COMMISSIONE
EUROPEA

Bruxelles, 24.6.2020
COM(2020) 264 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

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

{SWD(2020) 115 final}

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

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

1 LE NORME IN MATERIA DI PROTEZIONE DEI DATI COME PILASTRO DELL'AUTONOMIA DEI CITTADINI E DELL'APPROCCIO DELL'UE ALLA TRANSIZIONE DIGITALE

La presente relazione è la prima relazione sulla valutazione e sul riesame del regolamento generale sulla protezione dei dati[1], in particolare sull'applicazione e sul funzionamento delle norme sul trasferimento di dati personali verso paesi terzi e organizzazioni internazionali e delle norme in materia di cooperazione e coerenza, a norma dell'articolo 97 di detto regolamento.

Il regolamento generale sulla protezione dei dati, che si applica dal 25 maggio 2018, si colloca al centro del quadro dell'UE[2] che garantisce il diritto fondamentale alla protezione dei dati, sancito dalla Carta dei diritti fondamentali dell'Unione europea (articolo 8) e dai trattati (articolo 16 del trattato sul funzionamento dell'Unione europea, "TFUE"). Il regolamento generale sulla protezione dei dati rafforza le garanzie in materia di protezione dei dati, fornisce alle persone fisiche diritti aggiuntivi e più forti, aumenta la trasparenza e garantisce che tutti coloro che trattano dati personali nell'ambito della sua applicazione siano maggiormente responsabilizzati e responsabili. Conferisce alle autorità indipendenti di protezione dei dati poteri di esecuzione più forti e armonizzati e istituisce un nuovo sistema di governance. Crea inoltre parità di condizioni per tutte le imprese che operano sul mercato dell'UE, indipendentemente dal luogo in cui sono stabilite, e garantisce la libera circolazione dei dati all'interno dell'UE, rafforzando così il mercato interno.

Il regolamento generale sulla protezione dei dati costituisce una componente importante dell'approccio alla tecnologia incentrato sulla persona nonché la bussola per l'impiego della tecnologia nel contesto della duplice transizione, ecologica e digitale, che caratterizza la definizione delle politiche dell'UE. Questo aspetto è stato sottolineato più recentemente dal Libro bianco sull'intelligenza artificiale[3] e dalla

---

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GU L 119 del 4.5.2016, pag. 1).

[2] In seguito alla sua integrazione nell'accordo sullo Spazio economico europeo (SEE), il regolamento si applica anche alla Norvegia, all'Islanda e al Liechtenstein.

[3] https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_it.

comunicazione "Una strategia europea per i dati"[4] (in appresso "la strategia in materia di dati") del febbraio 2020.

In un'economia sempre più basata sul trattamento di dati, compresi i dati personali, il regolamento generale sulla protezione dei dati è uno strumento essenziale per garantire che le persone dispongano di un migliore controllo sui loro dati personali e che tali dati siano trattati per una finalità legittima, in maniera lecita, corretta e trasparente. Allo stesso tempo, il regolamento contribuisce a promuovere un'innovazione degna di fiducia, in particolare attraverso il suo approccio basato sul rischio e principi quali la tutela della vita privata fin dalla progettazione e per impostazione predefinita. La Commissione ha proposto di integrare il quadro legislativo in materia di protezione dei dati e della vita privata[5] mediante il regolamento sulla vita privata e le comunicazioni elettroniche[6], destinato a sostituire l'attuale direttiva relativa alla vita privata e alle comunicazioni elettroniche[7]. La proposta è attualmente all'esame dei colegislatori e sarebbe molto importante garantirne la rapida adozione.

Nel quadro delle principali priorità della Commissione di "Un'Europa pronta per l'era digitale"[8] e del "Green Deal europeo"[9] è possibile sviluppare iniziative nuove destinate a consentire ai cittadini di svolgere un ruolo maggiormente attivo nella transizione digitale e nello sfruttamento di strumenti digitali per consentire la realizzazione di una società a impatto climatico zero e di uno sviluppo sostenibile. Il regolamento generale sulla protezione dei dati stabilisce un quadro per tali iniziative e garantisce che queste siano concepite in maniera tale da permettere effettivamente alle persone di agire in autonimia.

La strategia in materia di dati[10] richiede la creazione di uno "spazio unico europeo di dati", un vero e proprio mercato unico dei dati, nonché di dieci spazi comuni europei di dati settoriali pertinenti per la duplice transizione, ecologica e digitale[11]. Per tutte queste priorità è fondamentale un quadro chiaro e praticabile per la condivisione sicura e

---

[4] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_it.

