COMMISSIONE
EUROPEA

Bruxelles, 25.7.2024
COM(2024) 357 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Seconda relazione sull'applicazione del regolamento generale sulla protezione dei dati

1 INTRODUZIONE

La presente è la seconda relazione della Commissione sull'applicazione del regolamento generale sulla protezione dei dati (*General Data Protection Regulation*, GDPR) ed è stata adottata a norma dell'articolo 97 di detto regolamento. La prima relazione è stata adottata il 24 giugno 2020 ("la relazione del 2020")([1]).

Il GDPR è uno dei fondamenti dell'approccio dell'UE alla trasformazione digitale. I suoi principi fondamentali (trattamento equo, sicuro e trasparente dei dati personali, volto a garantire che le persone mantengano il controllo su di essi) sono alla base di tutte le politiche dell'UE che comportano il trattamento di dati personali.

In seguito all'adozione della relazione del 2020, l'UE ha adottato una serie di iniziative volte a mettere le persone al centro della transizione digitale. Ciascuna iniziativa persegue un obiettivo specifico, ad esempio creare un ambiente online più sicuro, rendere l'economia digitale più equa e competitiva, agevolare la ricerca innovativa, garantire lo sviluppo di un'intelligenza artificiale sicura e affidabile e creare un autentico mercato unico dei dati. Ogniqualvolta comportano il trattamento di dati personali, le iniziative si basano sul GDPR. Quest'ultimo fornisce inoltre una base per iniziative settoriali che incidono sul trattamento dei dati personali, ad esempio nei settori dei servizi finanziari, della salute, dell'occupazione, della mobilità e dell'applicazione delle norme.

I portatori di interessi, le autorità di protezione dei dati e gli Stati membri concordano ampiamente sul fatto che, nonostante alcune sfide, il GDPR abbia prodotto risultati importanti per le persone e per le imprese. L'approccio basato sul rischio e tecnologicamente neutro assicura una solida protezione degli interessati e impone obblighi proporzionati ai titolari del trattamento e ai responsabili del trattamento. Allo stesso tempo dovrebbero essere compiuti ulteriori progressi in vari ambiti. In particolare, nei prossimi anni bisognerebbe prestare particolare attenzione a sostenere gli sforzi di conformità compiuti dai portatori di interessi, in particolare dalle piccole e medie imprese (PMI), dai piccoli operatori, dai ricercatori e dagli istituti di ricerca, garantendo che gli orientamenti forniti dalle autorità di protezione dei dati siano più chiari e più facilmente attuabili e rendendo l'interpretazione e l'applicazione del GDPR più coerenti in tutta l'UE.

A norma dell'articolo 97 del GDPR, la Commissione dovrebbe esaminare in particolare l'applicazione e il funzionamento del trasferimento internazionale di dati personali verso paesi terzi (ossia paesi al di fuori dell'UE/del SEE) (capo V del GDPR) e dei meccanismi di cooperazione e coerenza tra le autorità nazionali di protezione dei dati (capo VII del GDPR). Tuttavia, analogamente alla relazione del 2020, la presente relazione fornisce una valutazione generale dell'applicazione del GDPR che va oltre i suddetti due elementi: essa individua anche una serie di azioni necessarie a sostenere l'applicazione efficace del GDPR in settori prioritari fondamentali.

La presente relazione tiene conto delle fonti seguenti: i) la posizione e le conclusioni del Consiglio, adottate nel dicembre 2023([2]); ii) gli input forniti dai portatori di interessi, in particolare attraverso il gruppo multilaterale sul GDPR([3]) e nell'ambito di un invito

---

([1]) La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati (COM(2020) 264 final del 24.6.2020).

([2]) https://data.consilium.europa.eu/doc/document/ST-15507-2023-INIT/it/pdf.

([3]) Una sintesi del contributo fornito dal gruppo multilaterale di esperti sul GDPR è disponibile al link seguente: Report from Multistakeholder Expert group on GDPR application - June 2024.pdf. Gli input

pubblico a presentare contributi([4]); e iii) gli input forniti dalle autorità di protezione dei dati attraverso il contributo del comitato europeo per la protezione dei dati (*European Data Protection Board*, EDPB)([5]) ("il comitato") e una relazione elaborata dall'Agenzia per i diritti fondamentali (FRA) sulla base di colloqui con singole autorità di protezione dei dati([6]) ("la relazione della FRA"). La relazione si basa inoltre sul monitoraggio continuo dell'applicazione del GDPR da parte della Commissione, anche attraverso dialoghi bilaterali con gli Stati membri in merito alla conformità della legislazione nazionale, il contributo attivo alle attività del comitato e contatti stretti con un'ampia gamma di portatori di interessi in relazione all'applicazione pratica del regolamento.

2 L'APPLICAZIONE DEL GDPR E IL FUNZIONAMENTO DEI MECCANISMI DI COOPERAZIONE E COERENZA

Il sistema di applicazione di tipo "sportello unico" del GDPR mira a garantire un'interpretazione e un'applicazione armonizzate da parte delle autorità indipendenti di protezione dei dati. Il sistema richiede la cooperazione tra le autorità di protezione dei dati nei casi di trattamento transfrontaliero, che incidono in modo sostanziale su interessati di molteplici Stati membri. Eventuali controversie tra le autorità sono risolte dal comitato nell'ambito del meccanismo di coerenza del GDPR.

2.1 Rendere più efficiente la gestione dei casi transfrontalieri: la proposta relativa alle norme procedurali

La relazione del 2020 ha rilevato la necessità di rendere più efficiente e armonizzato il trattamento dei casi transfrontalieri in tutta l'UE, in particolare alla luce delle notevoli differenze tra le procedure amministrative e le interpretazioni nazionali dei concetti nell'ambito del meccanismo di cooperazione del GDPR. Nel luglio 2023 la Commissione ha pertanto adottato una proposta di regolamento relativa alle norme procedurali([7]), basata tra l'altro su un elenco di questioni che il comitato ha portato all'attenzione della Commissione nell'ottobre 2022([8]) e su contributi forniti dai portatori di interessi([9]) e dagli Stati membri([10]). La proposta integra il GDPR stabilendo norme dettagliate sui reclami transfrontalieri, sul coinvolgimento del reclamante, sui diritti della difesa delle parti oggetto dell'indagine (titolari del trattamento e responsabili del trattamento) e sulla cooperazione tra le autorità di protezione dei dati. L'armonizzazione di tali aspetti procedurali favorirebbe il tempestivo completamento delle indagini e l'offerta di rimedi rapidi alle persone. La proposta è attualmente oggetto di negoziati in seno al Parlamento europeo e al Consiglio.

---

ricevuti in risposta all'invito pubblico a presentare contributi e attraverso le riunioni bilaterali con i portatori di interessi rispecchiano in larga misura le opinioni espresse dai membri del gruppo multilaterale di esperti sul GDPR.

([4]) Di' la tua - Consultazioni pubbliche e feedback (europa.eu) .

([5]) Contribution of the EDPB to the evaluation of the GDPR under Article 97 | comitato europeo per la protezione dei dati (europa.eu).

([6]) GDPR in practice – Experiences of data protection authorities | Agenzia dell'Unione europea per i diritti fondamentali (europa.eu).

([7]) Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme procedurali aggiuntive relative all'applicazione del regolamento (UE) 2016/679 (COM(2023) 348 final).

([8]) https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-eu-commission-procedural-aspects-could-be_it.

([9]) Attraverso il gruppo multilaterale di esperti sul GDPR e nell'ambito di un invito a presentare contributi pubblicato nel febbraio 2023.

([10]) In particolare attraverso il gruppo di esperti degli Stati membri sul GDPR: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=it&do=groupDetail.groupDetail&groupID=3461.

2.2 Una maggiore cooperazione tra le autorità di protezione dei dati e il ricorso al meccanismo di coerenza

Il numero di casi transfrontalieri è aumentato notevolmente negli ultimi anni. Le autorità di protezione dei dati hanno dimostrato una maggiore disponibilità ad avvalersi degli strumenti di cooperazione previsti dal GDPR. Tutte le autorità di protezione dei dati

hanno fatto ricorso allo strumento di assistenza reciproca([11]) e a richieste "informali" di assistenza reciproca su base volontaria. Le autorità di protezione dei dati prediligono le richieste informali, che non impongono un termine né un rigoroso obbligo di risposta.

([11]) Articolo 61 del GDPR.

Benché nel 2021 il comitato abbia adottato orientamenti sulle operazioni congiunte([12]), le autorità non hanno ancora fatto un uso significativo di tale strumento([13]), adducendo a motivo di ciò differenze tra le procedure nazionali e una mancanza di chiarezza in merito alla procedura.

Il GDPR offre alle autorità di protezione dei dati interessate la possibilità di sollevare un'obiezione pertinente e motivata qualora non concordino con un progetto di decisione dell'autorità di protezione dei dati capofila in un caso transfrontaliero. Se le autorità di protezione dei dati non riescono a raggiungere un consenso su un'obiezione pertinente e motivata, il GDPR prevede la composizione delle controversie da parte del comitato([14]). Le questioni sollevate più di frequente nelle obiezioni pertinenti e motivate sono state le seguenti: i) la base giuridica del trattamento; ii) gli obblighi di informazione e trasparenza; iii) la notifica delle violazioni dei dati; iv) i diritti degli interessati; v) le deroghe per i trasferimenti internazionali; vi) il ricorso a misure correttive; e vii) l'importo di una sanzione amministrativa pecuniaria.

Il sistema di applicazione del GDPR presuppone una cooperazione leale ed efficace tra le autorità di protezione dei dati. Sebbene la procedura di composizione delle controversie svolga un ruolo importante nell'architettura dell'applicazione delle norme, essa dovrebbe essere utilizzata in maniera conforme allo spirito con cui è stata concepita, tenendo debitamente conto in particolare della ripartizione delle competenze tra le autorità di protezione dei dati, della necessità di rispettare i diritti della difesa e dell'interesse degli interessati a una tempestiva risoluzione del caso. Ciascuna procedura di composizione delle controversie esige l'utilizzo di risorse significative da parte dell'autorità capofila, delle autorità interessate e della segreteria del comitato e ritarda l'offerta di un rimedio agli interessati.

Maggiore ricorso agli strumenti di cooperazione da parte delle autorità di protezione dei dati

- Nel sistema di scambio di informazioni del comitato sono registrati quasi 2 400 casi([15]).
- Le autorità di protezione dei dati capofila hanno adottato circa 1 500 progetti di decisione([16]), 990 dei quali si sono tradotti in decisioni definitive che hanno accertato una violazione del GDPR([17]).
- Le autorità di protezione dei dati hanno presentato quasi 1 000 richieste "formali" di assistenza reciproca([18]) e circa 12 300 richieste "informali"([19]).
- Sono state avviate cinque operazioni congiunte alle quali hanno partecipato le autorità di protezione dei dati di sette Stati membri.

([12]) internal_edpb_document_1_2021_on_art_62_joint_operations_en.pdf (europa.eu)
([13]) Articolo 62 del GDPR.
([14]) Articolo 65 del GDPR.
([15]) Al 3 novembre 2023 (contributo fornito dal comitato).
([16]) Ai sensi dell'articolo 60, paragrafo 3, del GDPR.
([17]) Al 3 novembre 2023.
([18]) L'autorità irlandese ha presentato il maggior numero di richieste formali (246), mentre le autorità tedesche hanno ricevuto il maggior numero di richieste (516).
([19]) L'autorità irlandese ha presentato il maggior numero di richieste informali (4 245), seguita dalle autorità tedesche (2 036).

- Le autorità di protezione dei dati di 18 Stati membri hanno sollevato obiezioni pertinenti e motivate([20]).

Le autorità di protezione dei dati utilizzano in misura crescente il meccanismo di coerenza del GDPR, il quale si articola in tre componenti: i) i pareri del comitato; ii) la composizione delle controversie da parte del comitato; e iii) la procedura d'urgenza([21]).

I pareri del comitato vertono in misura crescente su importanti questioni in materia di applicazione generale([22]). Il comitato dovrebbe garantire una consultazione tempestiva e significativa prima dell'adozione di tali pareri. La composizione delle controversie ha affrontato casi riguardanti questioni quali la base giuridica del trattamento dei dati per la pubblicità comportamentale sui social media e il trattamento dei dati dei minori online. La maggior parte delle successive decisioni vincolanti è stata impugnata dinanzi al Tribunale.

La trasparenza del processo decisionale del comitato è un elemento fondamentale per garantire il rispetto del diritto a una buona amministrazione sancito dalla Carta dei diritti fondamentali dell'UE. La procedura d'urgenza del GDPR consente alle autorità di protezione dei dati di derogare al meccanismo di cooperazione e coerenza per adottare misure urgenti, ove ciò sia necessario per tutelare i diritti e le libertà degli interessati. In deroga alla normale procedura di cooperazione prevista dal GDPR, strumenti come la procedura d'urgenza sono concepiti per essere utilizzati solo in circostanze eccezionali e laddove la normale procedura di cooperazione non sia in grado di tutelare i diritti e le libertà degli interessati.

Il meccanismo di coerenza

- Il comitato ha adottato 190 pareri in materia di coerenza.
- Nove decisioni vincolanti sono state adottate nell'ambito della composizione delle controversie([23]). Tutte hanno imposto all'autorità di protezione dei dati capofila di modificare il suo progetto di decisione e molte hanno comportato l'irrogazione di sanzioni pecuniarie significative.
- Cinque autorità di protezione dei dati hanno adottato misure provvisorie nell'ambito della procedura d'urgenza (Germania, Finlandia, Italia, Norvegia e Spagna).
- Due autorità di protezione dei dati hanno chiesto l'emissione di una decisione vincolante d'urgenza del comitato([24]) e quest'ultimo ha disposto l'adozione di misure definitive urgenti in un caso.

([20]) Delle 289 obiezioni pertinenti e motivate segnalate dalle autorità, 101 (35 %) sono state sollevate dalle autorità tedesche. Il tasso di successo nel raggiungere un consenso sulle obiezioni pertinenti e motivate varia dal 15 % (delle obiezioni sollevate dalle autorità tedesche) al 100 % (delle obiezioni sollevate dall'autorità polacca).
([21]) Rispettivamente articoli 64, 65 e 66 del GDPR.
([22]) Pareri a norma dell'articolo 64, paragrafo 2, del GDPR.
([23]) A norma dell'articolo 65, paragrafo 1, lettera a), del GDPR.
([24]) A norma dell'articolo 66, paragrafo 2, del GDPR.

2.3 Un'applicazione più rigorosa delle norme

Negli ultimi anni si è verificato un notevole miglioramento dell'attività di applicazione delle norme da parte delle autorità di protezione dei dati, tra cui l'imposizione di sanzioni pecuniarie significative nei confronti di grandi imprese tecnologiche multinazionali nell'ambito di casi di rilevanza storica. Sono state ad esempio irrogate sanzioni pecuniarie per: i) la violazione della liceità e della sicurezza del trattamento; ii) la violazione del trattamento di categorie particolari di dati personali; e iii) il mancato rispetto di diritti delle persone fisiche([25]). Ciò ha indotto le imprese private a prendere sul serio la protezione dei dati([26]) e ha contribuito a creare una cultura del rispetto delle norme in seno alle organizzazioni. Le autorità di protezione dei dati adottano decisioni che accertano violazioni del GDPR nell'ambito di casi aperti sulla base di reclami o di propria iniziativa. Sebbene non in tutti gli Stati membri siano disponibili procedure di "composizione amichevole", molte autorità di protezione dei dati hanno fatto un uso efficace di tali procedure per risolvere casi basati su reclami in modo rapido e soddisfacente per il reclamante. La proposta relativa alle norme procedurali riconosce la possibilità di risolvere i reclami mediante composizione amichevole([27]).

