e siti web, nonché a ottimizzare la produzione e il marketing mediante targetizzazione della clientela; sull'altro versante i consumatori, che hanno interesse a trovare ed eventualmente comparare in modo rapido beni, servizi e prezzi, così come a beneficiare di costi di

transazione ridotti, della disponibilità di servizi innovativi e della personalizzazione di offerte e funzionalità basata sull'intercettazione dei propri bisogni, gusti e interessi.

Quale che sia il modello di business prescelto, l'ambito di operatività o la dimensione, l'attività delle piattaforme online (quali motori di ricerca, siti comparatori, *marketplace*, fornitori di contenuti audio-visivi, social e professional network e così via) si fonda sulla raccolta e l'elaborazione di dati. Attraverso le nuove tecnologie il dato, e il dato personale in particolare, può essere archiviato, sezionato, analizzato, confrontato, condiviso e assume rilevanza come asset strategico da cui estrarre valore. Se i dati sono il nuovo petrolio, le piattaforme ne sono giganteschi serbatoi.

In ragione della centralità dei dati, la tutela della privacy e l'esigenza di assicurare un effettivo controllo sui dati da parte della persona a cui i dati si riferiscono assumono un ruolo cruciale nel sistema. Emergono nuovi e spesso imprevedibili rischi, amplificati man mano che le tecnologie si evolvono (si pensi all'avvento dell'intelligenza artificiale e ai sistemi di *big data analytics* e *data mining*) e si delineano nuove sfide per il quadro regolatorio e l'*enforcement*, così come per la compliance, alla ricerca del punto di equilibrio tra esigenze di tutela e necessità di non frenare lo sviluppo della *data economy* e le opportunità dell'innovazione *data-driven*.

L'Unione europea ha compiuto una scelta molto chiara in favore di un approccio che, muovendo dal riconoscimento del valore dei dati come leva per l'innovazione e la crescita economica, sia incentrato sull'utilizzo corretto, trasparente, responsabile e consapevole dei dati e sulla protezione dei diritti degli individui come presupposto per la libera circolazione dei dati stessi e la creazione di un mercato unico digitale. Ai principi e alle prescrizioni del GDPR, già ampiamente ispirati all'esigenza di definire un quadro più solido e coerente in materia di protezione dei dati personali, tenendo conto delle sfide poste dall'evoluzione tecnologica e dalla globalizzazione, si è affiancata la Dichiarazione europea sui diritti e principi digitali, che afferma la centralità della persona nel contesto della trasformazione digitale e impegna l'Unione europea e gli Stati membri a farsi promotori di questa visione anche in sede internazionale. In particolare, la Dichiarazione richiama il diritto delle persone a un ambiente digitale sicuro e protetto, che tuteli la vita privata fin dalla progettazione "traducendosi in un elevato livello di riservatezza, integrità, disponibilità e autenticità delle informazioni trattate" e il diritto degli individui a un controllo effettivo su come sono utilizzati i propri dati e con chi sono condivisi. Una speciale attenzione è dedicata al tema della protezione dei bambini e dei giovani rispetto a determinate condotte proprie dell'ambiente digitale e delle

piattaforme (diffusione di contenuti dannosi e illegali, sfruttamento, manipolazione e abusi online nonché tracciamento, profilazione e targeting illegali, in particolare a fini commerciali) e all'esigenza di renderli più autonomi e responsabili nell'ambiente digitale, offrendo loro "opportunità per acquisire le necessarie capacità e competenze, tra cui l'alfabetizzazione mediatica e il pensiero critico, per navigare e interagire nell'ambiente digitale in modo attivo e sicuro e per compiere scelte informate".

Sulla cornice di principi per la creazione della fiducia digitale fissati dal GDPR e richiamati dalla Dichiarazione si innestano le altre iniziative della Strategia digitale europea, che includono regole volte a prevenire gli abusi di potere economico delle piattaforme '*gatekeeper*', garantendo mercati aperti, equi e contendibili (*Digital Markets Act*-DMA), e regole per rafforzare la responsabilità delle grandi piattaforme nel contrasto alla disinformazione e alla diffusione di contenuti illeciti e per assicurare maggiore trasparenza nelle pratiche relative a pubblicità e sistemi di raccomandazione online, con specifiche misure a tutela dei minori (*Digital Services Act*-DSA). Va sottolineato che questi atti normativi, sia pure con formule diverse, fanno espressamente salvi il rispetto e l'applicazione del GDPR. Analogamente, il regolamento europeo sull'intelligenza artificiale (AI Act), che stabilisce i requisiti per la commercializzazione e l'utilizzo nel territorio dell'Unione dei sistemi di IA, come anticipato sempre più integrati nell'attività di profilazione svolta dalle piattaforme, lascia impregiudicate le norme in materia di protezione dei dati personali. Il diritto alla privacy e al controllo dei dati è e resta quindi uno dei pilastri dell'intero sistema.