[5] Tale quadro legislativo comprende anche la direttiva in materia di protezione dei dati da parte delle autorità di contrasto (direttiva (UE) 2016/680) e il regolamento in materia di protezione dei dati da parte delle istituzioni, degli organi e degli organismi dell'Unione (regolamento (UE) 2018/1725).

[6] Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM(2017) 10 final - 2017/03 (COD).

[7] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_it.

[9] Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Il Green Deal europeo, COM(2019) 640 final.

[10] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni: Una strategia europea per i dati, COM(2020) 66 final.

[11] Tali dieci spazi comuni europei di dati settoriali riguardano: salute, produzione industriale, energia, mobilità, agricoltura, dati finanziari, pubblica amministrazione, uno spazio comune europeo di dati concernente i dati relativi alle competenze, uno spazio di dati relativo al Green Deal europeo e un cloud europeo per la scienza aperta (*European Open Science Cloud*).

una maggiore disponibilità dei dati. La strategia in materia di dati ha altresì annunciato l'intenzione della Commissione di esaminare nella futura legislazione in che modo consentire l'utilizzo dei dati conservati nelle banche dati pubbliche per finalità di ricerca scientifica in maniera conforme al regolamento generale sulla protezione dei dati. Gli spazi di dati devono essere sostenuti dalla federazione europea del cloud, che fornisce servizi di trattamento dei dati e di infrastrutture cloud conformi a detto regolamento. Quest'ultimo garantisce un elevato livello di protezione dei dati personali e un ruolo centrale delle persone fisiche in tutti questi spazi di dati, offrendo allo stesso tempo la flessibilità necessaria per consentire approcci diversi.

La necessità di garantire la fiducia e la domanda di protezione dei dati personali non sono certamente aspetti limitati all'UE. Le persone fisiche di tutto il mondo conferiscono un'importanza sempre maggiore alla tutela della vita privata e alla sicurezza dei loro dati. Come dimostrato da una recente indagine su scala mondiale[12], le persone ritengono che tale aspetto sia un fattore importante che influenza le loro decisioni di acquisto e il loro comportamento online. Un numero crescente di imprese ha risposto a tale domanda di tutela della vita privata, in particolare estendendo volontariamente taluni dei diritti e delle garanzie previsti nel regolamento generale sulla protezione dei dati ai clienti che non hanno sede nell'UE. Molte imprese promuovono altresì il rispetto dei dati personali come differenziatore competitivo e un fattore di vendita sul mercato mondiale, offrendo prodotti e servizi innovativi dotati di nuove soluzioni in materia di tutela della vita privata o sicurezza dei dati. Inoltre la maggiore capacità dei soggetti attivi nel settore pubblico e in quello privato di raccogliere e trattare dati su larga scala solleva questioni importanti e complesse che pongono sempre di più la tutela della vita privata al centro del dibattito pubblico in diverse parti del mondo.

L'adozione del regolamento generale sulla protezione dei dati ha spinto altri paesi in numerose regioni del mondo a prendere in considerazione la possibilità di seguire l'esempio. Si tratta di una tendenza realmente universale che va dal Cile alla Corea del Sud, dal Brasile al Giappone, dal Kenya all'India e dalla California all'Indonesia. La leadership dell'UE in materia di protezione dei dati mostra che può fungere da punto di riferimento a livello mondiale per la regolamentazione dell'economia digitale ed è stata accolta con favore da voci importanti della comunità internazionale, quali il Segretario generale delle Nazioni Unite António Guterres, il quale ha sottolineato come il regolamento generale sulla protezione dei dati "*abbia fissato un esempio* [...] *che ispira misure analoghe*" ed ha "*esorta[to] l'UE e i suoi Stati membri a continuare ad agire da leader nel plasmare l'era digitale e nell'essere all'avanguardia in materia di innovazione tecnologica e regolamentazione*"[13].

L'attuale crisi dettata dalla pandemia di Covid-19 offre un chiaro esempio di questa globalizzazione del dibattito sulla tutela della vita privata durante la crisi e il mondo

---

[12] Cfr., ad esempio, il *Consumer Privacy Study* [Studio sulla tutela della vita privata dei consumatori] di Cisco del 2019 (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf). Secondo tale studio che ha coinvolto 2 600 consumatori a livello mondiale, un numero significativo di consumatori ha già adottato misure per proteggere la propria vita privata, ad esempio cambiando società o fornitori a causa delle loro politiche in materia di dati o delle loro pratiche di condivisione dei dati.