Le autorità di protezione dei dati hanno fatto ampio uso dei loro poteri correttivi, anche se il numero delle misure correttive imposte varia notevolmente da un'autorità all'altra. Oltre alle sanzioni pecuniarie, le misure correttive più comunemente utilizzate sono state avvertimenti, ammonimenti e ordini di rispettare il GDPR. I titolari del trattamento e i responsabili del trattamento impugnano spesso le decisioni che accertano violazioni del GDPR dinanzi a organi giurisdizionali nazionali, nella maggior parte dei casi per motivi procedurali([28]).

Un'applicazione più rigorosa delle norme

- Le autorità di protezione dei dati hanno avviato oltre 20 000 indagini di propria iniziativa([29]).
- Collettivamente, ricevono oltre 100 000 reclami all'anno([30]).
- Il tempo mediano di trattamento dei reclami da parte delle autorità di protezione dei dati (dal ricevimento alla chiusura del caso) varia da 1 a 12 mesi ed è pari o inferiore a 3 mesi in cinque Stati membri (Danimarca (1 mese), Spagna (1,5 mesi), Estonia (3 mesi), Grecia (3 mesi) e Irlanda (3 mesi)).
- Oltre 20 000 reclami sono stati risolti mediante composizione amichevole. Tale meccanismo viene più comunemente utilizzato in Austria, Ungheria, Lussemburgo e Irlanda.
- Nel 2022 le autorità tedesche di protezione dei dati hanno adottato il maggior numero di decisioni che impongono una misura correttiva (3 261), seguite dalle autorità spagnole (774), lituane (308) ed estoni (332). I paesi che hanno imposto il

([25]) Cfr. il punto 5.3.4 del contributo del comitato.
([26]) Relazione della FRA, pag. 36.
([27]) Proposta relativa alle norme procedurali, articolo 5.
([28]) In Romania tutte e 26 le decisioni che hanno accertato una violazione sono state impugnate dinanzi a organi giurisdizionali, mentre nei Paesi Bassi il tasso di impugnazione è stato del 23 %. Il tasso più elevato di accoglimento delle impugnazioni è stato registrato in Belgio (39 %).
([29]) Le autorità tedesche di protezione dei dati hanno avviato il maggior numero di indagini di propria iniziativa (7 647), seguite dalle autorità ungheresi (3 332), austriache (1 681) e francesi (1 571).
([30]) Nel 2022 nove autorità di protezione dei dati hanno ricevuto oltre 2 000 reclami. Il numero più elevato di reclami è stato registrato in Germania (32 300), Italia (30 880), Spagna (15 128), Paesi Bassi (13 133) e Francia (12 193), mentre il numero più basso è stato registrato in Liechtenstein (40), Islanda (140) e Croazia (271).

minor numero di misure correttive sono stati il Liechtenstein (8), la Cechia (8), l'Islanda (10), i Paesi Bassi (17) e il Lussemburgo (22).

- Le autorità di protezione dei dati hanno irrogato oltre 6 680 sanzioni pecuniarie, per un importo totale di circa 4,2 miliardi di EUR([31]). L'autorità irlandese ha irrogato le sanzioni pecuniarie dall'importo complessivamente più elevato (2,8 miliardi di EUR), seguita dalle autorità lussemburghesi (746 milioni di EUR), italiane (197 milioni di EUR) e francesi (131 milioni di EUR). Il Liechtenstein (9 600 EUR), l'Estonia (201 000 EUR) e la Lituania (435 000 EUR) hanno irrogato le sanzioni pecuniarie dall'importo più basso.

Sebbene la maggior parte delle autorità di protezione dei dati ritenga adeguati i propri strumenti di indagine, alcune necessitano di strumenti aggiuntivi a livello nazionale, come sanzioni adeguate qualora i titolari del trattamento non cooperino o non forniscano le informazioni necessarie([32]). Le autorità di protezione dei dati ritengono che le risorse insufficienti e le lacune nelle competenze tecniche e giuridiche siano il principale fattore che incide sulla loro capacità di far rispettare le norme([33]).

2.4 Il comitato

Il comitato è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal Garante europeo della protezione dei dati, con la partecipazione della Commissione senza diritto di voto. Il comitato, coadiuvato nel suo lavoro dalla sua segreteria, ha il compito di garantire l'applicazione coerente del GDPR([34]). La maggior parte delle autorità di protezione dei dati ritiene che il comitato abbia svolto un ruolo positivo nel rafforzamento della cooperazione tra di loro([35]). Molte autorità di protezione dei dati dedicano risorse significative alle attività del comitato, anche se le autorità più piccole segnalano che le loro dimensioni impediscono loro di essere pienamente coinvolte([36]). Alcune autorità ritengono che l'efficienza dei processi del comitato debba essere migliorata, in particolare riducendo il numero delle riunioni e prestando minore attenzione alle questioni meno rilevanti([37]). A seconda dell'esito dei negoziati sulla proposta relativa alle norme procedurali del GDPR, che mira a ridurre il numero dei casi sottoposti all'attenzione del comitato ai fini della composizione delle controversie, potrebbe essere necessario valutare se il comitato necessiti di risorse aggiuntive.

A novembre 2023 il comitato aveva adottato 35 documenti di orientamento. Sebbene i portatori di interessi e le autorità di protezione dei dati li abbiano ritenuti utili, entrambe le parti ritengono che gli orientamenti dovrebbero essere forniti più rapidamente e che la qualità dovrebbe essere migliorata([38]). I portatori di interessi osservano che spesso gli orientamenti sono eccessivamente teorici, sono troppo lunghi e non riflettono l'approccio

([31]) Tutte le autorità hanno irrogato sanzioni amministrative pecuniarie, ad eccezione della Danimarca, che non prevede l'irrogazione di tali sanzioni. Il maggior numero di sanzioni è stato irrogato in Germania (2 106) e in Spagna (1 596). I paesi in cui è stato irrogato il minor numero di sanzioni sono stati il Liechtenstein (3), l'Islanda (15) e la Finlandia (20).
([32]) Relazione della FRA, pag. 38.
([33]) Relazione della FRA, pagg. 20 e 23. Cfr. anche la posizione e le conclusioni del Consiglio, punto 17.
([34]) Articolo 70, paragrafo 1, del GDPR.
([35]) Relazione della FRA, pag. 64.
([36]) Relazione della FRA, pag. 67. Nel 2023 le autorità tedesche di protezione dei dati hanno dedicato la maggior parte delle proprie risorse alle attività del comitato (26 equivalenti a tempo pieno (ETP)), seguite da Irlanda (16) e Francia (12) (contributo del comitato).
([37]) Relazione della FRA, pag. 67.
([38]) Relazione della FRA, pag. 67; sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.

basato sul rischio del GDPR([39]). Le autorità di protezione dei dati e il comitato dovrebbero fornire orientamenti concisi e pratici che forniscano risposte a problemi concreti e che rispecchino un equilibrio tra la protezione dei dati e altri diritti fondamentali. Gli orientamenti dovrebbero inoltre essere di facile comprensione per le persone che non hanno una formazione giuridica, ad esempio nelle PMI e nelle organizzazioni di volontariato([40]). Un modo per conseguire tale obiettivo è rendere più trasparente l'elaborazione degli orientamenti e prevedere consultazioni in una fase precoce per favorire una migliore comprensione delle dinamiche di mercato, delle pratiche commerciali e delle modalità per applicare gli orientamenti nella pratica([41]). È apprezzabile che, nell'ambito della sua strategia 2024-2027, il comitato abbia sottolineato l'obiettivo di fornire orientamenti pratici accessibili al pubblico di riferimento([42]).

I portatori di interessi sottolineano la necessità di ulteriori orientamenti, in particolare in materia di anonimizzazione e pseudonimizzazione([43]), legittimo interesse e ricerca scientifica([44]). Nella relazione del 2020 la Commissione ha invitato il comitato ad adottare orientamenti sulla ricerca scientifica, il che non è tuttavia ancora avvenuto. Riconoscendo l'importanza della ricerca scientifica nella società, in particolare per monitorare le malattie e sviluppare trattamenti, nonché per promuovere l'innovazione, è essenziale che le autorità di protezione dei dati provvedano senza ulteriori ritardi a chiarire tali questioni([45]). Anche le autorità pubbliche trarrebbero vantaggio da orientamenti che affrontino le specifiche sfide con cui si confrontano([46]).

2.5 Le autorità di protezione dei dati

2.5.1 Indipendenza e risorse

L'indipendenza delle autorità di protezione dei dati è sancita dalla Carta dei diritti fondamentali dell'Unione europea e dal trattato sul funzionamento dell'Unione europea. Il GDPR contiene prescrizioni volte a garantire la "piena indipendenza" delle autorità di protezione dei dati([47]). La relazione della FRA ha rilevato che la maggior parte delle autorità di protezione dei dati opera in maniera indipendente dal governo, dal parlamento o da qualsiasi altro organismo pubblico([48]).

Le autorità di protezione dei dati necessitano di risorse umane, tecniche e finanziarie adeguate per poter svolgere in modo efficace e indipendente i loro compiti a norma del GDPR. Nella relazione del 2020 la Commissione ha osservato che l'assegnazione di risorse alle autorità di protezione dei dati non era ancora soddisfacente e ha sistematicamente portato la questione all'attenzione degli Stati membri. Da allora la situazione è migliorata.

Maggiori risorse per le autorità di protezione dei dati([49])

- Tra il 2020 e il 2024 tutte le autorità di protezione dei dati tranne due hanno beneficiato di un aumento del personale, che ha superato il 25 % in 14 Stati membri.

([39]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([40]) Cfr. anche la posizione e le conclusioni del Consiglio, punto 45.
([41]) Cfr. anche la posizione e le conclusioni del Consiglio, punto 34.
([42]) https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf.
([43]) Cfr. anche la posizione e le conclusioni del Consiglio, punto 31, lettera d).
([44]) I portatori di interessi chiedono chiarezza, in particolare, sul significato del termine "ricerca scientifica", sul ruolo del consenso al trattamento dei dati personali per la ricerca, sulla base giuridica pertinente e sui ruoli e le responsabilità dei soggetti coinvolti.
([45]) Cfr. anche la posizione e le conclusioni del Consiglio, punto 31, lettera b).
([46]) Posizione e conclusioni del Consiglio, punti 27 e 28.
([47]) Articolo 52 del GDPR.
([48]) Relazione della FRA, pag. 31.
([49]) Cfr. il punto 4.4.1 del contributo del comitato, anche per le cifre assolute.

- L'autorità irlandese di protezione dei dati ha registrato l'aumento più elevato del personale (79 %), seguita dalle autorità estoni, svedesi (entrambe 57 %) e bulgare (56 %).
- Si è registrata una lieve riduzione del personale dell'autorità ceca (-1 %), mentre non è stato rilevato alcun aumento in Liechtenstein e gli aumenti a Cipro (4 %) e in Ungheria (8 %) sono stati di lieve entità.
- Tra il 2020 e il 2024 tutte le autorità di protezione dei dati tranne una hanno beneficiato di un aumento della propria dotazione finanziaria, che ha superato il 50 % in 13 Stati membri.
- L'autorità cipriota di protezione dei dati ha registrato l'aumento più consistente della propria dotazione finanziaria (130 %), seguita dalle autorità austriache (107 %), bulgare (100 %) ed estoni (97 %).
- La dotazione finanziaria dell'autorità greca di protezione dei dati è diminuita del 15 %, mentre le dotazioni delle autorità del Liechtenstein (1 %), della Slovacchia (6 %) e della Cechia (8 %) sono aumentate in misura modesta.

Sebbene le statistiche mostrino una generale tendenza all'aumento delle risorse a disposizione delle autorità di protezione dei dati, le stesse autorità ritengono di non disporre ancora di risorse umane sufficienti([50]). Le autorità sottolineano la necessità di conoscenze tecniche molto specialistiche, in particolare per quanto riguarda le tecnologie nuove ed emergenti([51]), la cui mancanza incide sulla quantità e sulla qualità del loro lavoro, e le difficoltà di competere con il settore privato per le risorse umane. Le autorità di protezione dei dati indicano l'insufficienza delle conoscenze giuridiche e la mancanza di competenze linguistiche come fattori che incidono sulle loro prestazioni. La bassa retribuzione, l'incapacità di selezionare autonomamente il personale e l'elevato carico di lavoro sono menzionati come fattori chiave che incidono sulla capacità delle autorità di assumere e trattenere il personale([52]). Le autorità di protezione dei dati sottolineano inoltre la necessità di risorse finanziarie per aggiornare e digitalizzare i loro processi e acquistare attrezzature tecniche([53]). Tutte le autorità di protezione dei dati svolgono compiti che vanno al di là di quelli loro affidati dal GDPR([54]), assolvendo ad esempio anche le funzioni di autorità di controllo ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie e della direttiva relativa alla vita privata e alle comunicazioni elettroniche, mentre molte di esse esprimono preoccupazione per le responsabilità aggiuntive derivanti dalla nuova normativa sul digitale([55]).

2.5.2 Difficoltà di gestione dell'elevato numero di reclami

Diverse autorità di protezione dei dati segnalano di dover destinare una quota eccessiva delle loro risorse alla gestione dell'elevato numero di reclami, la maggior parte dei quali è a loro avviso irrilevante e infondata, dato che il trattamento di ciascun reclamo è un obbligo

([50]) Solo cinque autorità di protezione dei dati ritengono di disporre di risorse umane adeguate (contributo del comitato, pag. 33).
([51]) Relazione della FRA, pag. 20. Alcune autorità di protezione dei dati affidano determinati compiti a fornitori esterni, quali la gestione dei reclami, l'analisi giuridica e l'analisi forense.
([52]) Relazione della FRA, pag. 24.
([53]) Relazione della FRA, pag. 22.
([54]) Cfr. il punto 4.4.5 del contributo del comitato.
([55]) Contributo del comitato, pag. 32.

soggetto a controllo giurisdizionale a norma del GDPR([56]). Ciò significa che le autorità di protezione dei dati non possono assegnare risorse sufficienti ad altre attività, quali indagini di propria iniziativa, campagne di sensibilizzazione del pubblico e interazioni con i responsabili del trattamento([57]). In qualità di autorità pubbliche, le autorità di protezione dei dati hanno la facoltà di assegnare le proprie risorse nel modo che esse ritengono più opportuno per lo svolgimento di ciascuno dei loro compiti (elencati all'articolo 57, paragrafo 1, del GDPR) nell'interesse del pubblico. Molte autorità di protezione dei dati hanno adottato strategie per aumentare l'efficienza della gestione dei reclami, quali l'automazione([58]), il ricorso a procedure di composizione amichevole([59]) e il "raggruppamento" dei reclami relativi a questioni simili([60]).

2.5.3 L'interpretazione del GDPR da parte delle autorità nazionali di protezione dei dati

Un obiettivo centrale del GDPR era ovviare all'approccio frammentario alla protezione dei dati dettato dalla precedente direttiva sulla protezione dei dati (direttiva 95/46/CE)([61]). Le autorità di protezione dei dati continuano tuttavia ad adottare interpretazioni divergenti di vari concetti chiave in materia di protezione dei dati([62]). I portatori di interessi ritengono che questo sia il principale ostacolo all'applicazione coerente del GDPR nell'UE. La persistenza di interpretazioni divergenti determina un'incertezza del diritto e aumenta i costi per le imprese (ad esempio a causa della necessità di produrre documenti differenti nei vari Stati membri), perturbando la libera circolazione dei dati personali nell'UE, pregiudicando le attività commerciali transfrontaliere e ostacolando la ricerca e l'innovazione in relazione a sfide sociali urgenti.