2. Attività delle piattaforme e criticità per la protezione dei dati personali

Guardando all'operatività delle piattaforme, tra le principali aree critiche per la protezione dei dati personali si annoverano quelle di seguito sinteticamente illustrate. Come si vedrà, le questioni sono perlopiù legate all'attività di profilazione, intesa come trattamento automatizzato di dati personali per valutare, analizzare o prevedere determinati aspetti della persona (rendimento professionale, situazione economica, salute, preferenze personali, interessi, affidabilità, comportamento, ubicazione o spostamenti), che è al cuore dei modelli di business delle piattaforme. In questa breve, e necessariamente non esaustiva, esposizione verranno messi in rilievo gli indirizzi e i chiarimenti resi negli ultimi anni dalle autorità a diverso titolo chiamate ad interpretare e applicare le norme a tutela della privacy a livello

nazionale, europeo e internazionale.

2.1. Eccesso di dati raccolti

Un primo ambito problematico riguarda l'eccessiva ampiezza e pervasività della raccolta di dati (dagli identificativi classici agli identificativi online, dalle tracce di navigazione ai dati frutto di inferenze), che possono risultare in contrasto con i principi di correttezza, minimizzazione e limitazione delle finalità del trattamento posti dal GDPR, oltre ad aumentare i rischi di accessi non autorizzati, scraping indiscriminato e data breach. Va sottolineato che la correttezza/*fairness* si afferma sempre più come parametro di riferimento ai fini della valutazione di legittimità delle condotte relative alla fornitura di servizi online, in un'accezione ampia che comprende "il riconoscimento delle ragionevoli aspettative degli interessati, la considerazione di eventuali conseguenze negative per gli interessati a causa del trattamento e la valutazione del rapporto fra interessati e titolare del trattamento nonché degli effetti potenzialmente derivanti da squilibri in tale rapporto" (*European Data Protection Board* – EDPB, *Guidelines* 2/2019). In questa prospettiva, ad esempio, forme di profilazione molto intrusive nella sfera personale possono presentare di per sé una incompatibilità con il GDPR.

2.2. Insufficiente trasparenza

Vi è poi la questione della trasparenza, spesso insufficiente, nei confronti dell'interessato in ordine alle modalità e finalità del trattamento-profilazione svolto dalle piattaforme o ai tempi di conservazione dei dati. Per quanto l'utente medio che naviga online stia diventando progressivamente più consapevole del possibile utilizzo dei dati personali per finalità pubblicitarie, la giurisprudenza ha chiarito che resta fermo a carico delle piattaforme l'onere di adottare "un sistema informativo sulla profilazione dei dati personali chiaro, esaustivo e di immediata percezione, tanto più che non è irragionevole ritenere che la maggioranza degli utenti accede ai servizi in modo rapido, senza soffermarsi eccessivamente sulle indicazioni preliminari; per cui è necessario che le informazioni siano immediatamente percepibili, senza la necessità di interpretare le stesse o consultare ulteriori link" (Cons. Stato, sez. VI, sent. 7 gennaio 2025, n. 80). La mancanza di trasparenza non consente all'interessato di valutare in modo appropriato il 'costo' e le conseguenze del conferimento dei suoi dati.