[13] Discorso del Segretario generale delle Nazioni Unite al Senato italiano, 18 dicembre 2019 (disponibile al seguente indirizzo: https://www.un.org/press/en/2019/sgsm19916.doc.htm).

sta cercando di uscirne. All'interno dell'Unione diversi Stati membri hanno adottato misure di emergenza per tutelare la salute pubblica. Il regolamento generale sulla protezione dei dati è chiaro nell'affermare che qualsiasi restrizione deve rispettare l'essenza dei diritti e delle libertà fondamentali ed essere una misura necessaria e proporzionata in una società democratica per salvaguardare un interesse pubblico, quale quello della sanità pubblica. Mentre si provvede a un allentamento graduale delle misure di contenimento, i decisori devono far fronte alle aspettative dei cittadini che si aspettano di vedersi offrire soluzioni digitali affidabili e rispettose dei diritti alla tutela della vita privata e alla protezione dei dati personali.

In numerosi paesi le misure di tutela integrata della vita privata, come ad esempio la registrazione su base volontaria degli utenti, la minimizzazione dei dati e la sicurezza, nonché l'esclusione della geolocalizzazione, sono considerate essenziali per garantire l'affidabilità e l'accettazione da parte della società di soluzioni basate sui dati volte a monitorare e contenere la diffusione del virus, a calibrare le contromisure di ordine pubblico, ad assistere i pazienti o ad attuare strategie di uscita. Nell'UE il quadro legislativo in materia di protezione dei dati e tutela della vita privata[14] si è dimostrato uno strumento sufficientemente flessibile per consentire lo sviluppo di soluzioni pratiche (ad esempio app di tracciamento), garantendo allo stesso tempo un livello elevato di protezione dei dati personali. In tale contesto il 16 aprile 2020 la Commissione ha pubblicato orientamenti sulle app a sostegno della lotta contro la pandemia in relazione alla protezione dei dati[15].

La protezione dei dati personali è fondamentale anche ai fini della prevenzione della manipolazione delle scelte dei cittadini, in particolare attraverso il micro-targeting degli elettori basato sul trattamento illecito dei dati personali, la prevenzione di ingerenze nei processi democratici e la tutela dell'apertura, della correttezza e della trasparenza del dibattito, elementi essenziali di una democrazia. Per questo motivo, nel settembre 2018 la Commissione ha pubblicato i suoi orientamenti sull'applicazione del diritto dell'Unione in materia di protezione dei dati nel contesto elettorale[16].

Ai fini della presente attività di valutazione e riesame, la Commissione ha tenuto conto dei contributi del Consiglio[17], del Parlamento europeo[18], del comitato europeo

---

[14] Tale quadro comprende, oltre al regolamento generale sulla protezione dei dati, la direttiva relativa alla vita privata e alle comunicazioni elettroniche (direttiva 2002/58/CE) che prevede, tra l'altro, norme in materia di accesso e conservazione delle informazioni sugli apparecchi terminali degli utenti.

[15] Comunicazione della Commissione Orientamenti sulle app a sostegno della lotta alla pandemia di Covid-19 relativamente alla protezione dei dati 2020/C 124 I/01 – C/2020/2523 (GU C 124I del 17.4.2020, pag. 1). Il 16 aprile 2020 gli Stati membri dell'UE, sostenuti dalla Commissione, hanno sviluppato un insieme di strumenti dell'UE per l'uso di applicazioni mobili per tracciare i contatti e fornire avvertimenti in risposta alla pandemia di coronavirus. Tale attività rientra in un approccio coordinato comune destinato a sostenere la graduale revoca delle misure di confinamento. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[16] Documento di orientamento, Orientamenti della Commissione sull'applicazione del diritto dell'Unione in materia di protezione dei dati nel contesto elettorale Contributo della Commissione europea all'incontro dei leader di Salisburgo del 19-20 settembre 2018, COM(2018) 638 final.

[17] Posizione e conclusioni del Consiglio in merito all'applicazione del regolamento generale sulla protezione dei dati (regolamento generale sulla protezione dei dati): https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/it/pdf.

per la protezione dei dati (di seguito "il comitato")[19] e delle autorità di protezione dei dati personali[20], del gruppo multilaterale di esperti[21] e di altre parti interessate, anche attraverso il riscontro fornito in merito alla tabella di marcia[22].