Tra le questioni specifiche sollevate dai portatori di interessi figurano: i) il fatto che le autorità di protezione dei dati in tre Stati membri abbiano ciascuna un'opinione diversa sulla base giuridica appropriata per il trattamento dei dati personali nell'ambito della sperimentazione clinica; ii) la frequente divergenza di opinioni circa il fatto che un soggetto sia titolare del trattamento o responsabile del trattamento; e iii) il fatto che in alcuni casi le autorità di protezione dei dati non seguono gli orientamenti del comitato o pubblicano orientamenti a livello nazionale in conflitto con quelli del comitato([63]). Tali questioni si aggravano quando più autorità di protezione dei dati all'interno di un unico Stato membro adottano interpretazioni contrastanti.

Alcuni portatori di interessi ritengono inoltre che alcune autorità di protezione dei dati e il comitato adottino interpretazioni che si discostano dall'approccio basato sul rischio del GDPR, il che comporta una sfida per lo sviluppo dell'economia digitale([64]) e per la libertà e la pluralità dei media. Tra le fonti di preoccupazione menzionate figurano: i) l'interpretazione dell'anonimizzazione; ii) la base giuridica del legittimo interesse e del consenso([65]); e iii) le eccezioni al divieto di un processo decisionale automatizzato relativo alle persone fisiche([66]). È opportuno ricordare che le autorità di protezione dei dati e il

([56]) Relazione della FRA, pag. 48.
([57]) Relazione della FRA, pag. 45. Le autorità di protezione dei dati considerano particolarmente importanti le indagini d'ufficio, in quanto i reclamanti potrebbero non essere a conoscenza di molte violazioni del GDPR.
([58]) Relazione della FRA, pag. 8.
([59]) Relazione della FRA, pag. 39.
([60]) Relazione della FRA, pag. 41.
([61]) Considerando 9 del GDPR.
([62]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([63]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([64]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([65]) Rispettivamente articolo 6, paragrafo 1, lettere f) e a), del GDPR.
([66]) Articolo 22, paragrafo 2, del GDPR.

comitato hanno il compito di garantire sia la protezione delle persone fisiche in relazione al trattamento dei loro dati personali sia la libera circolazione dei dati personali all'interno dell'UE. Come riconosciuto nel GDPR([67]), il diritto alla protezione dei dati di carattere personale va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità.

2.5.4 Interazioni con titolari del trattamento e responsabili del trattamento

I portatori di interessi sottolineano il vantaggio di avere l'opportunità di avviare un dialogo costruttivo con le autorità di protezione dei dati per garantire che rispettino il GDPR fin dall'inizio, in particolare per quanto riguarda le tecnologie emergenti. I portatori di interessi osservano che alcune autorità di protezione dei dati interagiscono attivamente con i titolari del trattamento, mentre altre sono lente nel rispondere, forniscono risposte vaghe o non rispondono affatto([68]).

3 L'ATTUAZIONE DEL GDPR DA PARTE DEGLI STATI MEMBRI

3.1 Frammentazionedell'applicazione a livello nazionale

Sebbene il GDPR, essendo un regolamento, sia direttamente applicabile, esso impone agli Stati membri di legiferare in determinati settori e offre loro la possibilità di precisarne ulteriormente l'applicazione in un numero limitato di ambiti([69]). Quando legiferano a livello nazionale, gli Stati membri devono farlo nel rispetto delle condizioni e dei limiti stabiliti dal GDPR. Come nel 2020, i portatori di interessi segnalano difficoltà derivanti dalla frammentazione delle norme nazionali nei settori in cui gli Stati membri hanno la possibilità di precisare l'applicazione del GDPR, in particolare per quanto riguarda:

- l'età minima per il consenso dei minori in relazione all'offerta di servizi della società dell'informazione agli stessi([70]);
- l'introduzione, da parte degli Stati membri, di ulteriori condizioni con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute([71]);
- il trattamento dei dati personali relativi a condanne penali e reati([72]), che crea difficoltà in alcuni settori regolamentati.

È importante osservare che al tempo stesso molti portatori di interessi segnalano che i problemi di frammentazione derivano principalmente da interpretazioni divergenti del GDPR da parte delle autorità di protezione dei dati, piuttosto che dall'adozione di norme di specificazione facoltative da parte degli Stati membri.

Gli Stati membri ritengono che un livello limitato di frammentazione possa essere accettabile e che le possibilità di specificazione previste dal GDPR siano comunque vantaggiose, in particolare per quanto riguarda il trattamento dei dati da parte delle autorità pubbliche([73]). Il GDPR impone agli Stati membri di consultare le rispettive autorità nazionali di protezione dei dati durante il processo di elaborazione della legislazione relativa al trattamento dei dati personali([74]). La relazione della FRA ha rilevato che alcuni

([67]) Considerando 4.
([68]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([69]) Ad esempio l'età minima per il consenso dei minori in relazione ai servizi della società dell'informazione (articolo 8, paragrafo 1, del GDPR).
([70]) Articolo 8, paragrafo 1, del GDPR.
([71]) Possibilità prevista dall'articolo 9, paragrafo 4, del GDPR.
([72]) Articolo 10 del GDPR.
([73]) Posizione e conclusioni del Consiglio, punto 30.
([74]) Articolo 36 del GDPR.

Stati hanno fissato scadenze molto strette per tali autorità e che in alcuni casi non le consultano affatto([75]).

3.2 Il monitoraggio della Commissione

La Commissione monitora costantemente l'attuazione del GDPR. Essa ha avviato procedure di infrazione nei confronti di taluni Stati membri in relazione a questioni quali l'indipendenza delle autorità di protezione dei dati (tra cui l'immunità da pressioni esterne e la disponibilità di un ricorso giurisdizionale in caso di rimozione)([76]) e il diritto degli interessati a un ricorso giurisdizionale effettivo qualora l'autorità di protezione dei dati non tratti un reclamo([77]). Nell'ambito del proprio monitoraggio, la Commissione chiede inoltre alle autorità di protezione dei dati di fornire, su base strettamente riservata, informazioni periodiche([78]) sui casi transfrontalieri di vasta portata in corso, in particolare quando riguardano grandi imprese tecnologiche multinazionali.

La Commissione comunica periodicamente con gli Stati membri in merito all'attuazione del GDPR. Come indicato nella relazione del 2020, la Commissione ha continuato ad avvalersi del gruppo di esperti degli Stati membri sul GDPR([79]) per agevolare il dibattito e la condivisione di esperienze sull'attuazione efficace del regolamento. Il gruppo di esperti ha tenuto discussioni specifiche sui temi seguenti: i) il controllo delle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali (articolo 55 del GDPR; articolo 8 della Carta); ii) la conciliazione del diritto alla protezione dei dati con il diritto alla libertà d'espressione (articolo 85 del GDPR); e iii) il diritto a un ricorso giurisdizionale effettivo nei confronti di un'autorità di controllo (articolo 78 del GDPR). A seguito di tali discussioni, la Commissione ha elaborato panoramiche degli approcci adottati per l'attuazione di tali disposizioni negli Stati membri([80]). La Commissione si è inoltre avvalsa del gruppo di esperti per uno scambio di opinioni con gli Stati membri nell'ambito dell'elaborazione della proposta relativa alle norme procedurali.

La conformità della legislazione e delle prassi nazionali alle norme sulla protezione dei dati stabilite dal diritto dell'UE sullo spazio Schengen viene esaminata anche nell'ambito delle valutazioni Schengen, condotte congiuntamente dagli Stati membri e dalla Commissione. Ogni anno vengono effettuate almeno cinque valutazioni della protezione dei dati in loco, che attualmente si concentrano sui sistemi IT su larga scala e sul sistema d'informazione Schengen, sul sistema di informazione visti e sul ruolo di controllo delle autorità nazionali di protezione dei dati su tali sistemi.

La Commissione contribuisce attivamente all'elevato numero di cause avviate dinanzi alla Corte di giustizia (con circa 30 pronunce pregiudiziali all'anno negli ultimi anni), che svolgono un ruolo centrale ai fini di un'interpretazione coerente dei concetti chiave del GDPR. Un numero crescente di pronunce della Corte fornisce diversi chiarimenti, ad esempio in merito alla definizione di dati personali([81]), alle categorie particolari di dati

([75]) Relazione della FRA, pag. 11.
([76]) Belgio (2021/4045) e Belgio (2022/2160).
([77]) Finlandia (2022/4010) e Svezia (2022/2022).
([78]) Comprese informazioni sull'identificativo di riferimento del caso e sul tipo di indagine (di propria iniziativa o basata su reclami), informazioni sintetiche sulla portata dell'indagine e informazioni sulle autorità di protezione dei dati interessate, sulle principali misure procedurali adottate e sulle relative date, sulle misure di indagine o di altro tipo adottate e sulle relative date.
([79]) https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=it&do=groupDetail.groupDetail&groupID=3461.
([80]) https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=it&meetingId=31754&fromExpertGroups=3461.
([81]) Causa C-319/22, ECLI:EU:C:2023:837.

personali([82]), al titolare del trattamento([83]), al consenso([84]), al legittimo interesse([85]), al diritto di accesso([86]), al diritto alla cancellazione([87]), al diritto al risarcimento([88]), al processo decisionale automatizzato relativo alle persone fisiche([89]), alle sanzioni amministrative pecuniarie([90]), ai responsabili della protezione dei dati([91]), alla pubblicazione dei dati personali nei registri([92]) e all'applicazione del GDPR alle attività dei parlamenti([93]).

4 I DIRITTI DEGLI INTERESSATI

Conoscenza delle persone in merito al GDPR e alle autorità di protezione dei dati (Eurobarometro 549 del 2024 su giustizia, diritti e valori)

- Il 72 % dei rispondenti in tutta l'UE dichiara di aver sentito parlare del GDPR e il 40 % sa che cos'è.
- In 19 Stati membri oltre il 70 % dei rispondenti afferma di essere a conoscenza del GDPR e il paese in cui il maggior numero di rispondenti è a conoscenza del regolamento è la Svezia (92 %), seguita da Paesi Bassi (88 %), Malta e Danimarca (84 %), mentre il paese in cui il minor numero di rispondenti è a conoscenza del regolamento è la Bulgaria (59 %), seguita da Lituania (63 %) e Francia (64 %).
- Il 68 % dei rispondenti in tutta l'UE afferma di aver sentito parlare di un'autorità nazionale responsabile della protezione dei loro diritti in materia di protezione dei dati, mentre il 24 % di tutti gli intervistati dichiara di sapere anche qual è l'autorità pubblica competente.
- In tutti gli Stati membri almeno la metà dei rispondenti ha sentito parlare di tale autorità nazionale e i livelli più elevati si registrano nei Paesi Bassi (82 %), in Cechia, Slovenia e Polonia (tutti 75 %) e in Portogallo (74 %). Austria (56 %) e Spagna (58 %) sono i paesi in cui il minor numero di rispondenti è a conoscenza di tale autorità.

Le persone sono sempre più consapevoli dei loro diritti a norma del GDPR e li esercitano attivamente([94]). Le autorità di protezione dei dati destinano ingenti risorse alla sensibilizzazione del pubblico in merito ai diritti e agli obblighi in materia di protezione dei dati, ad esempio attraverso i social media e le campagne televisive, le linee telefoniche di assistenza, le newsletter e le presentazioni negli istituti di istruzione([95]). Molte di tali iniziative hanno beneficiato di finanziamenti dell'UE([96]). L'Agenzia per i diritti

([82]) Causa C-184/20, ECLI:EU:C:2022:601; causa C-252/21, ECLI:EU:C:2023:537.
([83]) Causa C-683/21, ECLI:EU:C:2023:949; causa C-604/22, ECLI:EU:C:2024:214; causa C-231/22, ECLI:EU:C:2024:7.
([84]) Causa C-61/19, ECLI:EU:C:2020:901.
([85]) Causa C-597/19, ECLI:EU:C:2021:492; causa C-252/21, ECLI:EU:C:2023:537.
([86]) Causa C-307/22, ECLI:EU:C:2023:811; causa C-154/21, ECLI:EU:C:2023:3.
([87]) Causa C-460/20, ECLI:EU:C:2022:962.
([88]) Causa C-300/21, ECLI:EU:C:2023:370; causa C-687/21, ECLI:EU:C:2024:72; causa C-667/21, ECLI:EU:C:2023:1022.
([89]) Cause riunite C-26/22 e C-64/22, ECLI:EU:C:2023:958.
([90]) Causa C-807/21, ECLI:EU:C:2023:950; causa C-683/21, ECLI:EU:C:2023:949.
([91]) Causa C-453/21, ECLI:EU:C:2023:79.
([92]) Causa C-439/19, ECLI:EU:C:2021:504; causa C-184/20, ECLI:EU:C:2022:601.
([93]) Causa C-33/22, ECLI:EU:C:2024:46; causa C-272/19, ECLI:EU:C:2020:535.
([94]) Posizione e conclusioni del Consiglio, punto 13.
([95]) Contributo del comitato, sezione 6.
([96]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_it.

fondamentali osserva che, sebbene la consapevolezza della protezione dei dati da parte del pubblico sia aumentata, la comprensione di tale protezione è ancora carente, come dimostrato dall'elevato numero di reclami irrilevanti o infondati([97]). Per agevolare l'esercizio dei diritti da parte degli interessati sono stati sviluppati diversi strumenti digitali di facile utilizzo([98]). Atti legislativi come il regolamento sulla governance dei dati([99]) dovrebbero portare alla creazione di ulteriori modalità per consentire agli interessati di esercitare i propri diritti in futuro. Le imprese osservano che il diritto alla cancellazione viene esercitato in misura crescente, mentre il diritto di rettifica e il diritto di opposizione vengono esercitati raramente.

4.1 Il diritto di accesso

I titolari del trattamento riferiscono che il diritto di accesso (articolo 15 del GDPR) è il diritto esercitato più frequentemente dagli interessati. Sebbene il comitato abbia adottato orientamenti su tale diritto nel 2022, i titolari del trattamento continuano a segnalare difficoltà, ad esempio nell'interpretare la nozione di "richieste infondate o eccessive"([100]), nel rispondere all'elevato numero di richieste e nel gestire richieste presentate per finalità non connesse alla protezione dei dati, ad esempio allo scopo di raccogliere prove per procedimenti giudiziari([101]). Le organizzazioni della società civile osservano che spesso le risposte alle richieste di accesso vengono fornite in ritardo o sono incomplete, mentre i dati ricevuti non sono sempre in un formato leggibile([102]). Le autorità pubbliche menzionano difficoltà riguardanti l'interazione tra il diritto di accesso e le norme sull'accesso del pubblico ai documenti([103]). È pertanto positivo che nel febbraio 2024 il comitato abbia avviato un'azione congiunta sul diritto di accesso nell'ambito del quadro di applicazione coordinata([104]).