2.3. Base giuridica del trattamento

Altro aspetto controverso è quello dell'individuazione, da effettuare alla luce del principio di accountability, della base giuridica più appropriata per la raccolta e l'utilizzo di dati da parte delle piattaforme. A valle delle pronunce che hanno escluso la possibilità di invocare la necessità-oggettiva indispensabilità del trattamento per l'esecuzione del contratto ed evidenziato la difficoltà di ricorrere al legittimo interesse per giustificare pratiche intrusive di profilazione e tracciamento a fini di marketing (C. Giust., sent. 4 luglio 2023, C-252/21, *Meta Platforms*; EDPB, *Guidelines 1/2024*; GPDP, provv. 7 luglio 2022, n. 248), alcune piattaforme hanno introdotto un modello '*pay or consent*', che pone, in sostanza, l'interessato di fronte alla scelta tra l'autorizzazione ad essere profilato a fini commerciali e il versamento di un corrispettivo monetario per la fruizione del servizio. Tale modalità risulta controversa in quanto non garantisce una genuina e libera (i.e. non condizionata dalla prospettiva di un possibile pregiudizio nel caso di mancato consenso) manifestazione di volontà dell'interessato. La posizione assunta al riguardo dall'EDPB è nel senso che spetti alla piattaforma offrire all'utente un'alternativa equivalente, gratuita e senza pubblicità comportamentale (EDPB, *Parere 8/2024*). Alla base di questo approccio vi è l'idea che determinati servizi offerti dalle piattaforme possono risultare insostituibili per la persona e decisivi per la partecipazione alla vita sociale. È ragionevole ritenere che a una diversa soluzione possa pervenirsi nelle ipotesi di applicazione del modello '*pay or consent*' ad opera di soggetti diversi dalle (grandi) piattaforme, qualora l'utente abbia la possibilità di accedere ad alternative soddisfacenti disponibili sul mercato.

Nella recente attività del Garante si segnala la decisione relativa a una piattaforma che raccoglieva i dati personali dei clienti (per conferimento diretto o acquisendoli da terzi su delega degli interessati) per elaborare e vendere profili di consumo e attribuire poi ai clienti stessi una percentuale dei ricavi ottenuti (GPDP, provv. 14 novembre 2024, n. 704). Il Garante ha ritenuto che il trattamento non potesse essere considerato necessario per l'esecuzione del contratto tra piattaforma e cliente e ha indicato nel consenso dell'interessato la base giuridica più appropriata, rilevando tuttavia nel caso di specie il rischio che il riconoscimento di un corrispettivo economico per la cessione di dati potesse pregiudicare la natura libera del consenso, in particolare per le persone vulnerabili.

Per assicurare la piena consapevolezza della persona, la richiesta di consenso deve in ogni caso essere specifica in relazione a finalità di trattamento identificate in modo chiaro e preciso. Secondo l'orientamento consolidato del Garante, la capacità di autodeterminazione non è assicurata

quando si raccoglie il consenso in modo indifferenziato per perseguire distinte finalità, ben potendo essere ciascuna di esse perseguita singolarmente in presenza di un'autonoma valutazione e determinazione dell'interessato. Nella stessa prospettiva è da stigmatizzare la pratica di utilizzare, nell'individuazione delle finalità del trattamento, formule vaghe, che facciano generico riferimento al miglioramento dell'esperienza utente o a scopi di marketing.

2.4. I dark pattern

Tra le condotte delle piattaforme in contrasto con le disposizioni a tutela dei dati personali, con speciale riguardo ai principi di correttezza, trasparenza e *privacy-by-design*, un'attenzione particolare meritano i dark pattern, intesi come interfacce e processi di navigazione progettati per sfruttare i bias cognitivi e indurre gli utenti a prendere decisioni involontarie e potenzialmente dannose dal punto di vista della privacy. Secondo la tipizzazione effettuata dall'EDPB con riferimento alle piattaforme di social media (*Guidelines 03/2022*), tali pratiche decettive includono: il sovraccarico di richieste/opzioni/possibilità, tali da sollecitare gli utenti a condividere più dati possibili o consentire involontariamente al trattamento (*overloading*); la progettazione di interfacce che portino gli utenti a trascurare gli aspetti di protezione dei dati (*skipping*); le tecniche che influenzano le scelte degli utenti facendo appello alle loro emozioni o utilizzando sollecitazioni visive (*stirring*); gli ostacoli alla possibilità degli utenti di informarsi correttamente sul trattamento e gestire i propri dati (*obstructing*); la mancanza di coerenza e chiarezza nella progettazione delle interfacce, che rende difficile per l'utente avvalersi degli strumenti di controllo della privacy e comprendere la finalità del trattamento (*fickle*); la progettazione delle interfacce in modo da nascondere informazioni o strumenti di controllo della privacy, lasciando gli utenti nell'incertezza (*left in the dark*). Molto opportunamente l'EDPB ha formulato raccomandazioni che mirano sia a guidare la progettazione delle interfacce in modo da evitare i dark pattern, sia a sensibilizzare maggiormente gli utenti sui propri diritti e sui rischi potenziali derivanti dalla condivisione di una quantità eccessiva di dati.