Secondo l'opinione generale, due anni dopo l'inizio della sua applicazione il regolamento generale sulla protezione dei dati ha conseguito con successo i propri obiettivi di rafforzare la protezione del diritto delle persone fisiche alla protezione dei dati personali e di garantire la libera circolazione dei dati personali all'interno dell'UE[23]. Tuttavia sono stati individuati anche diversi settori da migliorare in futuro. In linea con la maggioranza delle parti interessate e delle autorità di protezione dei dati, la Commissione ritiene che sarebbe prematuro, in questa fase, trarre conclusioni definitive in merito all'applicazione del regolamento generale sulla protezione dei dati. È probabile che la maggior parte delle questioni individuate dagli Stati membri e dalle parti interessate trarrà beneficio da una maggiore esperienza nell'applicazione del regolamento nei prossimi anni. Tuttavia la presente relazione mette in evidenza le difficoltà incontrate finora nell'applicazione del regolamento e illustra modi possibili per affrontarle.

Nonostante l'attenzione sia incentrata sulle due questioni evidenziate dall'articolo 97, paragrafo 2, del regolamento generale sulla protezione dei dati, ossia i trasferimenti internazionali e i meccanismi di cooperazione e coerenza, la presente attività di valutazione e riesame adotta un approccio di più ampio respiro e affronta anche questioni sollevate da vari soggetti nel corso degli ultimi due anni.

2 PRINCIPALI CONCLUSIONI

Applicazione del regolamento generale sulla protezione dei dati e funzionamento dei meccanismi di cooperazione e coerenza

Il regolamento generale sulla protezione dei dati ha istituito un sistema di governance innovativo basato su autorità indipendenti di protezione dei dati negli Stati membri e sulla loro cooperazione nel contesto di casi transfrontalieri e nell'ambito del comitato europeo per la protezione dei dati ("il comitato"). Secondo l'opinione generale le autorità di protezione dei dati hanno esercitato in maniera equilibrata i propri poteri correttivi rafforzati, compresi avvertimenti e ammonimenti, sanzioni e limitazioni temporanee o definitive del trattamento[24]. La Commissione osserva che le autorità

---

[18] Lettera della commissione LIBE (commissione per le libertà civili, la giustizia e gli affari interni) del Parlamento europeo del 21 febbraio 2020 al commissario Reynders, rif.: IPOL-COM-LIBE D (2020)6525.

[19] Contributo del comitato alla valutazione del regolamento generale sulla protezione dei dati ai sensi dell'articolo 97, adottato il 18 febbraio 2020: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en.

[20] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_en.

[21] Il gruppo multilaterale di esperti sul regolamento istituito dalla Commissione coinvolge la società civile nonché rappresentanti delle imprese, il mondo accademico e professionisti del settore: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&Lang=IT.

[22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation/feedback?p_id=7669437.

[23] Cfr. ad esempio la posizione e le conclusioni del Consiglio, nonché il contributo del comitato.

[24] Cfr. la sezione 2.1 del documento di lavoro dei servizi della Commissione.

hanno utilizzato sanzioni amministrative pecuniarie che variano da qualche migliaio a diversi milioni di euro, a seconda della gravità delle violazioni. Altre sanzioni, quali i divieti di trattamento, possono avere un effetto deterrente pari se non persino superiore a quello delle sanzioni pecuniarie. L'obiettivo ultimo del regolamento generale sulla protezione dei dati è quello di modificare la cultura e il comportamento di tutti i soggetti coinvolti a beneficio delle persone fisiche. Informazioni più dettagliate sull'uso dei poteri correttivi da parte delle autorità di protezione dei dati sono presentate nel documento di lavoro dei servizi della Commissione che accompagna la presente relazione.

Sebbene sia ancora presto per valutare pienamente il funzionamento dei nuovi meccanismi di cooperazione e coerenza, le autorità di protezione dei dati hanno sviluppato la loro cooperazione attraverso il meccanismo dello sportello unico[25] e un ampio ricorso all'assistenza reciproca[26]. Si ricorre al meccanismo dello sportello unico, che è una risorsa fondamentale del mercato interno, per decidere numerosi casi transfrontalieri[27]. Sono attualmente pendenti importanti decisioni aventi dimensione transfrontaliera che saranno soggette al meccanismo dello sportello unico. Tali decisioni, che coinvolgono spesso società multinazionali tecnologiche di grandi dimensioni, avranno un impatto sostanziale sui diritti delle persone fisiche in numerosi Stati membri.