4.2 Il diritto alla portabilità

Nella relazione del 2020 la Commissione si è impegnata a esaminare mezzi pratici per favorire un maggior esercizio del diritto alla portabilità (articolo 20 del GDPR) da parte delle persone fisiche, coerentemente con la strategia per i dati. Da allora la Commissione ha adottato una serie di iniziative che integrano tale diritto. Tali iniziative agevolano il passaggio da un servizio all'altro, così da incrementare le possibilità di scelta a disposizione delle persone, favorire la concorrenza e l'innovazione e consentire alle persone di trarre vantaggi dall'uso dei loro dati. Il regolamento sui dati conferisce agli utenti di dispositivi intelligenti un diritto rafforzato alla portabilità dei dati generati attraverso tali dispositivi e impone che la progettazione del prodotto o un server di back-end del fabbricante o del titolare dei dati renda tecnicamente possibile tale portabilità. Il regolamento sui mercati digitali impone ai fornitori di servizi di piattaforma di base individuati come "gatekeeper" di garantire l'effettiva portabilità dei dati degli utenti, compreso l'accesso continuo e in tempo reale a tali dati. Diverse altre iniziative della Commissione che sono attualmente oggetto di negoziati o sulle quali è stato raggiunto un accordo politico prevedono diritti rafforzati alla portabilità in settori specifici, quali la direttiva sul lavoro mediante

([97]) Relazione della FRA, pagg. 9 e 48.
([98]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([99]) Articolo 10 del regolamento (UE) 2022/868 (regolamento sulla governance dei dati, GU L 152 del 3.6.2022, pag. 1).
([100]) Articolo 12, paragrafo 5, del GDPR.
([101]) La Corte di giustizia ha tuttavia chiarito che l'interessato non è tenuto a motivare la richiesta di accesso ai dati personali: causa C-307/22, ECLI:EU:C:2023:811, punto 38.
([102]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([103]) Posizione e conclusioni del Consiglio, punti 27 e 28.
([104]) https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access_it.

piattaforme digitali([105]), lo spazio europeo dei dati sanitari([106]) e il quadro per l'accesso ai dati finanziari([107]).

4.3 Il diritto di proporre reclamo

Come dimostrato dall'elevato numero di reclami, vi è un'ampia consapevolezza del diritto di proporre reclamo a un'autorità di protezione dei dati. Le organizzazioni della società civile segnalano differenze ingiustificate nelle prassi nazionali per il trattamento dei reclami, questione che viene affrontata dalla proposta della Commissione relativa alle norme procedurali. Pochi Stati membri si sono avvalsi della possibilità prevista dal GDPR di attribuire a un organismo senza scopo di lucro il diritto di intraprendere azioni indipendentemente dal mandato conferito dall'interessato (articolo 80, paragrafo 2). Tuttavia la direttiva relativa alle azioni rappresentative([108]), adottata nel 2020, comporterà una maggiore armonizzazione in tale ambito, agevolando le azioni collettive intraprese dalle persone fisiche per violazione del GDPR. Le misure nazionali di attuazione della direttiva sono entrate in vigore nel giugno 2023.

4.4 La protezione dei dati personali dei minori

I minori necessitano di una protezione specifica in caso di trattamento dei loro dati personali([109]). Il GDPR è parte integrante di un quadro giuridico completo che garantisce la protezione dei minori sia offline che online([110]). Dato l'aumento della presenza di minori online, negli ultimi anni sono state intraprese varie azioni a livello dell'UE e nazionale per favorire la protezione dei minori online. Le autorità di protezione dei dati hanno irrogato sanzioni pecuniarie significative alle imprese del settore dei social media per violazioni del GDPR nell'ambito del trattamento di dati di minori. Esse cooperano inoltre con altre autorità per sollecitare una maggiore protezione dei minori nel settore della pubblicità. Nella relazione del 2020 la Commissione ha invitato il comitato ad adottare orientamenti sul trattamento dei dati dei minori e tale attività è attualmente in corso([111]). Il regolamento sui servizi digitali include disposizioni specifiche volte a garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori che utilizzano le piattaforme online.

Alcuni portatori di interessi riferiscono difficoltà per quanto riguarda l'esercizio dei diritti degli interessati quando questi ultimi sono minori. In particolare, segnalano che i minori non comprendono pienamente i loro diritti, non dispongono di competenze di alfabetizzazione digitale e possono essere soggetti a influenze indebite([112]). La Commissione ha finanziato diverse iniziative a livello nazionale sulla protezione dei

([105]) Lavoratori delle piattaforme digitali: il Consiglio conferma l'accordo su nuove norme volte a migliorare le loro condizioni di lavoro | Consilium (europa.eu).
([106]) Proposta di regolamento sullo spazio europeo dei dati sanitari (COM(2022) 197 final).
([107]) Proposta di regolamento relativo a un quadro per l'accesso ai dati finanziari e che modifica i regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010, (UE) n. 1095/2010 e (UE) 2022/2554 (COM(2023) 360 final).
([108]) Direttiva (UE) 2020/1828, del 25 novembre 2020, relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE (GU L 409 del 4.12.2020, pag. 1).
([109]) Considerando 38 del GDPR.
([110]) Raccomandazione sullo sviluppo e il rafforzamento dei sistemi integrati di protezione dei minori nell'interesse superiore del minore: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/combating-violence-against-children-and-ensuring-child-protection_it.
([111]) Posizione e conclusioni del Consiglio, punto 31, lettera a).
([112]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.

dati dei minori e sulla sensibilizzazione dei minori in merito alla protezione dei dati([113]). Nell'ambito della strategia per un'internet migliore per i ragazzi (BIK+), la Commissione fornisce ai minori risorse volte a sensibilizzarli e formarli circa i loro diritti digitali, anche in relazione alla protezione dei dati (ad esempio il consenso digitale)([114]). Viene prestata sempre più attenzione alla necessità di predisporre strumenti di verifica dell'età efficaci e rispettosi della vita privata delle persone. All'inizio del 2024 la Commissione ha istituito una task force sulla verifica dell'età insieme agli Stati membri, al comitato e al gruppo dei regolatori europei per i servizi di media audiovisivi, con l'obiettivo di discutere e favorire lo sviluppo di un approccio a livello dell'UE per la verifica dell'età. Tale lavoro continuerà adesso nel quadro del comitato del regolamento sui servizi digitali, in seno al gruppo di lavoro sulla protezione dei minori. Nel contesto del regolamento sull'identità digitale europea([115]), entrato in vigore nel maggio 2024, la Commissione sta lavorando per garantire che il portafoglio europeo di identità digitale sia offerto a tutti i cittadini e i residenti dell'Unione nel 2026, anche ai fini della verifica dell'età. Nel frattempo, prima che l'ecosistema dei portafogli sia pienamente operativo, sarà sviluppata e resa disponibile in tutta l'UE una soluzione a breve termine per la verifica dell'età.

5 OPPORTUNITÀ E SFIDE PER LE ORGANIZZAZIONI, IN PARTICOLARE PER LE PMI

Il GDPR ha creato condizioni di parità per le imprese che operano nel mercato interno e il suo approccio tecnologicamente neutro e favorevole all'innovazione consente alle imprese di ridurre la burocrazia e di godere di una maggiore fiducia da parte dei consumatori([116]). Molte imprese hanno sviluppato una cultura interna della protezione dei dati e considerano il rispetto della vita privata e la protezione dei dati come parametri chiave della concorrenza. Le imprese apprezzano l'approccio basato sul rischio del GDPR in quanto principio guida che consente la flessibilità e la scalabilità dei loro obblighi([117]).

5.1 Il pacchetto di strumenti per le imprese

Il GDPR fornisce un pacchetto di strumenti che consentono alle organizzazioni di gestire in modo flessibile e dimostrare la loro conformità, compresi codici di condotta, meccanismi di certificazione e clausole contrattuali tipo. Come anticipato nella relazione del 2020, nel 2021 la Commissione ha adottato clausole contrattuali tipo sul rapporto tra titolare del trattamento e responsabile del trattamento([118]). Tali clausole contrattuali tipo forniscono uno strumento volontario di conformità pronto all'uso e di facile attuazione, che è particolarmente utile per le PMI o le organizzazioni che potrebbero non disporre delle risorse per negoziare contratti individuali con i loro partner commerciali. Le imprese

([113]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_it.

([114]) https://digital-strategy.ec.europa.eu/it/policies/strategy-better-internet-kids.

([115]) Regolamento (UE) 2024/1183 che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale (GU L, 2024/1183, 30.4.2024).

([116]) Come riconosciuto dalla relazione della piattaforma "Fit for future", un gruppo di esperti ad alto livello istituito per sostenere gli sforzi della Commissione volti a semplificare la normativa dell'UE e ridurre i relativi costi superflui: https://commission.europa.eu/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-less-costly-and-future-proof/fit-future-platform-f4f_it. Cfr. anche la sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR e la posizione e le conclusioni del Consiglio, punto 12.

([117]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.

([118]) Decisione di esecuzione (UE) 2021/915 della Commissione, del 4 giugno 2021, relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio (C/2021/3701 – GU L 199 del 7.6.2021, pag. 18).

segnalano riscontri contrastanti sull'uso delle clausole contrattuali tipo, nel senso che alcune imprese (principalmente PMI) le utilizzano in tutto o in parte, mentre altre (per lo più imprese di maggiori dimensioni) tendono a non utilizzarle perché preferiscono ricorrere alle proprie clausole.

Le imprese sottolineano che i codici di condotta hanno grandi potenzialità in qualità di strumento di conformità settoriale ed efficace sotto il profilo dei costi([119]). Tuttavia l'elaborazione di codici di condotta è limitata([120]). In base alle informazioni finora disponibili, a livello dell'UE sono stati approvati solo due codici (entrambi nel settore del cloud), mentre a livello nazionale sono stati approvati sei codici([121]). I portatori di interessi segnalano prescrizioni gravose (tra cui la necessità di istituire un organismo di monitoraggio accreditato), la mancanza di impegno da parte delle autorità di protezione dei dati e un processo di approvazione lungo quali fattori principali che limitano l'adozione di codici di condotta([122]).

Occorrono una maggiore trasparenza del processo e tempistiche chiare per l'approvazione. Le autorità di protezione dei dati e, nel caso dei codici a livello dell'UE, il comitato dovrebbero incoraggiare più attivamente l'elaborazione di codici di condotta collaborando con le associazioni che li sviluppano. Ciò contribuirà a eliminare le divergenze di interpretazione e ad accelerare il processo di approvazione. I portatori di interessi lamentano i considerevoli ritardi nell'adozione dei codici di condotta, causati da questioni discusse parallelamente nell'ambito dei lavori sugli orientamenti. Analogamente, le imprese riferiscono che non viene fatto ampio uso della certificazione in quanto il processo di sviluppo è lento e complesso. Come per i codici di condotta, le autorità di protezione dei dati dovrebbero stabilire tempistiche più chiare per il riesame e l'approvazione delle certificazioni.

Nella sua strategia 2024-2027 il comitato si è impegnato a continuare a sostenere misure di conformità quali la certificazione e i codici di condotta, anche dialogando con gruppi chiave di portatori di interessi per illustrare in che modo possono essere utilizzati gli strumenti([123]).

5.2 Sfide specifiche per le PMI e i piccoli operatori

Nella relazione del 2020 la Commissione ha invitato a intensificare gli sforzi volti a favorire la conformità delle PMI al GDPR. Negli ultimi anni le autorità di protezione dei dati e il comitato hanno continuato a sviluppare strumenti di conformità per le PMI, sostenuti in parte da finanziamenti della Commissione([124]). Nell'aprile 2023 il comitato ha pubblicato una guida alla protezione dei dati per le piccole imprese([125]), che fornisce alle PMI informazioni pratiche in un formato accessibile e facilmente comprensibile.

In molti Stati membri le PMI sottolineano i vantaggi di un sostegno su misura da parte delle loro autorità locali di protezione dei dati. Tuttavia, alla luce della diversità degli approcci alla sensibilizzazione e all'orientamento adottati dalle autorità di protezione dei dati, in alcuni Stati membri le PMI percepiscono la conformità come una questione

([119]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([120]) Posizione e conclusioni del Consiglio, punto 25.
([121]) https://www.edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_it?f%5B0%5D=coc_scope%3Anational.
([122]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([123]) https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf.
([124]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_it.
([125]) https://edpb.europa.eu/sme-data-protection-guide/home_en.

complessa e temono di essere oggetto di misure di applicazione delle norme([126]). Le autorità di protezione dei dati dovrebbero raddoppiare gli sforzi volti ad affrontare tali sfide, anche dialogando proattivamente con le PMI per dissipare eventuali preoccupazioni infondate in materia di conformità. Le autorità di protezione dei dati dovrebbero concentrarsi sul fornire un sostegno su misura e strumenti pratici, quali modelli (ad esempio per l'esecuzione di valutazioni d'impatto sulla protezione dei dati), linee telefoniche di assistenza, esempi illustrativi, liste di controllo e orientamenti su specifiche operazioni di trattamento (ad esempio la fatturazione o l'invio di newsletter), nonché misure tecniche e organizzative. Poiché la maggior parte delle PMI non dispone al proprio interno di competenze in materia di protezione dei dati, qualsiasi orientamento rivolto alle PMI dovrebbe essere di facile comprensione per persone che non hanno una formazione giuridica([127]).

In linea con l'approccio basato sul rischio del GDPR, le PMI che svolgono attività di trattamento a basso rischio non sono soggette a un onere di conformità sostanziale. Sebbene la deroga all'obbligo di tenere registri delle attività di trattamento([128]) si applichi in circostanze limitate([129]), le PMI che effettuano operazioni di trattamento a basso rischio possono conformarsi conservando registri semplificati basati su modelli forniti dalle autorità di protezione dei dati. Tali registri dovrebbero essere inoltre considerati dalle PMI uno strumento utile per fare il punto delle loro attività di trattamento.

5.3 I responsabili della protezione dei dati

I responsabili della protezione dei dati svolgono un ruolo importante nel garantire il rispetto del GDPR in seno alle organizzazioni in cui operano. In generale, i responsabili della protezione dei dati che operano nell'UE dispongono delle conoscenze e delle competenze necessarie per svolgere i loro compiti a norma del GDPR e la loro indipendenza viene rispettata([130]). Persistono tuttavia diverse sfide, tra cui: i) difficoltà nel nominare responsabili della protezione dei dati dotati delle competenze necessarie; ii) la mancanza di norme a livello dell'UE per quanto riguarda l'istruzione e la formazione; iii) l'integrazione non adeguata dei responsabili della protezione dei dati nei processi organizzativi; iv) la mancanza di risorse; v) i compiti aggiuntivi che esulano dalla protezione dei dati; e vi) l'insufficiente anzianità di servizio([131]). Il comitato ha osservato che è necessario che le autorità di protezione dei dati intensifichino le attività di sensibilizzazione, nonché le loro misure di informazione e di applicazione delle norme per garantire che i responsabili della protezione dei dati possano svolgere il loro ruolo a norma del GDPR([132]).

([126]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([127]) Cfr. la posizione e le conclusioni del Consiglio, punto 24, e la sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([128]) Articolo 30, paragrafo 5, del GDPR.
([129]) Se l'organizzazione ha meno di 250 dipendenti, fatti salvi i casi in cui il trattamento effettuato possa comportare un rischio per i diritti e le libertà degli interessati, non sia occasionale oppure includa categorie particolari di dati di cui all'articolo 9, paragrafo 1, del GDPR o dati personali relativi a condanne penali e a reati di cui all'articolo 10 del GDPR.
([130]) Posizione e conclusioni del Consiglio, punto 26; documento "EDPB 2023 Coordinated Enforcement Action – Designation and Position of Data Protection Officers": https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf.
([131]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([132]) Cfr. le raccomandazioni contenute nel documento "EDPB Coordinated Enforcement Action".