L'importanza del tema ha determinato inoltre un'iniziativa di cooperazione internazionale, sotto forma di un'indagine congiunta (*sweep*) sui dark pattern utilizzati da siti web e app, nell'ambito del *Global Privacy Enforcement Network*, per la prima volta insieme all'analoga rete delle autorità a tutela dei consumatori (*International Consumer Protection and Enforcement Network*). Si tratta di un modello apprezzabile di coordinamento tra autorità preposte all'*enforcement* di norme diverse ma strettamente connesse, che è

auspicabile prosegua nel segno del dialogo costruttivo e della sinergia di competenze.

2.5. Le decisioni interamente automatizzate

Un rischio significativo di compressione dei diritti e delle libertà fondamentali caratterizza l'utilizzo della profilazione nell'ambito di processi decisionali automatizzati. Per tale motivo il legislatore europeo ha previsto un quadro di garanzie rafforzate (art. 22 del GDPR), riconoscendo all'interessato il diritto di non essere sottoposto a decisioni interamente automatizzate che incidono significativamente sulla sua sfera personale, a meno che la decisione sia necessaria per l'esecuzione di un contratto, o sia autorizzata, con adeguate misure di tutela, dal diritto europeo o nazionale, oppure sia stato acquisito un consenso esplicito dell'interessato stesso. In queste ipotesi, l'interessato – oltre a dover essere preventivamente informato sulla logica utilizzata ai fini della profilazione (da intendersi come schema esecutivo dell'algoritmo, che specifica i passi da eseguire in sequenza per giungere al risultato, C. Cass., sez. I civ., ord. 6 ottobre 2023, n. 28538) e sulle possibili conseguenze – ha il diritto di chiedere l'intervento umano, esprimere la propria opinione e, previo l'ottenimento di spiegazioni concise e comprensibili sulla procedura e i principi alla base del trattamento (C. Giust., sent. 27 febbraio 2025, C-203/22, *DB*), contestare la decisione.

2.6. Ia ed effetto manipolativo

Su come evitare che le tecniche di profilazione e personalizzazione comportino una lesione della sfera individuale, oltre alle importanti indicazioni fornite dall'EDPB (*Guidelines wp251rev.01*), utili chiarimenti emergono dalle recenti Linee guida della Commissione europea sulle pratiche di intelligenza artificiale vietate ai sensi dell'AI Act (C(2025) 5052 final). La Commissione sottolinea l'esigenza di distinguere tra manipolazione, che restringe l'autonomia dell'individuo, e persuasione, che opera nei confini della trasparenza e del rispetto dell'individuo. Ne deriva, in linea di principio (e sempre fatta salva la compliance con il GDPR oltre che con il DSA), che sono legittime le forme di raccomandazione e advertising personalizzato realizzate dalle piattaforme sulla base di algoritmi trasparenti e preferenze dell'utente, mentre non sono ammissibili, ad esempio, sistemi di IA volti a inferire le emozioni dei consumatori in modo nascosto per offrire prodotti a prezzi più elevati in uno specifico momento, sfruttando la maggiore propensione all'acquisto dell'interessato.

2.7. La questione dell'age verification

Il rapporto tra minori e piattaforme merita una considerazione particolare. È noto che, quando sono coinvolti minori, eventuali violazioni in materia di trattamento dei dati personali possono più facilmente tradursi in rischi gravi per la sicurezza e l'incolumità, ad esempio se in base alla profilazione vengono proposti contenuti inadatti o violenti o addirittura suggeriti comportamenti autolesionistici, nonché in caso di accesso non autorizzato ad informazioni che potrebbero consentire a terzi malintenzionati l'identificazione e l'adescamento del minore (OCSE, *Towards Digital Safety by Design for Children*, 2024). Una questione ulteriore riguarda le misure di tutela, in particolare i meccanismi di *age verification*, che potrebbero essere configurati in modo da comportare da parte della piattaforma l'acquisizione ingiustificata, in contrasto col principio di minimizzazione, di informazioni sensibili o dati biometrici relativi al minore.