Tuttavia lo sviluppo di una cultura europea veramente comune in materia di protezione dei dati tra le autorità di protezione dei dati è un processo ancora in corso. Le autorità di protezione dei dati non si sono ancora pienamente avvalse degli strumenti previsti dal regolamento generale sulla protezione dei dati, quali le operazioni congiunte che potrebbero condurre a indagini congiunte. A volte, la ricerca di un approccio comune ha comportato un avanzamento secondo il denominatore comune più basso e, di conseguenza, non sono state sfruttate le possibilità per promuovere una maggiore armonizzazione[28].

Sono necessari ulteriori progressi per rendere più efficiente e armonizzata la gestione dei casi transfrontalieri in tutta l'UE, anche sotto il profilo procedurale, ad esempio in merito a questioni quali le procedure di trattamento dei reclami, i criteri di ammissibilità per i reclami, la durata dei procedimenti dovuti a scadenze diverse o all'assenza di termini nel diritto processuale amministrativo nazionale, il momento della procedura in cui è concesso il diritto di essere ascoltati o di informazione e la partecipazione, durante il procedimento, di coloro che presentano il reclamo. Il processo di riflessione avviato dal comitato in relazione a questo aspetto è accolto con favore e la Commissione sta partecipando a tali discussioni[29].

---

[25] Se un'impresa tratta dati transfrontalieri, l'autorità di protezione dei dati competente è quella degli Stati membri nei quali detta impresa ha il proprio stabilimento principale.

[26] Cfr. la sezione 2.2 del documento di lavoro dei servizi della Commissione.

[27] Tra il 25 maggio 2018 e il 31 dicembre 2019 sono stati presentati 141 progetti di decisione attraverso la procedura dello sportello unico, 79 dei quali hanno portato a decisioni definitive.

[28] Gli elenchi nazionali dei tipi di trattamento che richiedono una valutazione dell'impatto sulla protezione dei dati ai sensi dell'articolo 35 del regolamento generale sulla protezione dei dati avrebbero potuto ad esempio essere armonizzati meglio.

[29] Cfr. la sezione 2.2 del documento di lavoro dei servizi della Commissione.

Le attività e gli orientamenti del comitato sono di fondamentale importanza per un ulteriore sviluppo coerente degli scambi tra il comitato e le parti interessate[30]. Alla fine del 2019 il comitato aveva adottato 67 documenti tra i quali 10 orientamenti[31] e 43 pareri[32] nuovi. Le parti interessate accolgono in generale con favore gli orientamenti del comitato e ne richiedono ulteriori in merito a concetti chiave del regolamento generale sulla protezione dei dati, tuttavia rilevano anche incongruenze tra gli orientamenti nazionali e quelli del comitato. Sottolineano inoltre la necessità di una consulenza più pratica, in particolare di esempi maggiormente concreti, nonché la necessità che le autorità di protezione dei dati dispongano delle risorse umane, tecniche e finanziarie necessarie per svolgere efficacemente i loro compiti.

La Commissione ha costantemente ribadito l'obbligo per gli Stati membri di destinare risorse umane, finanziarie e tecniche sufficienti alle autorità nazionali di protezione dei dati[33]. La maggior parte delle autorità ha beneficiato di un aumento del personale e del bilancio tra il 2016 e il 2019[34], tra queste le autorità irlandesi, olandesi, islandesi, lussemburghesi e finlandesi hanno beneficiato dei maggiori aumenti relativi in termini di personale. Dato che le grandi multinazionali tecnologiche più importanti sono stabilite in Irlanda e in Lussemburgo, le autorità di protezione dei dati di questi paesi agiscono in qualità di autorità capofila in numerosi casi transfrontalieri significativi e possono necessitare di risorse maggiori rispetto a quanto la loro popolazione suggerirebbe altrimenti. Tuttavia la situazione è ancora disomogenea tra gli Stati membri e non è ancora complessivamente soddisfacente. Le autorità di protezione dei dati svolgono un ruolo essenziale nel garantire che il regolamento generale sulla protezione dei dati sia applicato a livello nazionale e che il meccanismo di cooperazione e coerenza nell'ambito del comitato funzioni in maniera efficace, compreso in particolare il meccanismo dello sportello unico per i casi transfrontalieri. Gli Stati membri sono pertanto invitati a fornire loro risorse adeguate, come previsto dal regolamento generale sulla protezione dei dati[35].