6 IL GDPR QUALE PIETRA ANGOLARE DELLA POLITICA DELL'UE NEL SETTORE DIGITALE

6.1 Una politica sul digitale basata sul GDPR

Nella relazione del 2020 la Commissione si è impegnata a sostenere un'applicazione coerente del quadro per la protezione dei dati in relazione alle nuove tecnologie in maniera da fornire sostegno all'innovazione e agli sviluppi tecnologici. Da allora l'UE ha adottato una serie di iniziative, alcune delle quali integrano il GDPR o specificano le relative modalità di applicazione in determinati settori al fine di perseguire specifici obiettivi, come illustrato di seguito.

- Il regolamento sui servizi digitali([133]), che mira a garantire un ambiente online sicuro per le persone e le imprese, vieta alle piattaforme online di mostrare pubblicità basate sulla profilazione utilizzando le "categorie particolari di dati personali" definite nel GDPR.
- Per rendere i mercati digitali più equi e contendibili, il regolamento sui mercati digitali([134]) vieta agli operatori designati come "gatekeeper" di "combinare" e "utilizzare in modo incrociato" i dati personali tra i loro servizi di piattaforma di base e altri servizi, fatto salvo il caso in cui l'utente abbia fornito il proprio consenso ai sensi del GDPR.
- Il regolamento sull'IA ([135]) precisa le norme dell'UE in materia di protezione dei dati in settori specifici in cui viene utilizzata l'intelligenza artificiale, ad esempio in relazione ai sistemi di identificazione biometrica remota, al trattamento di categorie particolari di dati per rilevare distorsioni e all'ulteriore trattamento dei dati personali negli spazi di sperimentazione normativa.
- La direttiva sul lavoro mediante piattaforme digitali([136]) integra il GDPR nel settore dell'occupazione stabilendo norme sui sistemi decisionali e di monitoraggio automatizzati utilizzati dalle piattaforme di lavoro digitali, in particolare per quanto riguarda le limitazioni al trattamento dei dati personali, la trasparenza, la sorveglianza umana, il riesame e la portabilità.
- Il regolamento sulla pubblicità politica ([137]) vieta di utilizzare categorie particolari di dati personali nella pubblicità politica e richiede una maggiore trasparenza in merito alle tecniche di targeting e amplificazione utilizzate.
- Il regolamento sull'identità digitale europea consente la creazione di un portafoglio europeo di identità digitale universale, affidabile e sicuro. Ciò consentirà alle persone di dimostrare attributi personali, come età, patenti di guida, diplomi e conti bancari, mantenendo il pieno controllo dei loro dati personali e senza inutili condivisioni di dati.

([133]) Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) (GU L 277 del 27.10.2022, pag. 1).

([134]) Regolamento (UE) 2022/1925 (regolamento sui mercati digitali, GU L 265 del 12.10.2022, pag. 1).

([135]) Regolamento (UE) 2024/1689 (regolamento sull'intelligenza artificiale), GU L, 2024/1689, 12.7.2024).

([136]) Lavoratori delle piattaforme digitali: il Consiglio conferma l'accordo su nuove norme volte a migliorare le loro condizioni di lavoro | Consilium (europa.eu).

([137]) Regolamento (UE) 2024/900 relativo alla trasparenza e al targeting della pubblicità politica (GU L, 2024/900, 20.3.2024).

La proposta di regolamento sulla vita privata e le comunicazioni elettroniche([138]), volta a sostituire l'attuale direttiva relativa alla vita privata e alle comunicazioni elettroniche([139]) e a integrare il quadro legislativo in materia di rispetto della vita privata e protezione dei dati, è oggetto di negoziati che si protraggono ormai da diversi anni. È necessaria una riflessione sulle prossime tappe di questa iniziativa, nonché sulla sua relazione con il GDPR.

Il regolamento su un'Europa interoperabile([140]) mira a rendere interoperabili in tutta l'UE i servizi pubblici digitali. Esso sostiene la cooperazione tra le autorità di protezione dei dati, in particolare attraverso spazi di sperimentazione normativa per l'interoperabilità.

Diverse iniziative dell'UE forniscono una base giuridica per il trattamento dei dati personali da parte di soggetti privati a fini di prevenzione, indagine, accertamento e perseguimento di reati. Qualsiasi normativa di questo tipo deve essere orientata con precisione in modo da ridurre al minimo le interferenze con il diritto alla protezione dei dati personali e deve essere proporzionata all'obiettivo perseguito([141]). La Carta, il GDPR e la giurisprudenza della Corte di giustizia forniscono un quadro rispetto al quale dovrebbero essere misurate dette iniziative. Il pacchetto antiriciclaggio proposto([142]) include garanzie sostanziali per la protezione dei dati personali, senza compromettere l'obiettivo di attenuare i rischi di riciclaggio e di finanziamento del terrorismo e di individuare efficacemente i tentativi criminosi di abusare del sistema finanziario dell'UE.

In tale contesto, il Consiglio ha sottolineato che qualsiasi nuova normativa dell'UE contenente disposizioni sul trattamento dei dati personali dovrebbe essere coerente con il GDPR e con la giurisprudenza della Corte di giustizia.

6.2 Un quadro giuridico volto a migliorare la condivisione dei dati

La strategia per i dati mira a creare un mercato unico dei dati in cui i dati possano circolare liberamente all'interno dell'UE e tra i vari settori a vantaggio delle imprese, dei ricercatori e delle pubbliche amministrazioni. Un obiettivo fondamentale della strategia per i dati è la creazione di spazi comuni europei di dati che agevolino la messa in comune, l'accesso e la condivisione dei dati. Per quanto riguarda i dati personali, il GDPR fornisce il quadro per tutte le iniziative volte a potenziare la libera circolazione dei dati nell'UE, che è a sua volta un obiettivo del regolamento. Per quanto riguarda i dati personali, le tutele del GDPR non vengono intaccate.

Il regolamento sulla governance dei dati([143]) e il regolamento sui dati([144]) sono pilastri della strategia per i dati. Il regolamento sulla governance dei dati stabilisce norme concrete sul riutilizzo dei dati del settore pubblico contenenti dati personali e predispone un quadro legislativo per i servizi di intermediazione dei dati, compresi i servizi di gestione di informazioni personali o i cloud di dati personali offerti al fine di consentire agli interessati di esercitare i loro diritti a norma del GDPR. Definisce inoltre le condizioni quadro per l'utilizzo dei dati a fini altruistici. Il regolamento sui dati rafforza il controllo degli interessati sui dati generati attraverso l'uso di oggetti intelligenti da loro posseduti, presi in locazione o noleggiati, stabilendo requisiti tecnici per l'accesso ai dati e la loro portabilità.

([138]) Proposta di regolamento sulla vita privata e le comunicazioni elettroniche (COM(2017) 10 final).
([139]) Direttiva 2002/58/CE (direttiva relativa alla vita privata e alle comunicazioni elettroniche, GU L 201 del 31.7.2002, pag. 37).
([140]) Regolamento (UE) 2024/903 (regolamento su un'Europa interoperabile, GU L, 2024/903, 22.3.2024).
([141]) Cfr. la posizione e le conclusioni del Consiglio, punto 31, lettera f).
([142]) https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_it.
([143]) Regolamento (UE) 2022/868 (regolamento sulla governance dei dati, GU L 152 del 3.6.2022, pag. 1).
([144]) Regolamento (UE) 2023/2854 (regolamento sui dati, GU L, 2023/2854, 22.12.2023).

Lo spazio europeo dei dati sanitari([145]) riflette le esigenze specifiche individuate nel settore dei dati sanitari, basandosi nel contempo anche sul GDPR. Consente alle persone di accedere facilmente ai propri dati sanitari in formato elettronico e di condividerli con gli operatori sanitari, anche in altri Stati membri, migliorando in tal modo l'erogazione dell'assistenza sanitaria e aumentando il controllo dei pazienti sui loro dati. Predispone inoltre un quadro giuridico comune per il riutilizzo dei dati sanitari per finalità quali la ricerca, l'innovazione e la salute pubblica, sulla base di un'autorizzazione rilasciata da un organismo responsabile dell'accesso ai dati sanitari. Per garantire la protezione dei dati personali, lo spazio europeo dei dati sanitari offrirà un contesto affidabile per l'accesso sicuro ai dati sanitari e per il loro trattamento. La Commissione continua a sostenere il lavoro sullo sviluppo di spazi comuni europei di dati in 14 settori attuando il nuovo quadro legislativo e finanziando iniziative settoriali.

6.3 La governance delle nuove norme sul digitale

Lo sviluppo di normative sul digitale fa sorgere la necessità di una stretta cooperazione in tutti i settori normativi([146]). Tale cooperazione è tanto più necessaria in quanto le questioni relative alla protezione dei dati si intersecano sempre più con le questioni relative, ad esempio, al diritto della concorrenza, al diritto dei consumatori, alle norme sui mercati digitali, alla regolamentazione delle comunicazioni elettroniche e alla cibersicurezza. Ciò avviene ad esempio nel caso della valutazione della compatibilità dei modelli "*pay or OK*" ("dai il consenso o paga") con il diritto dell'UE.

In alcuni casi le autorità di protezione dei dati sono incaricate di applicare disposizioni specifiche della nuova normativa dell'UE sul digitale([147]). I nuovi regolamenti sul digitale creano inoltre strutture su misura che riuniscono le autorità di regolamentazione competenti per garantire un'applicazione coerente, come il gruppo ad alto livello del regolamento sui mercati digitali, il comitato europeo per l'innovazione in materia di dati (istituito a norma del regolamento sulla governance dei dati) e il comitato europeo per i servizi digitali (istituito a norma del regolamento sui servizi digitali). La direttiva NIS 2([148]) stabilisce norme più dettagliate sulla cooperazione tra le autorità di regolamentazione e le autorità di protezione dei dati per quanto riguarda la gestione degli incidenti di sicurezza che comportano violazioni di dati personali.

Al di fuori di dette strutture formali, le autorità di protezione dei dati stanno adottando misure volte a garantire che le loro azioni siano complementari e coerenti con altri settori normativi. Nel luglio 2020 le autorità preposte alla tutela dei consumatori e alla protezione dei dati hanno istituito un "gruppo di volontari" allo scopo di individuare le migliori pratiche e condividere le proprie esperienze in materia di applicazione delle norme. Le autorità di protezione dei dati continuano a partecipare a seminari congiunti con la rete di cooperazione per la tutela dei consumatori. Nel 2023 il comitato ha istituito una task force sull'interazione tra protezione dei dati, concorrenza e tutela dei consumatori.

Sebbene tali sviluppi siano positivi, sussiste la necessità di creare strumenti di cooperazione più strutturati ed efficienti, in particolare per affrontare situazioni che interessano un vasto numero di persone nell'UE e coinvolgono diverse autorità di regolamentazione([149]). Tali strutture dovrebbero garantire che le autorità rimangano

([145]) https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_IT.html.

([146]) Cfr. la posizione e le conclusioni del Consiglio, punti 40 e 41, e la sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.

([147]) Cfr. ad esempio l'articolo 37, paragrafo 3, del regolamento sui dati.

([148]) Direttiva (UE) 2022/2555 (direttiva NIS 2, GU L 333 del 27.12.2022, pag. 80).

([149]) Cfr. la posizione e le conclusioni del Consiglio, punti 18, 40 e 41, e la sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.

sempre responsabili di tutte le questioni relative al rispetto delle norme nei rispettivi settori di competenza. Gli Stati membri dovrebbero inoltre adoperarsi per garantire un'adeguata cooperazione a livello nazionale([150]).

7 I TRASFERIMENTI INTERNAZIONALI E LA COOPERAZIONE GLOBALE

7.1 Il pacchetto di strumenti di trasferimento del GDPR

I flussi di dati sono diventati parte integrante della trasformazione digitale della società e della globalizzazione dell'economia. Più che mai, il rispetto della vita privata è una condizione per flussi commerciali stabili, sicuri e competitivi, nonché un fattore abilitante per molte forme di cooperazione internazionale. Il capo V del GDPR predispone un pacchetto di strumenti per gestire i trasferimenti in vari scenari differenti, garantendo nel contempo che i dati continuino a beneficiare di un elevato livello di protezione quando escono dall'UE.

Da quando è stata elaborata la relazione del 2020 le prescrizioni relative ai trasferimenti di dati contenute nella normativa dell'UE in materia di protezione dei dati sono state ulteriormente chiarite e il pacchetto di strumenti di trasferimento ha continuato a evolversi. Un importante chiarimento riguarda la nozione di "trasferimento internazionale", che è stata definita dal comitato([151]) come comprendente qualsiasi comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento il cui trattamento è soggetto al GDPR a un altro titolare del trattamento o responsabile del trattamento in un paese terzo, a prescindere dal fatto che il trattamento da parte di quest'ultimo sia o meno soggetto al GDPR([152]). Tali orientamenti del comitato sono stati particolarmente importanti per garantire la certezza del diritto ai titolari del trattamento e ai responsabili del trattamento europei in relazione agli scenari in cui è necessario uno strumento di trasferimento a norma del capo V del GDPR.

Ulteriori chiarimenti sono stati forniti dalla Corte di giustizia nella sentenza *Schrems II*([153]) sulla protezione che deve essere garantita da diversi strumenti di trasferimento per garantire che il livello di protezione assicurato dal GDPR non venga compromesso([154]). In particolare, tali strumenti devono garantire che alle persone i cui dati vengono trasferiti al di fuori dell'UE sia riconosciuto un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE([155]). È responsabilità dell'esportatore di dati dell'UE valutare se ciò si verifichi, tenendo conto delle circostanze specifiche dei suoi trasferimenti([156]).

Per valutare il livello di protezione, gli esportatori di dati devono prendere in considerazione sia le garanzie in materia di protezione dei dati previste dallo strumento di trasferimento concluso con un importatore di dati di un paese terzo (ad esempio un contratto), sia gli aspetti pertinenti dell'ordinamento giuridico del paese in cui si trova l'importatore, in particolare per quanto riguarda l'eventuale accesso ai dati da parte delle autorità pubbliche di tale paese([157]). Questi ultimi devono essere valutati alla luce dei criteri

([150]) La Germania ha istituito un "cluster digitale", che comprende autorità di regolamentazione di vari settori, con l'obiettivo di ampliare la loro cooperazione su tutti gli aspetti della digitalizzazione e condividere conoscenze e migliori pratiche: https://www.dataguidance.com/news/germany-bsi-announces-formation-digital-cluster-bonn.
([151]) Linee guida 05/2021 dell'EDPB.
([152]) Sezione 2 delle linee guida 05/2021 dell'EDPB.
([153]) Causa C-311/18, ECLI:EU:C:2020:559 (*Schrems II*).
([154]) *Schrems II*, punto 93.
([155]) *Schrems II*, punti 96 e 105.
([156]) *Schrems II*, punto 131.
([157]) *Schrems II*, punto 105.

per le valutazioni di adeguatezza di cui all'articolo 45 del GDPR. La Corte ha inoltre approfondito ulteriormente tali criteri, in particolare in relazione alle norme sull'accesso ai dati personali da parte delle autorità pubbliche a fini di contrasto e di sicurezza nazionale.

Tale interpretazione è stata integrata anche negli orientamenti del comitato, che ha aggiornato i propri "criteri di riferimento per l'adeguatezza"([158]) che hanno fornito orientamenti sugli elementi di cui la Commissione deve tenere conto quando effettua una valutazione dell'adeguatezza) Il comitato ha inoltre adottato nuovi orientamenti che forniscono ulteriori chiarimenti per quanto riguarda: i) gli elementi che i singoli esportatori di dati devono prendere in considerazione nel valutare il livello di protezione; ii) una panoramica delle potenziali fonti che possono essere utilizzate; e iii) esempi di possibili misure supplementari (ad esempio garanzie contrattuali e tecniche)([159]). Gli orientamenti sottolineano nello specifico che ogni valutazione effettuata dagli esportatori di dati è a sé stante e che essi devono pertanto tenere conto delle caratteristiche specifiche di ciascun trasferimento, le quali possono variare a seconda della finalità del trasferimento di dati, dei tipi di soggetti coinvolti, del settore in cui avviene il trasferimento, delle categorie di dati personali trasferiti ecc. ([160]).