Per far fronte alle questioni menzionate, è essenziale promuovere l'adozione di architetture privacy specificamente '*child-friendly*' e assicurare che ai minori siano fornite informazioni semplici, chiare e facilmente accessibili riguardo al trattamento dei loro dati e ai diritti conseguenti. Accanto a un *enforcement* rigoroso delle regole da parte delle autorità preposte (si pensi ai provvedimenti del Garante nei confronti di Tik Tok o del chatbot Replika), assumono quindi fondamentale importanza le iniziative di soft law, quali raccomandazioni, best practices e codici di condotta, che orientino le piattaforme verso la migliore attuazione dei principi di *privacy-by-design* e *privacy-by-default* con riferimento ai servizi di intermediazione online fruibili dai minori. Data la rilevanza e l'impatto *cross-border* delle questioni in gioco, il confronto di esperienze (GPDP, *Vulnerable Individuals. Tools for Online Protection. Children and Age Verification - Spring Conference* 2023) e l'elaborazione di soluzioni condivise a livello UE (come previsto ad esempio nell'ambito *European strategy for a better internet for kids - BIK+, 2022)* dovrebbero rappresentare la via maestra.

3. Sfide per la regolazione e l'*enforcement* ed esigenza di coordinamento degli attori coinvolti

Il quadro normativo relativo all'attività delle piattaforme è oggi reso complesso dall'interazione di varie discipline, il cui *enforcement* è affidato ad autorità diverse. La profilazione, ad esempio, che in quanto trattamento di dati personali risponde alle regole del GDPR, soggiace al contempo alle norme a tutela dei consumatori (potendo l'assenza di trasparenza circa lo

sfruttamento commerciale dei dati del consumatore dar luogo a una pratica commerciale scorretta ed essendo previsto un obbligo informativo precontrattuale specifico in caso di personalizzazione del prezzo basata su un processo decisionale automatizzato) nonché ai requisiti e alle prescrizioni specifiche contenuti nel DMA (obbligo di chiedere il consenso degli utenti per combinare i loro dati personali tra i servizi o di rendere comunque accessibile un'alternativa meno personalizzata ma equivalente; obbligo di presentare una descrizione, sottoposta ad audit indipendente, di tutte le tecniche di profilazione dei consumatori realizzate), nel DSA (obbligo di assicurare la riconoscibilità della pubblicità personalizzata e di consentire l'identificazione dei parametri utilizzati per determinarne il destinatario; divieto di pubblicità personalizzata basata su categorie di dati sensibili o rivolta a minori) e ai divieti dell'AI Act quando l'algoritmo di profilazione possa determinare manipolazione comportamentale e danneggiare le persone o sia funzionale al *social scoring*. Un caso analogo è quello delle condotte qualificabili come *dark pattern*, che sono suscettibili di ricadere nel campo di applicazione non solo del GDPR, ma anche della disciplina in tema di pratiche commerciali scorrette e del DSA.

A fronte di uno scenario caratterizzato da pluralità di norme e interventi che insistono potenzialmente sulle stesse fattispecie, l'Unione europea sta oggi valutando l'introduzione di un ulteriore strumento legislativo, un *Digital Fairness Act*, per rafforzare la protezione dei consumatori rispetto a determinate pratiche tipiche del contesto digitale (tra cui *dark pattern*, design che crea dipendenza, personalizzazione dei prezzi e della pubblicità, rinnovi automatici e recesso dai contratti online) e colmare i gap di tutela percepiti. Nell'ambito di questa iniziativa, l'Unione si interroga anche sull'opportunità di misure di semplificazione della legislazione volte a ridurre determinati oneri per le imprese.

L'obiettivo da perseguire, per un mercato unico digitale che contribuisca al rilancio della competitività europea, dovrebbe essere un quadro di riferimento semplice e snello, basato sui principi fondamentali della trasparenza e della correttezza e sul pieno riconoscimento del diritto dell'individuo al controllo dei propri dati personali. L'approccio lungimirante della *privacy-by-design-and-by-default* introdotto dal GDPR può, se correttamente implementato, già consentire di evitare molte delle criticità per la protezione dei dati legate all'attività delle piattaforme. Sulla base dell'esperienza, per prevenire il rischio di incoerenze nella regolazione andrebbe seguita l'indicazione del Consiglio UE secondo cui l'adozione di ogni norma contenente previsioni in materia di trattamento di dati personali dovrebbe essere preceduta da una solida analisi di impatto (*Council position and findings*

on the application of the GDPR, 15507/23, 17 november 2023, para. 40), non limitandosi al semplice richiamo della formula che lascia impregiudicata l'applicazione del GDPR.