Norme armonizzate, tuttavia persiste un certo grado di frammentazione e approcci divergenti

La Commissione sta monitorando l'attuazione del regolamento generale sulla protezione dei dati nella legislazione nazionale. Al momento della stesura della presente relazione, fatta eccezione per la Slovenia, tutti gli Stati membri hanno adottato una nuova legislazione o adattato il proprio diritto nazionale in materia di

[30] In particolare rappresentanti delle imprese e della società civile. Cfr. la sezione 2.3 del documento di lavoro dei servizi della Commissione.
[31] Tali orientamenti vanno ad aggiungersi ai 10 adottati dal gruppo di lavoro Articolo 29 durante il periodo antecedente l'inizio del periodo di applicazione del regolamento e approvati dal comitato. Il comitato ha inoltre adottato 4 orientamenti supplementari tra gennaio e la fine di maggio del 2020 e ha aggiornato una versione esistente.
[32] 42 di tali pareri sono stati adottati ai sensi dell'articolo 64 del regolamento generale sulla protezione dei dati e uno ai sensi dell'articolo 70, paragrafo 1, lettera s), dello stesso, riguardante la decisione di adeguatezza rispetto al Giappone.
[33] Comunicazione della Commissione al Parlamento europeo e al Consiglio, Le norme sulla protezione dei dati come strumento generatore di fiducia nell'UE e oltre i suoi confini: un bilancio, COM(2019) 374 final del 24.7.2019.
[34] Nel complesso, tra il 2016 e il 2019 si è registrato un aumento del 42 % del personale e del 49 % del bilancio delle autorità nazionali di protezione dei dati.
[35] Cfr. la sezione 2.4 del documento di lavoro dei servizi della Commissione.

protezione dei dati. Alla Slovenia[36] è stato chiesto di fornire chiarimenti alla Commissione in merito alla finalizzazione di tale processo[37].

Il regolamento generale sulla protezione dei dati prevede un approccio coerente per le norme in materia di protezione dei dati in tutta l'UE. Tuttavia impone agli Stati membri di legiferare in taluni settori[38] e fornisce loro la possibilità di specificare ulteriormente il regolamento generale sulla protezione dei dati in altri[39]. Di conseguenza si registra ancora un certo grado di frammentazione, dovuto in particolare all'ampio ricorso a clausole di specificazione facoltative. Ad esempio, la differenza tra gli Stati membri in termini di età del consenso dei minori in relazione ai servizi della società dell'informazione crea incertezza nei minori e nei loro genitori in merito all'applicazione dei loro diritti di protezione dei dati nel mercato unico. Tale frammentazione crea altresì sfide per lo svolgimento di attività commerciali transfrontaliere, per l'innovazione, in particolare per quanto riguarda i nuovi sviluppi tecnologici e le soluzioni di cibersicurezza. Per garantire il funzionamento efficace del mercato interno ed evitare oneri inutili per le imprese, è altresì essenziale che la legislazione nazionale non vada oltre i margini fissati dal regolamento generale sulla protezione dei dati o introduca requisiti supplementari dove non sono presenti margini.

Una sfida specifica per la legislazione nazionale consiste nel conciliare il diritto alla protezione dei dati personali con la libertà di espressione e di informazione e nel corretto bilanciamento di tali diritti. Talune legislazioni nazionali stabiliscono il principio della priorità della libertà di espressione, mentre altre stabiliscono quella della protezione dei dati personali ed esentano dall'applicazione delle norme in materia di protezione dei dati soltanto in situazioni specifiche, come nel caso in cui si tratti di un soggetto pubblico. Infine altri Stati membri prevedono un certo equilibrio da parte del legislatore e/o una valutazione caso per caso per quanto riguarda le deroghe a talune disposizioni del regolamento generale sulla protezione dei dati.

La Commissione proseguirà la propria valutazione della legislazione nazionale. La conciliazione deve essere prevista dalla legge, rispettare il contenuto essenziale di tali diritti fondamentali ed essere proporzionata e necessaria[40]. Le norme in materia di protezione dei dati (nonché la loro interpretazione e applicazione) non dovrebbero incidere sull'esercizio della libertà di espressione e di informazione, ad esempio creando un effetto dissuasivo o esercitando pressioni sui giornalisti affinché divulghino le loro fonti. La definizione di un equilibrio tra tali due diritti da parte delle legislazioni nazionali dovrebbe essere inquadrata dalla giurisprudenza della Corte di giustizia e della Corte europea dei diritti dell'uomo[41].