Tenendo conto dei diversi chiarimenti riguardanti le prescrizioni in materia di trasferimenti internazionali di dati, negli ultimi anni sono stati compiuti passi significativi per sviluppare ulteriormente il pacchetto di strumenti di trasferimento del GDPR e per renderli operativi.

7.1.1 Le decisioni di adeguatezza

Come emerge anche dai riscontri forniti dai portatori di interessi, le decisioni di adeguatezza continuano a svolgere un ruolo chiave nel pacchetto di strumenti di trasferimento del GDPR([161]), fornendo una soluzione semplice e completa per i trasferimenti di dati senza la necessità che l'esportatore fornisca ulteriori garanzie o ottenga alcuna autorizzazione. Consentendo la libera circolazione dei dati personali, tali decisioni hanno aperto canali commerciali agli operatori dell'UE, integrando e ampliando tra l'altro i vantaggi degli accordi commerciali, e hanno favorito la collaborazione con partner stranieri in un ampio ventaglio di settori, dalla cooperazione normativa alla ricerca.

Da quando è stata elaborata la relazione del 2020 è cresciuto costantemente il numero dei paesi che hanno emanato leggi moderne in materia di protezione dei dati, che disciplinano tra l'altro i principi fondamentali della protezione dei dati, i diritti individuali e l'efficace applicazione delle norme da parte di autorità di regolamentazione indipendenti. Tale tendenza([162]) ha inoltre consentito alla Commissione di intensificare il proprio lavoro in materia di adeguatezza. Ciò comprende l'adozione di una decisione di adeguatezza relativa al Regno Unito([163]), che è fondamentale per garantire il corretto funzionamento dei vari accordi conclusi con il Regno Unito a seguito della Brexit. Per garantire la sua costante adeguatezza alle esigenze future, la decisione di adeguatezza comprende una "clausola di temporaneità" che fissa al 2025 la scadenza della decisione, la quale potrà essere prorogata se il livello di protezione continuerà a essere adeguato. La Commissione ha inoltre adottato una decisione di adeguatezza relativa alla Repubblica di Corea([164]), che integra l'accordo di libero scambio UE-Corea per quanto riguarda i flussi di dati personali e facilita la

([158]) Raccomandazioni 2/2020 dell'EDPB e criteri di riferimento per l'adeguatezza, WP 254 rev. 01.
([159]) Raccomandazioni 1/2020 dell'EDPB, integrate dalle raccomandazioni 2/2020.
([160]) Cfr. ad esempio i punti da 8 a 13 e i punti 32 e 33 delle raccomandazioni 1/2020 dell'EDPB.
([161]) Cfr. ad esempio il contributo del comitato, pagg. 7 e 8, la posizione e le conclusioni del Consiglio, punto 36, e la sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([162]) Comunicazione della Commissione "Scambio e protezione dei dati personali in un mondo globalizzato" (COM(2017) 7 final del 10.1.2017).
([163]) Decisione di esecuzione (UE) 2021/1772 della Commissione (GU L 360 del 11.10.2021, pag. 1).
([164]) Decisione di esecuzione (UE) 2022/254 della Commissione (GU L 44 del 24.2.2022, pag. 1).

cooperazione normativa. Un primo riesame della decisione di adeguatezza è previsto verso la fine del 2024.

A seguito dell'annullamento della decisione di adeguatezza sullo scudo UE-USA per la privacy, la Commissione ha inoltre avviato colloqui con il governo degli Stati Uniti per elaborare un ulteriore accordo che rispetti le prescrizioni su cui la Corte ha fatto chiarezza([165]). Il presidente degli Stati Uniti ha adottato un nuovo provvedimento esecutivo sul rafforzamento delle garanzie per le attività statunitensi di intelligence dei segnali, che ha introdotto nuove garanzie vincolanti e azionabili per assicurare che sia possibile accedere ai dati a fini di sicurezza nazionale solo nella misura necessaria e proporzionata, e che i cittadini europei dispongano di mezzi di ricorso efficaci. Alla luce di ciò, la Commissione ha adottato la decisione di adeguatezza relativa al quadro UE-USA per la protezione dei dati([166]), che consente la libera circolazione dei dati personali dall'UE alle imprese statunitensi che aderiscono a detto quadro. Poiché le garanzie predisposte dal governo degli Stati Uniti nel settore della sicurezza nazionale si applicano a tutti i trasferimenti di dati verso imprese negli Stati Uniti, a prescindere dal meccanismo di trasferimento del GDPR utilizzato, l'uso di altri strumenti, quali le clausole contrattuali tipo e le norme vincolanti d'impresa, è stato notevolmente agevolato. Un primo riesame del funzionamento del quadro UE-USA per la protezione dei dati avrà luogo durante l'estate del 2024 e verificherà che tutti gli elementi pertinenti siano stati pienamente attuati nel quadro giuridico statunitense e funzionino efficacemente nella pratica.

Sono attualmente in corso negoziati sull'adeguatezza con il Brasile e il Kenya e, per la prima volta, con diverse organizzazioni internazionali (ad esempio, i colloqui sull'adeguatezza con l'Organizzazione europea dei brevetti si trovano in una fase avanzata)([167]). In linea anche con le richieste di vari portatori di interessi([168]), la Commissione ha partecipato attivamente a colloqui esplorativi con paesi di diverse regioni del mondo.

La Commissione controlla inoltre in maniera costante gli sviluppi nei paesi che già beneficiano di accertamenti dell'adeguatezza e riesamina periodicamente le decisioni vigenti, in ottemperanza ai suoi obblighi pertinenti a norma del GDPR([169]). Nell'aprile 2023 la Commissione ha adottato la relazione sul primo riesame periodico della decisione di adeguatezza relativa al Giappone([170]), in cui ha concluso che il Giappone continua a garantire un livello di protezione adeguato([171]). Il riesame ha dimostrato che, dall'adozione delle decisioni di adeguatezza reciproca, i quadri in materia di protezione dei dati di UE e Giappone si sono ulteriormente ravvicinati.

Inoltre, conformemente all'articolo 97 del GDPR, nell'ambito della valutazione 2020 dell'applicazione e del funzionamento del regolamento è stato avviato il primo riesame

([165]) https://commission.europa.eu/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-2020-08-10_it.

([166]) Decisione di esecuzione (UE) 2023/1795 della Commissione (GU L 231 del 20.9.2023, pag. 118).

([167]) L'Organizzazione europea dei brevetti è un'organizzazione intergovernativa istituita sulla base della convenzione sul brevetto europeo. Il suo compito principale è la concessione di brevetti europei. In tale contesto, collabora strettamente con imprese e autorità pubbliche degli Stati membri dell'UE, nonché con diverse istituzioni e diversi organi dell'Unione.

([168]) Contributo del comitato, pagg. 7 e 8.

([169]) Articolo 45, paragrafi 4 e 5, del GDPR. Cfr. anche *Schrems I*, punto 76.

([170]) Decisione di esecuzione (UE) 2019/419 della Commissione (GU L 76 del 19.3.2019, pag. 1). Cfr. anche https://ec.europa.eu/commission/presscorner/detail/it/IP_19_421. Tale decisione ha costituito la prima decisione di adeguatezza adottata a norma del GDPR e il primo accordo di adeguatezza reciproca.

([171]) Relazione della Commissione sul primo riesame del funzionamento della decisione di adeguatezza relativa al Giappone (COM(2023) 275 final e SWD(2023) 75 final del 3.4.2023).

delle 11 decisioni di adeguatezza([172]) adottate a norma del precedente quadro dell'UE in materia di protezione dei dati (la direttiva sulla protezione dei dati). La conclusione di questo aspetto del riesame è stata rinviata, in particolare per tenere conto della sentenza della Corte di giustizia nella causa *Schrems II* e della successiva interpretazione del comitato. I chiarimenti della Corte sopra menzionati riguardo agli elementi chiave del livello di adeguatezza hanno portato a scambi approfonditi con i paesi e territori interessati in merito ad aspetti pertinenti dei loro quadri giuridici e dei loro meccanismi di vigilanza e applicazione delle norme.

Il 15 gennaio 2024 la Commissione ha pubblicato la relazione sulle suddette 11 decisioni, unitamente ad altre dettagliate relazioni che descrivono gli sviluppi verificatisi in ciascuno dei paesi e territori dall'adozione delle decisioni di adeguatezza, nonché le norme che si applicano all'accesso ai dati da parte delle autorità pubbliche, in particolare a fini di contrasto e di sicurezza nazionale([173]). La relazione conclude che tutti gli 11 paesi e territori continuano a garantire un livello adeguato di protezione dei dati personali trasferiti dall'UE. Essa constata che tutti i paesi e territori interessati hanno aggiornato e rafforzato in modi diversi il rispettivo quadro giuridico in materia di tutela della vita privata. Inoltre, per superare le differenze nel livello di protezione, con alcuni di essi sono state negoziate e concordate ulteriori garanzie per i dati personali trasferiti dall'Europa, qualora necessario per assicurare la continuità della decisione di adeguatezza.

Detti riesami dimostrano inoltre che le decisioni di adeguatezza, anziché rappresentare un "punto finale", hanno gettato le basi per una più stretta cooperazione e un'ulteriore convergenza normativa tra l'UE e i partner che condividono gli stessi principi. Ad esempio, la relazione sul primo riesame della decisione di adeguatezza relativa al Giappone riconosce che l'ulteriore rafforzamento del quadro giapponese in materia di protezione dei dati può aprire la strada a un'estensione della decisione di adeguatezza al di là degli scambi commerciali, al fine di inserirvi i trasferimenti attualmente esclusi dal suo ambito di applicazione, ad esempio nel settore della cooperazione normativa e della ricerca. Sono attualmente in corso colloqui per valutare tale possibile estensione. In generale, le decisioni di adeguatezza sono divenute una componente strategica delle relazioni complessive dell'UE con questi partner stranieri e sono riconosciute come un importante fattore che consente di approfondire la cooperazione in un'ampia gamma di settori.

Oltre a fornire una solida base per una maggiore cooperazione bilaterale, la crescente rete di paesi e territori oggetto di decisioni di adeguatezza dell'UE offre nuove opportunità per massimizzare i benefici di una circolazione dei dati sicura e libera e per cooperare più strettamente con partner che condividono gli stessi principi per quanto riguarda l'applicazione delle norme in materia di protezione dei dati. Nel marzo 2024 la Commissione ha pertanto ospitato la prima riunione ad alto livello su una circolazione dei dati sicura, cui hanno partecipato i ministri competenti e le figure apicali delle autorità di protezione dei dati di 15 paesi e territori oggetto di decisioni di adeguatezza dell'UE, nonché il presidente del comitato europeo per la protezione dei dati([174]). Nel corso della riunione sono stati individuati diversi ambiti d'azione concreti, che sono attualmente oggetto di attività di follow-up in seno al gruppo.

Più in generale, grazie al loro "effetto rete" le decisioni di adeguatezza adottate dalla Commissione europea acquistano rilevanza sempre maggiore anche al di fuori dell'UE,

([172]) Andorra, Argentina, Canada (per gli operatori commerciali), Isole Fær Øer, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera e Uruguay.

([173]) Relazione della Commissione sul primo riesame del funzionamento delle decisioni di adeguatezza adottate a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE (COM(2024) 7 final e SWD(2024) 3 final del 15.1.2024).

([174]) https://ec.europa.eu/commission/presscorner/detail/it/mex_24_1307#11.

poiché consentono la libera circolazione dei dati non solo con le 30 economie del SEE, ma anche con molti altri Stati del mondo che riconoscono i paesi oggetto di decisioni di adeguatezza dell'UE come "destinazioni sicure" ai sensi delle proprie norme di protezione dei dati([175]).

7.1.2 Strumenti che forniscono garanzie adeguate

Da quando è stata elaborata la relazione del 2020 sono stati sviluppati ulteriori strumenti che forniscono garanzie adeguate e sono stati pubblicati orientamenti pratici per agevolarne l'uso.

Come annunciato nella relazione del 2020, la Commissione ha adottato clausole contrattuali tipo aggiornate([176]), elaborate in ampia misura sulla base dei riscontri di vari portatori di interessi([177]). Le nuove clausole contrattuali tipo hanno sostituito i tre insiemi di clausole contrattuali tipo adottati a norma della direttiva sulla protezione dei dati. Le principali innovazioni comprendono: i) garanzie aggiornate in linea con il GDPR; ii) un approccio modulare che offre un punto d'ingresso unico che contempla un'ampia gamma di scenari di trasferimento; iii) maggiore flessibilità per l'uso delle clausole contrattuali tipo da più parti; e iv) un pacchetto di strumenti pratici per conformarsi alla sentenza *Schrems II*.

Le clausole contrattuali tipo aggiornate sono state accolte con favore dai portatori di interessi e i riscontri ricevuti confermano che le clausole contrattuali tipo rimangono di gran lunga lo strumento più utilizzato dagli esportatori di dati dell'UE per i trasferimenti([178]). Per agevolare gli sforzi compiuti dagli esportatori di dati ai fini della conformità, la Commissione ha elaborato una raccolta di domande e risposte che fornisce ulteriori orientamenti sull'uso delle clausole([179]), la quale verrà ulteriormente aggiornata nel caso in cui sorgano nuove domande, anche alla luce degli ulteriori riscontri ricevuti nell'ambito della presente valutazione.

Molti esportatori di dati riferiscono di aver incontrato difficoltà nell'effettuare le "valutazioni d'impatto sui trasferimenti" richieste dalla sentenza *Schrems II*, facendo riferimento in particolare alla loro complessità, nonché ai costi e al tempo necessario per eseguirle([180]). Pur apprezzando gli orientamenti del comitato e le clausole contrattuali tipo, chiedono ulteriori orientamenti (ad esempio sulle responsabilità delle parti coinvolte e sul livello di dettaglio richiesto nelle valutazioni d'impatto sui trasferimenti) e strumenti supplementari che li assistano nell'esecuzione delle valutazioni (ad esempio modelli, valutazioni generali per paese, elenchi dei rischi). Sebbene i portatori di interessi abbiano fornito tali riscontri principalmente in relazione alle clausole contrattuali tipo, le stesse valutazioni sono necessarie anche per altri strumenti di trasferimento (come le norme vincolanti d'impresa). È pertanto importante che il comitato, sulla base dell'esperienza acquisita negli ultimi anni per quanto riguarda l'applicazione delle prescrizioni della sentenza *Schrems II*, anche nell'ambito delle attività di applicazione delle norme svolte dalle autorità nazionali di protezione dei dati, prenda in considerazione la possibilità di esaminare modalità/strumenti per agevolare ulteriormente gli sforzi compiuti dagli esportatori di dati ai fini della conformità in tale contesto.

([175]) Come Argentina, Colombia, Israele, Marocco, Svizzera e Uruguay.
([176]) Decisione di esecuzione (UE) 2021/914 della Commissione (GU L 199 del 7.6.2021, pag. 31).
([177]) Tra cui, ad esempio, il parere congiunto 2/2021 dell'EDPB e del GEPD nell'ambito della procedura di adozione delle clausole contrattuali tipo.
([178]) Posizione e conclusioni del Consiglio, punto 37; contributo del comitato, pag. 9; sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([179]) https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_it.
([180]) Cfr. ad esempio la sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.