Le Linee guida e i pareri dell'EDPB hanno già contribuito in modo significativo, come accennato in precedenza, a chiarire alcuni snodi cruciali del regime applicabile alle piattaforme e a promuovere un approccio armonizzato all'applicazione delle regole da parte delle autorità nazionali, fondamentale nel contesto della digitalizzazione e della globalizzazione dell'economia. Di particolare rilievo sono le recenti Linee guida sull'interazione tra GDPR e DSA, in cui vengono considerate e analizzate le disposizioni di quest'ultimo che implicano il trattamento dei dati personali da parte dei prestatori intermediari di servizi, per assicurare la compatibilità con il GDPR degli adempimenti previsti.

Altrettanto fondamentali per il buon funzionamento del sistema sono gli strumenti di co-regolazione previsti dal GDPR, in particolare i Codici di condotta, che possono consentire di adattare la disciplina alle sfide poste dalle nuove tecnologie secondo una visione condivisa dagli operatori, aumentando la fiducia e agevolando la compliance. È importante proseguire anche il ricorso alla consultazione come metodo per ricercare, nel dialogo con gli stakeholder, soluzioni coerenti e rendere la regolazione "il più possibile aderente alle istanze sociali" (GDPD, *Potere e responsabilità. La cultura della protezione dei dati,* Relazione del Presidente Pasquale Stanzione 2024).

Per rafforzare il livello di consapevolezza dei consumatori circa i propri diritti nel contesto online e nei rapporti con le piattaforme è richiesto un impegno collettivo, a vari livelli. Le autorità, e il Garante in particolare, già svolgono in relazione alle rispettive attribuzioni un'opera fondamentale di sensibilizzazione e promozione dell'educazione digitale. L'organizzazione di iniziative di formazione, soprattutto a beneficio delle giovani generazioni con campagne a livello scolastico, può rappresentare un terreno di elezione per sviluppare una cooperazione ad hoc tra autorità, associazioni di consumatori e operatori economici. L'esigenza di predisporre misure di alfabetizzazione degli utenti è peraltro costantemente ribadita dalle istituzioni europee (si pensi alle previsioni che stabiliscono un vero e proprio obbligo in questo senso a carico delle piattaforme per la condivisione di contenuti audiovisivi) ed è da ultimo stata recepita anche nell'ambito del regolamento sull'intelligenza artificiale.

L'esistenza di una pluralità di autorità competenti all'*enforcement* delle diverse norme pone la questione delle possibili sovrapposizioni e determina incertezze per gli operatori. L'esigenza di un efficace coordinamento tra autorità, ai fini di una convergenza di approcci interpretativi e di un *enfor-*

cement più efficace, è quanto mai sentita. I protocolli sono uno strumento utile, per assicurare una maggiore coerenza nelle valutazioni. Molto opportunamente, ad esempio, il protocollo tra AGCM e Garante valorizza la consultazione reciproca nell'ambito delle rispettive istruttorie. Un passo ulteriore che appare oggi sempre più auspicabile consiste nella previsione di una sede stabile di dialogo e confronto, estesa alle diverse autorità con competenze in materia di piattaforme e di digitale.

Data la dimensione globale delle sfide connesse all'economia digitale, anche la cooperazione tra ordinamenti diventa sempre più indispensabile. L'OCSE ha recentemente auspicato, ad esempio, l'interazione e lo sviluppo di policy integrate tra le community AI e *data protection* sulle questioni di comune interesse, per evitare duplicazione di interventi e applicazione di misure divergenti, che aumentano la complessità della *compliance* e dell'e*nforcement* (OECD, *AI, Data Governance and Privacy. Synergies and Areas of International Co-operation,* Artificial Intelligence Papers no. 22/2024). La spinta all'innovazione non implica infatti un arretramento in termini di tutele, ma richiede la ricerca di un assetto di regole e poteri equilibrato e ancorato alla salvaguardia dei diritti e delle libertà fondamentali, nel segno della proporzionalità.