La legislazione degli Stati membri segue approcci diversi in sede di applicazione delle deroghe al divieto generale di trattare categorie particolari di dati personali, per

[36] Più di recente con una lettera del commissario Reynders nel marzo 2020.
[37] Va osservato che l'autorità nazionale di protezione dei dati in Slovenia è istituita sulla base dell'attuale normativa nazionale in materia di protezione dei dati e vigila sull'applicazione del regolamento generale sulla protezione dei dati in tale Stato membro.
[38] Cfr. la sezione 3.1 del documento di lavoro dei servizi della Commissione.
[39] Cfr. la sezione 3.2 del documento di lavoro dei servizi della Commissione.
[40] Articolo 52, paragrafo 1, della Carta.
[41] Cfr. punto 3.1 del documento di lavoro dei servizi: conciliazione del diritto alla protezione dei dati personali con la libertà di espressione e di informazione.

quanto riguarda il livello di specifiche e garanzie, anche per finalità sanitarie e di ricerca. Per affrontare questo problema, la Commissione sta procedendo innanzitutto alla mappatura dei diversi approcci adottati dagli Stati membri[42] e, come passo ulteriore, sosterrà l'istituzione di codici di condotta che contribuiscano a un approccio più coerente in questo settore e facilitino il trattamento transfrontaliero di dati personali[43]. Inoltre gli orientamenti futuri del comitato sull'uso dei dati personali nel settore della ricerca scientifica contribuiranno a un approccio armonizzato. La Commissione fornirà un contributo al comitato, in particolare per quanto concerne la ricerca sanitaria, anche sotto forma di domande concrete e analisi di scenari specifici che le sono pervenute dalla comunità scientifica.

Dare alle persone gli strumenti d'azione per controllare i propri dati

Secondo un'indagine sui diritti fondamentali[44], il 69 % della popolazione dell'UE di età superiore a 16 anni ha sentito parlare del regolamento generale sulla protezione dei dati e il 71 % delle persone dell'UE conosce la propria autorità nazionale di protezione dei dati.

Le persone sono sempre più consapevoli dei loro diritti: diritti di accesso, rettifica, cancellazione e portabilità dei dati personali, diritto di opposizione al trattamento dei dati personali e maggiore trasparenza. Il regolamento generale sulla protezione dei dati ha rafforzato i diritti procedurali, che comprendono il diritto di proporre reclamo presso un'autorità di protezione dei dati, anche mediante azioni rappresentative, e il diritto al ricorso giurisdizionale. Le persone fisiche si avvalgono sempre più di tali diritti, tuttavia è necessario facilitarne l'esercizio e la piena applicazione. La riflessione condotta dal comitato chiarirà e agevolerà ulteriormente l'esercizio dei diritti da parte delle singole persone, mentre la proposta di direttiva sulle azioni rappresentative[45], una volta adottata, dovrebbe consentire alle persone fisiche di promuovere azioni collettive in tutti gli Stati membri e ridurrà i costi delle azioni transfrontaliere.

Il diritto alla portabilità dei dati presenta il potenziale evidente, non ancora pienamente utilizzato, di mettere le persone fisiche al centro dell'economia dei dati consentendo loro di passare da un fornitore di servizi a un altro, di combinare servizi diversi, di utilizzare altri servizi innovativi e di scegliere i servizi maggiormente rispettosi della protezione dei dati. Ciò favorirà indirettamente la concorrenza e sosterrà l'innovazione. Liberare tale potenziale è una delle priorità della Commissione, in particolare in ragione del fatto che, con il crescente uso dei dispositivi di "Internet delle cose", i consumatori generano una quantità sempre maggiore di dati e rischiano quindi di trovarsi di fronte a pratiche sleali ed effetti di dipendenza. La portabilità

---

[42] La Commissione ha avviato uno studio sulla "*Assessment of the Member States' rules on health data in the light of GDPR*" [Valutazione delle norme degli Stati membri in materia di dati relativi alla salute alla luce del regolamento generale sulla protezione dei dati], Chafea/2018/Health/03, contratto specifico n. 2019 70 01.

[43] Cfr. azioni annunciate nella strategia europea per i dati, pag. 30.

[44] Agenzia dell'Unione europea per i diritti fondamentali (FRA) (2020) - Indagine 2019 sui diritti fondamentali - Protezione dei dati e tecnologia: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection.