La Commissione sta elaborando ulteriori insiemi di clausole contrattuali tipo a integrazione delle clausole esistenti, nell'ottica di offrire agli esportatori di dati dell'UE un pacchetto completo e coerente. Ciò comprenderà clausole contrattuali tipo a norma del regolamento (UE) 2018/1725 per i trasferimenti di dati da parte delle istituzioni e degli organi dell'UE a operatori commerciali in paesi terzi([181]) e clausole contrattuali tipo per i trasferimenti di dati a importatori di dati di paesi terzi le cui operazioni di trattamento sono direttamente soggette al GDPR. Queste ultime rispondono alla richiesta avanzata dai portatori di interessi di tenere specificamente conto degli scenari in cui l'importatore di dati rientra nell'ambito di applicazione territoriale del GDPR (ad esempio in quanto il trattamento in questione interessa il mercato dell'UE a norma dell'articolo 3, paragrafo 2, del GDPR)([182]). Come chiarito dal comitato, anche in questo caso è necessario uno strumento di trasferimento a norma del capo V del GDPR, dati i maggiori rischi cui sono esposti i dati personali trattati al di fuori dell'UE, ad esempio a causa di eventuali leggi nazionali contrastanti o di un accesso sproporzionato della pubblica amministrazione nel paese terzo([183]). Le nuove clausole contrattuali tipo che la Commissione sta elaborando contempleranno specificamente tale scenario e terranno pienamente conto delle prescrizioni che già si applicano direttamente ai titolari del trattamento e ai responsabili del trattamento in questione a norma del GDPR ([184]).

Come riconosciuto anche da diversi tipi di portatori di interessi([185]), le clausole tipo svolgono un ruolo sempre più centrale nell'agevolare la circolazione dei dati in tutto il mondo. Diversi paesi hanno adottato le clausole contrattuali tipo dell'UE come meccanismo di trasferimento nell'ambito della propria normativa in materia di protezione dei dati, apportando adeguamenti formali limitati al loro ordinamento giuridico interno([186]). Altri paesi hanno adottato clausole tipo proprie che condividono caratteristiche importanti con le clausole contrattuali tipo dell'UE([187]). Un esempio particolarmente pertinente è l'elaborazione di clausole tipo da parte di altre organizzazioni o reti internazionali/regionali, come il comitato consultivo della convenzione 108 del Consiglio d'Europa, la rete iberoamericana per la protezione dei dati e l'Associazione delle nazioni del sud-est asiatico (ASEAN)([188]). Ciò apre nuove opportunità per agevolare la circolazione dei dati tra diverse regioni del mondo sulla base di clausole tipo. Un esempio concreto è la guida UE-ASEAN sulle clausole contrattuali tipo dell'UE e le clausole tipo dell'ASEAN, che, sulla base dei contributi ricevuti dalle imprese, le assiste nei loro sforzi di conformità in relazione a entrambi gli insiemi di clausole([189]).

([181]) Conformemente all'articolo 48, paragrafo 2, lettera b), del regolamento (UE) 2018/1725.

([182]) Posizione e conclusioni del Consiglio, punto 37; contributo del comitato, pag. 9; sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.

([183]) Linee guida 05/2021 dell'EDPB, pag. 3.

([184]) Come indicato anche nelle linee guida 05/2021 dell'EDPB, sezione 4.

([185]) Contributo del comitato, pag. 9; sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.

([186]) Ad esempio il Regno Unito (https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) e la Svizzera (https://www.edoeb.admin.ch/edoeb/it/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html).

([187]) Ad esempio la Nuova Zelanda (https://privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/) e l'Argentina (https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm).

([188]) Cfr. https://rm.coe.int/t-pd-2022-1rev10-en-final/1680abc6b4; https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf e https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.

([189]) https://commission.europa.eu/document/download/df5cd5a0-7387-4a2a-8058-8d2ccfec3062_en?filename=%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf.

Oltre alle clausole contrattuali tipo, le norme vincolanti d'impresa continuano a essere ampiamente utilizzate per la circolazione dei dati tra membri di gruppi societari o tra imprese che esercitano un'attività economica congiunta. Da quando si applica il GDPR, il comitato ha adottato 80 pareri positivi su decisioni nazionali che approvano norme vincolanti d'impresa([190]). Il comitato ha inoltre pubblicato orientamenti sugli elementi da includere nelle norme vincolanti d'impresa per i titolari del trattamento (e sulle informazioni da fornire nell'ambito dell'applicazione delle norme vincolanti d'impresa), che sono stati aggiornati per tenere conto delle prescrizioni del GDPR e della sentenza *Schrems II*([191]). Sono inoltre in fase di elaborazione orientamenti aggiornati sulle norme vincolanti d'impresa per i responsabili del trattamento([192]). Poiché le norme vincolanti d'impresa mirano a mettere in atto politiche/programmi vincolanti in materia di protezione dei dati nelle imprese, molti portatori di interessi le considerano uno strumento di conformità particolarmente utile e uno strumento di trasferimento affidabile([193]). Allo stesso tempo i portatori di interessi continuano a segnalare che la lunghezza e la complessità del processo di approvazione da parte delle autorità nazionali di protezione dei dati impediscono una più ampia diffusione delle norme vincolanti d'impresa. È pertanto importante che le autorità continuino ad adoperarsi per razionalizzare e abbreviare il processo di approvazione.

Da quando è stata elaborata la relazione del 2020 sono state adottate anche misure per agevolare il ricorso alla certificazione e ai codici di condotta come strumenti per i trasferimenti, ad esempio attraverso l'adozione da parte del comitato di appositi orientamenti riguardanti i due strumenti([194]). Allo stesso tempo i portatori di interessi segnalano le stesse problematiche relative alle tempistiche e alla complessità del processo di approvazione menzionate in precedenza per quanto riguarda la certificazione e i codici di condotta in qualità di strumenti di responsabilizzazione.

Infine, il GDPR prevede anche strumenti specifici (accordi internazionali e accordi amministrativi approvati dalle autorità di protezione dei dati) a disposizione delle autorità pubbliche per trasferire dati personali alle loro omologhe di paesi terzi o a organizzazioni internazionali. Il comitato ha adottato orientamenti sulle garanzie che dovrebbero essere incluse in tali strumenti([195]), le quali possono agevolare la negoziazione degli accordi in questione.

7.1.3 Garantire la complementarità con altre politiche

Poiché la circolazione dati è divenuta essenziale per molte attività, è fondamentale garantire che le politiche in materia di protezione dei dati e altre politiche si integrino a vicenda. L'inclusione di garanzie in materia di protezione dei dati negli strumenti internazionali è spesso non solo un presupposto per la circolazione dei dati, ma anche un importante fattore abitante di una cooperazione stabile e affidabile.

Ad esempio, gli accordi internazionali che prevedono le necessarie garanzie in materia di protezione dei dati, anche assicurando la continuità della protezione da parte di un'autorità richiedente, sono essenziali per garantire la cortesia e agevolare l'accesso transfrontaliero delle autorità di contrasto alle prove elettroniche detenute dalle imprese, favorendo così una lotta più efficace contro la criminalità. Tale approccio si riflette nel secondo protocollo

([190]) Contributo del comitato, pag. 9.
([191]) Raccomandazioni 1/2022 dell'EDPB.
([192]) Contributo del comitato, pag. 9.
([193]) Sintesi del feedback fornito dal gruppo multilaterale di esperti sul GDPR.
([194]) Linee guida 7/2022 e linee guida 4/2021 dell'EDPB.
([195]) Linee guida 2/2020 dell'EDPB.

addizionale alla convenzione sulla criminalità informatica([196]), che rafforza le norme esistenti per ottenere l'accesso transfrontaliero alle prove elettroniche nelle indagini penali, assicurando nel contempo adeguate garanzie in materia di protezione dei dati. Il protocollo è stato nel frattempo firmato da diversi Stati membri dell'UE. Analogamente, stanno procedendo i negoziati bilaterali tra l'UE e gli Stati Uniti su un accordo sull'accesso transfrontaliero alle prove elettroniche per la cooperazione in materia penale([197]).

Lo scambio dei dati del codice di prenotazione (*Passenger Name Record*, PNR) è un altro settore della politica di sicurezza dell'UE che ha beneficiato dello sviluppo di solide garanzie in materia di protezione dei dati. Nel 2023 l'UE e il Canada hanno concluso i negoziati su un nuovo accordo PNR in linea con i requisiti stabiliti dalla Corte di giustizia nel suo parere 1/15([198]). Garanzie analoghe sono state introdotte nel capitolo relativo al PNR dell'accordo sugli scambi e la cooperazione UE-Regno Unito. L'inclusione di una maggiore tutela della vita privata in tali accordi, che possono fungere da modello per futuri accordi con altri partner, garantisce ai vettori aerei la certezza del diritto, assicurando nel contempo la stabilità di importanti scambi di informazioni volti a contrastare il terrorismo e altri reati gravi di natura transnazionale.

La Commissione propone inoltre disposizioni rigorose per tutelare la vita privata e promuovere il commercio digitale nell'ambito dei negoziati in corso in seno all'Organizzazione mondiale del commercio sull'iniziativa per una dichiarazione comune sul commercio elettronico. Disposizioni analoghe sulla lotta agli ostacoli ingiustificati al commercio digitale, che tutelano nel contempo il necessario spazio strategico delle parti nel settore della protezione dei dati, sono state coerentemente incluse negli accordi di libero scambio conclusi dall'UE a seguito dell'entrata in applicazione del GDPR, in particolare nell'accordo sugli scambi e la cooperazione UE-Regno Unito e negli accordi con il Cile, il Giappone e la Nuova Zelanda. Disposizioni in materia di tutela della vita privata e circolazione dei dati sono oggetto di discussione anche nell'ambito dei negoziati sul commercio digitale in corso con Singapore e la Corea del Sud.

7.2 La cooperazione internazionale in materia di protezione dei dati

7.2.1 La dimensione bilaterale

La Commissione ha continuato a tenere un dialogo con paesi e organizzazioni internazionali sullo sviluppo, la riforma e l'attuazione delle norme in materia di tutela della vita privata, anche presentando contributi alle consultazioni pubbliche su progetti legislativi o misure normative in materia di riservatezza([199]), testimoniando dinanzi agli organi parlamentari competenti([200]) e partecipando ad apposite riunioni con rappresentanti dei governi, delegazioni parlamentari e autorità di regolamentazione di numerose regioni del mondo([201]). Alcune di queste attività sono state svolte attraverso il progetto finanziato dall'UE "Enhanced Data Protection and Data Flows", che sostiene i paesi che intendono sviluppare quadri moderni in materia di protezione dei dati o rafforzare la capacità delle

([196]) Secondo protocollo addizionale alla convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione delle prove elettroniche (STCE n. 224).

([197]) https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_it.

([198]) Proposta della Commissione di decisione del Consiglio relativa alla firma, a nome dell'Unione europea, di un accordo tra il Canada e l'Unione europea sul trasferimento e sul trattamento dei dati del codice di prenotazione (PNR) (COM(2024) 94 final).

([199]) Si è trattato di consultazioni organizzate, ad esempio, da Australia, Cina, Ruanda, Argentina, Brasile, Etiopia, Indonesia, Perù, Malaysia e Thailandia.

([200]) Ad esempio, dinanzi agli organi parlamentari di Cile, Ecuador e Paraguay.

([201]) Ciò ha incluso anche l'organizzazione di seminari e visite di studio, ad esempio in collaborazione con Kenya, Indonesia e Singapore.

loro autorità di regolamentazione attraverso la formazione, la condivisione delle conoscenze, lo sviluppo di capacità e lo scambio delle migliori pratiche. La Commissione ha inoltre contribuito ad altre iniziative, come l'alleanza digitale UE-CELAC.

La protezione dei dati continuerà inoltre a svolgere un ruolo chiave nelle attività della Commissione in materia di allargamento. La normativa dell'UE in materia di protezione dei dati è una componente importante dello sforzo complessivo compiuto dai paesi dell'allargamento per allineare i loro quadri giuridici a quelli dell'UE (soprattutto in quanto il trattamento e lo scambio di dati personali sono al centro di numerose politiche). L'indipendenza e il corretto funzionamento di un'autorità di protezione dei dati sono inoltre un elemento chiave del sistema generale di bilanciamento dei poteri e dello Stato di diritto e assumeranno sempre maggiore importanza nel contesto della graduale integrazione dei paesi dell'allargamento nel mercato unico dell'UE (come previsto da iniziative quali il piano di crescita per i Balcani occidentali).

Un aspetto sempre più importante del dialogo dell'UE con i paesi terzi è incentrato sugli scambi tra le autorità di regolamentazione. Come annunciato nella relazione del 2020, la Commissione ha istituito una "Accademia sulla protezione dei dati" per promuovere gli scambi tra le autorità di protezione dei dati dell'UE e dei paesi terzi, contribuendo in tal modo allo sviluppo di capacità e migliorando la cooperazione "sul campo". L'Accademia offre attività di formazione su misura su richiesta delle autorità di paesi terzi e riunisce le competenze dei rappresentanti della comunità delle autorità di contrasto, del mondo accademico, del settore privato e delle istituzioni europee. Il valore aggiunto delle attività di formazione risiede nell'adattamento delle diverse componenti agli interessi e alle esigenze dell'autorità che ne fa richiesta. Tali attività consentono inoltre alle autorità di protezione dei dati dell'UE e dei paesi terzi di stabilire contatti, condividere conoscenze, scambiare esperienze e migliori pratiche e individuare potenziali settori di cooperazione. Finora l'Accademia ha erogato formazione alle autorità di protezione dei dati di Indonesia, Brasile, Kenya, Nigeria e Ruanda e sta preparando attività di formazione per diversi altri paesi.

Al di là dell'importanza di mantenere un dialogo tra le autorità di regolamentazione, si rileva la crescente necessità, come riconosciuto anche nei riscontri forniti dal Consiglio e dal comitato([202]), di sviluppare strumenti giuridici adeguati per forme più strette di cooperazione e assistenza reciproca, anche consentendo il necessario scambio di informazioni nel contesto delle indagini. Di fatto, poiché le violazioni della vita privata producono in misura crescente effetti transfrontalieri, spesso possono essere efficacemente indagate e affrontate solo attraverso la cooperazione tra autorità di regolamentazione dell'UE e di paesi terzi. La Commissione chiederà pertanto l'autorizzazione ad avviare negoziati per concludere accordi di cooperazione in materia di applicazione delle norme con i paesi terzi interessati (come previsto anche dall'articolo 50 del GDPR). A tale riguardo, la Commissione prende atto della richiesta del comitato di considerare nello specifico i paesi con il maggior numero di operatori direttamente soggetti al GDPR come potenziali controparti, in particolare i paesi del G7 e/o i paesi che beneficiano di decisioni di adeguatezza([203]).

La predisposizione di simili accordi di cooperazione in materia di applicazione delle norme e di assistenza reciproca contribuirebbe anche a garantire la conformità degli operatori stranieri soggetti al GDPR e l'efficace applicazione delle norme nei loro confronti, ad esempio in quanto offrono beni o servizi rivolgendosi specificamente al mercato dell'UE. Il Consiglio rileva l'importanza di garantire il rispetto del GDPR in tali casi e manifesta

([202]) Contributo del comitato, pag. 8. Posizione e conclusioni del Consiglio, punto 38.
([203]) Contributo del comitato, pag. 8.

preoccupazioni in merito alla parità di condizioni rispetto ai soggetti dell'UE e all'effettiva tutela dei diritti delle persone([204]). La Commissione concorda con l'invito del Consiglio a esaminare diverse modalità per agevolare l'applicazione delle norme in tale scenario. Anche se modalità più formali di cooperazione con le autorità di regolamentazione dei paesi terzi potrebbero certamente svolgere un ruolo importante, anche il ricorso ad altre vie già esistenti dovrebbe essere promosso con maggior vigore. Ciò comprende il pieno utilizzo del pacchetto di strumenti di applicazione delle norme di cui all'articolo 58 del GDPR e il coinvolgimento di rappresentanti di imprese straniere nell'UE (nominati conformemente all'articolo 27 del GDPR).

7.2.2 La dimensione multilaterale

La Commissione continua inoltre a partecipare attivamente a una serie di consessi internazionali per promuovere valori condivisi e favorire una convergenza a livello regionale e mondiale.

Ciò comprende ad esempio il contributo attivo alle attività del comitato consultivo della convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (convenzione 108), l'unico strumento multilaterale giuridicamente vincolante nel settore della protezione dei dati personali. Finora 31 Stati hanno ratificato il protocollo di modifica volto ad aggiornare la convenzione 108([205]), tra cui molti Stati membri dell'UE e alcuni Stati non aderenti al Consiglio d'Europa (Argentina, Maurizio e Uruguay). Tra gli Stati membri dell'UE, la firma di un solo Stato membro([206]) è ancora in sospeso, mentre otto Stati membri([207]) hanno già firmato ma non ratificato la convenzione aggiornata. La Commissione esorta lo Stato membro rimanente a firmare la convenzione aggiornata e gli altri a procedere rapidamente alla ratifica, in maniera da consentirne l'entrata in vigore nel prossimo futuro. Inoltre continua ad incoraggiare in maniera proattiva l'adesione di paesi terzi.

A livello del G20 e del G7, le discussioni sulla tutela della vita privata e sulla circolazione dei dati si sono concentrate sull'attuazione del concetto, originariamente proposto dal Giappone, di "libera circolazione dei dati in un contesto di fiducia" (*Data Free Flow with Trust*, DFFT), che riconosce che la protezione e la sicurezza dei dati possono contribuire alla fiducia nell'economia digitale e agevolare la circolazione dei dati([208]). L'OCSE svolge un ruolo particolarmente importante in tale contesto, mettendo a disposizione un forum per una comunità di esperti della DFFT, che riunisce un'ampia gamma di portatori di interessi (governi, autorità di regolamentazione, industria, società civile, mondo accademico) allo scopo di fornire contributi su progetti specifici e questioni correlate alla DFFT. Inoltre un risultato significativo dell'iniziativa DFFT, alla quale la Commissione ha contribuito in modo significativo, è l'adozione da parte dell'OCSE di una dichiarazione sull'accesso del governo ai dati personali detenuti da entità del settore privato, che costituisce il primo strumento internazionale in questo settore. Nella dichiarazione figurano una serie di requisiti condivisi per tutelare la vita privata quando si accede a dati personali a fini di sicurezza nazionale e di contrasto. Nel contesto del crescente riconoscimento a livello mondiale del fatto che la fiducia nei trasferimenti di dati è influenzata negativamente da un accesso sproporzionato delle amministrazioni pubbliche, la dichiarazione rappresenta

([204]) Posizione e conclusioni del Consiglio, punto 39.
([205]) Protocollo che modifica la convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (STCE n. 223).
([206]) Danimarca.
([207]) Belgio, Cechia, Grecia, Irlanda, Lettonia, Lussemburgo, Paesi Bassi e Svezia.
([208]) Cfr. ad esempio https://www.g7germany.de/resource/blob/974430/2062292/fbdb2c7e996205aee402386aae057c5e/2022-07-14-leaders-communique-data.pdf?download=1.

un importante contributo all'agevolazione di una circolazione affidabile dei dati. La Commissione continuerà a incoraggiare i paesi ad aderire alla dichiarazione, che è aperta anche ai paesi non aderenti all'OCSE.

La Commissione sta inoltre dialogando con diverse organizzazioni e reti regionali che definiscono garanzie comuni in materia di protezione dei dati, tra cui ad esempio l'ASEAN, l'Unione africana, il forum delle autorità di tutela della vita privata Asia-Pacifico, la rete iberoamericana per la protezione dei dati e la rete delle autorità africane di protezione dei dati (NADPA – RADPD). L'elaborazione della già menzionata guida UE-ASEAN sulle clausole tipo è un esempio concreto di tale proficua cooperazione.

La Commissione mantiene infine un dialogo con diverse organizzazioni internazionali, anche allo scopo di esaminare modalità per agevolare ulteriormente la circolazione dei dati tra l'UE e tali organizzazioni. Poiché molte organizzazioni hanno aggiornato i propri quadri in materia di protezione dei dati negli ultimi anni o sono in procinto di farlo, stanno emergendo anche nuove opportunità di scambio di esperienze e migliori pratiche. A tale riguardo, i seminari annuali con organizzazioni internazionali e un'apposita task force sui trasferimenti internazionali di dati organizzati dal Garante europeo della protezione dei dati si sono dimostrati particolarmente utili per lo scambio e la valutazione di strumenti concreti di cooperazione, compreso lo scambio di dati personali([209]).

8 CONCLUSIONI

Nei sei anni trascorsi da quando è divenuto applicabile, il GDPR ha consentito alle persone di avere un controllo sui propri dati. Ha inoltre contribuito a creare condizioni di parità per le imprese e ha fornito le fondamenta per la gamma di iniziative che stanno guidando la transizione digitale nell'UE.

Per conseguire pienamente il duplice obiettivo del GDPR – vale a dire assicurare una solida protezione delle persone fisiche, garantendo nel contempo la libera circolazione dei dati personali all'interno dell'UE e flussi di dati sicuri al di fuori dell'UE – occorre concentrarsi su.

- una rigorosa applicazione di tale regolamento, a partire dalla rapida adozione della proposta della Commissione relativa alle norme procedurali, in modo da garantire la disponibilità di mezzi di ricorso rapidi e la certezza del diritto nei casi che interessano persone fisiche in tutta l'UE;
- un sostegno proattivo da parte delle autorità di protezione dei dati agli sforzi di conformità compiuti dai portatori di interessi, in particolare dalle PMI e dai piccoli operatori;
- un'interpretazione e un'applicazione coerenti del GDPR in tutta l'UE;
- una cooperazione efficace tra le autorità di regolamentazione a livello sia nazionale che dell'UE per garantire un'applicazione uniforme e coerente del crescente insieme di norme dell'UE sul digitale;
- ulteriori progressi nella strategia internazionale della Commissione in materia di protezione dei dati.

Per sostenere un'efficace applicazione del GDPR e orientare le riflessioni future sulla protezione dei dati, è necessaria la serie di azioni qui individuate. La Commissione sosterrà

([209]) https://www.edps.europa.eu/data-protection/our-work/edps-worldwide/data-protection-and-international-organisations_en.

e monitorerà la loro attuazione anche in vista della prossima relazione, la cui pubblicazione è prevista nel 2028.

Sviluppo di efficaci strutture di cooperazione

Il Parlamento europeo e il Consiglio sono invitati ad adottare rapidamente la proposta relativa alle norme procedurali del GDPR.

Il comitato e le autorità di protezione dei dati sono invitati a:

- instaurare una cooperazione regolare con altre autorità di regolamentazione settoriali su questioni che hanno un impatto sulla protezione dei dati, in particolare quelle istituite nell'ambito della nuova normativa dell'UE sul digitale, e partecipare attivamente alle strutture a livello dell'UE concepite per agevolare la cooperazione tra autorità di regolamentazione;
- avvalersi in misura maggiore degli strumenti di cooperazione previsti dal GDPR, in modo da ricorrere alla composizione delle controversie solo come ultima soluzione possibile;
- adottare modalità di lavoro più efficienti e mirate per l'elaborazione di orientamenti, pareri e decisioni e dare priorità alle questioni chiave, al fine di ridurre l'onere gravante sulle autorità di protezione dei dati e reagire più rapidamente alle evoluzioni del mercato.

Gli Stati membri devono:

- garantire l'indipendenza effettiva e piena delle autorità nazionali di protezione dei dati;
- assegnare risorse sufficienti alle autorità di protezione dei dati per consentire loro di svolgere i loro compiti, in particolare dotandole delle risorse tecniche e delle competenze necessarie per occuparsi delle tecnologie emergenti e ottemperare alle nuove responsabilità previste dalla normativa sul digitale;
- dotare le autorità di protezione dei dati degli strumenti di indagine necessari affinché possano esercitare efficacemente i poteri di esecuzione previsti dal GDPR;
- favorire il dialogo tra le autorità di protezione dei dati e altre autorità nazionali di regolamentazione, in particolare quelle istituite a norma della nuova normativa sul digitale.

La Commissione:

- sosterrà attivamente la rapida adozione della proposta relativa alle norme procedurali del GDPR da parte dei colegislatori;
- continuerà a monitorare attentamente l'indipendenza effettiva e completa delle autorità nazionali di protezione dei dati;
- creerà sinergie e coerenza tra il GDPR e tutta la normativa inerente al trattamento dei dati personali sulla base dell'esperienza e, se necessario, adotterà misure adeguate per garantire la certezza del diritto;
- rifletterà su come affrontare meglio la necessità di una cooperazione strutturata ed efficiente tra le autorità di regolamentazione per garantire l'applicazione efficace, uniforme e coerente delle norme dell'UE sul digitale, rispettando nel contempo la competenza delle autorità di protezione dei dati per quanto riguarda tutte le questioni inerenti al trattamento dei dati personali.

Attuazione e integrazione del quadro giuridico

Gli Stati membri devono:

- garantire che le autorità di protezione dei dati vengano consultate tempestivamente prima dell'adozione della normativa sul trattamento dei dati personali.

La Commissione:

- continuerà a utilizzare tutti gli strumenti a sua disposizione, comprese le procedure di infrazione, per garantire che gli Stati membri rispettino il GDPR;
- continuerà a favorire scambi di opinioni e prassi nazionali tra gli Stati membri, anche attraverso il gruppo di esperti degli Stati membri sul GDPR;
- provvederà affinché i minori siano protetti, responsabilizzati e rispettati online;
- rifletterà sulle possibili prossime azioni da compiere per quanto riguarda la proposta di regolamento sulla vita privata e le comunicazioni elettroniche, compresa la sua relazione con il GDPR.

Sostegno ai portatori di interessi

Il comitato e le autorità di protezione dei dati sono invitati a:

- avviare un dialogo costruttivo con i titolari del trattamento e i responsabili del trattamento sulla conformità al GDPR;
- intensificare ulteriormente gli sforzi volti a favorire la conformità delle PMI, fornendo orientamenti e strumenti su misura, rispondendo a eventuali preoccupazioni infondate in materia di conformità manifestate da PMI la cui attività principale non consiste nel trattamento di dati personali e coadiuvandole nei loro sforzi di conformità;
- sostenere l'attuazione di efficaci misure di conformità da parte delle imprese, quali la certificazione e i codici di condotta (anche come strumenti per i trasferimenti), interagendo con i portatori di interessi durante il processo di approvazione, stabilendo tempistiche chiare per le approvazioni e, conformemente all'impegno assunto nella strategia 2024-2027 del comitato, spiegando ai gruppi chiave di portatori di interessi in che modo possono essere utilizzati tali strumenti;
- garantire che gli orientamenti nazionali e l'applicazione del GDPR a livello nazionale siano coerenti con gli orientamenti del comitato e con la giurisprudenza della Corte di giustizia;
- risolvere le divergenze di interpretazione del GDPR tra le autorità di protezione dei dati, anche tra le autorità dello stesso Stato membro;
- fornire orientamenti concisi, pratici e accessibili al pubblico interessato, conformemente all'impegno assunto nella strategia 2024-2027 del comitato;
- garantire una consultazione più tempestiva e più significativa per quanto riguarda gli orientamenti e i pareri, così da comprendere meglio le dinamiche del mercato e le pratiche commerciali, prendere adeguatamente in considerazione i riscontri ricevuti e tenere conto dell'applicazione concreta delle interpretazioni adottate;
- portare a termine in via prioritaria le attività in corso sugli orientamenti riguardanti i dati dei minori, la ricerca scientifica, l'anonimizzazione, la pseudonimizzazione e il legittimo interesse;
- intensificare le attività di sensibilizzazione, di informazione e di applicazione delle norme per garantire che i responsabili della protezione dei dati possano svolgere il loro ruolo a norma del GDPR.

La Commissione:

- continuerà a fornire sostegno finanziario alle attività delle autorità di protezione dei dati che agevolano l'assolvimento degli obblighi previsti dal GDPR da parte delle PMI;
- utilizzerà tutti i mezzi disponibili per fornire chiarimenti rapidi su questioni importanti per i portatori di interessi, comprese le PMI, in particolare richiedendo il parere del comitato.

Ulteriore sviluppo del pacchetto di strumenti per i trasferimenti di dati e la cooperazione internazionale

Il comitato e le autorità di protezione dei dati sono invitati a:

- portare a termine le attività volte a razionalizzare e abbreviare il processo di approvazione delle norme vincolanti d'impresa e ad aggiornare gli orientamenti su elementi contenuti nelle norme vincolanti d'impresa per il responsabile del trattamento;
- esaminare modalità/strumenti per assistere ulteriormente gli esportatori di dati nei loro sforzi di conformità in relazione alle prescrizioni della sentenza *Schrems II*;
- esaminare ulteriori modalità per garantire un'applicazione efficace delle norme nei confronti degli operatori stabiliti in paesi terzi che rientrano nell'ambito di applicazione territoriale del GDPR.

Gli Stati membri devono:

- garantire quanto prima la firma e la ratifica della convenzione 108+ aggiornata del Consiglio d'Europa da parte degli Stati membri che non hanno ancora provveduto, così da consentirne l'entrata in vigore.

La Commissione:

- compirà ulteriori progressi nei colloqui in corso sull'adeguatezza, valuterà l'ulteriore sviluppo degli accertamenti dell'adeguatezza esistenti e intraprenderà nuovi dialoghi sull'adeguatezza con i partner interessati;
- favorirà una maggiore cooperazione in seno alla rete dei paesi che beneficiano di decisioni di adeguatezza;
- porterà a termine le attività sulle clausole contrattuali tipo aggiuntive, in particolare per i trasferimenti di dati il cui trattamento è direttamente soggetto al GDPR agli importatori di dati e per i trasferimenti di dati da parte delle istituzioni e degli organi dell'UE a norma del regolamento (UE) 2018/1725;
- coopererà con i partner internazionali per agevolare la circolazione dei dati sulla base di clausole contrattuali tipo;
- sosterrà i processi di riforma in corso nei paesi terzi per quanto riguarda norme nuove o aggiornate in materia di protezione dei dati, condividendo esperienze e migliori pratiche;
- dialogherà con le organizzazioni internazionali e regionali quali l'OCSE e il G7 per promuovere una circolazione affidabile dei dati sulla base di elevati standard di protezione dei dati, anche nel contesto dell'iniziativa DFFT;
- agevolerà e favorirà gli scambi tra le autorità di regolamentazione europee e internazionali, anche attraverso l'Accademia sulla protezione dei dati;

- contribuirà ad agevolare la cooperazione internazionale tra le autorità di controllo in materia di applicazione delle norme, anche attraverso la negoziazione di accordi di cooperazione e di assistenza reciproca.