[45] Una volta adottata, la proposta di direttiva sulle azioni rappresentative a tutela degli interessi collettivi dei consumatori (COM(2018) 184 final - 2018/089 (COD)) dovrebbe rafforzare il quadro per le azioni rappresentative anche nel settore della protezione dei dati.

potrebbe generare benefici significativi in termini di salute e benessere, riduzione dell'impronta ambientale, accesso a servizi pubblici e privati, aumento della produttività nella fabbricazione e incremento della qualità e della sicurezza dei prodotti.

La strategia in materia di dati ha sottolineato la necessità di affrontare difficoltà quali la mancanza di norme che consentano la fornitura di dati in un formato leggibile da un dispositivo automatico e di aumentare il ricorso effettivo al diritto alla portabilità dei dati, attualmente limitato a pochi settori (ad esempio, banche e telecomunicazioni). Ciò potrebbe essere realizzato in particolare mediante la progettazione di strumenti adeguati e di formati e interfacce standardizzati[46]. Tale maggiore uso potrebbe essere conseguito, in particolare, mediante l'obbligo di installare interfacce tecniche e formati leggibili da un dispositivo automatico che consentano la portabilità dei dati in tempo reale. Un maggiore ricorso al diritto alla portabilità potrebbe, tra l'altro, rendere più semplice per le persone fisiche dare l'autorizzazione all'utilizzo dei propri dati per il bene comune (ad esempio per promuovere la ricerca nel settore sanitario), qualora lo desiderino ("altruismo dei dati"). In preparazione del pacchetto relativo alla legge sui servizi digitali[47], la Commissione esaminerà più in generale il ruolo dei dati e delle pratiche relative ai dati nell'ecosistema delle piattaforme.

Opportunità e sfide per le organizzazioni, in particolare per le piccole e medie imprese

Il regolamento generale sulla protezione dei dati, unitamente al regolamento sulla libera circolazione dei dati non personali[48], offre opportunità alle imprese promuovendo la concorrenza e l'innovazione, garantendo la libera circolazione dei dati all'interno dell'UE e creando parità di condizioni con le imprese stabilite al di fuori dell'UE[49]. Il diritto alla portabilità, associato a un numero crescente di persone fisiche alla ricerca di soluzioni maggiormente rispettose della vita privata, potrebbe ridurre gli ostacoli all'ingresso da parte delle imprese e offrire possibilità di crescita basate sulla fiducia e sull'innovazione. Talune parti interessate hanno riferito che l'applicazione del regolamento generale sulla protezione dei dati è complessa, in particolare per le piccole e medie imprese (PMI). Secondo l'approccio basato sul rischio, non sarebbe opportuno prevedere deroghe in base alle dimensioni degli operatori, poiché le loro dimensioni non costituiscono di per sé un'indicazione dei rischi che il trattamento dei dati personali che essi intraprendono possa comportare per le persone fisiche. Diverse autorità di protezione dei dati hanno fornito strumenti pratici per facilitare l'attuazione del regolamento generale sulla protezione dei dati da parte delle PMI che svolgono attività di trattamento a basso rischio. Tali sforzi

[46] Tali strumenti possono comprendere strumenti di gestione del consenso e app per la gestione delle informazioni personali.
[47] https://ec.europa.eu/commission/presscorner/detail/it/ip_20_962.
[48] Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea (GU L 303 del 28.11.2018, pag. 59).
[49] Cfr. la sezione 5 del documento di lavoro dei servizi della Commissione. Cfr. anche il documento COM(2019) 250 final "Orientamenti sul regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea", che illustra le norme che disciplinano il trattamento di serie di dati miste, composte da dati tanto personali quanto non personali, rendendolo pratico per le imprese, comprese le PMI.

dovrebbero essere intensificati e diffusi, preferibilmente nel contesto di un approccio europeo comune al fine di non creare ostacoli al mercato unico.

Le autorità di protezione dei dati hanno sviluppato una serie di attività per aiutare le PMI a rispettare il regolamento generale sulla protezione dei dati, ad esempio attraverso la predisposizione di modelli per i contratti di trattamento e le registrazioni delle attività di trattamento, seminari e linee telefoniche dirette per la consultazione. Numerose di tali iniziative hanno beneficiato di finanziamenti dell'UE[50]. Si dovrebbero prendere in considerazione ulteriori attività destinate a facilitare l'applicazione del regolamento generale sulla protezione dei dati per le PMI.

Il regolamento generale sulla protezione dei dati mette a disposizione di tutti i tipi di imprese e organizzazioni un insieme di strumenti con l'obiettivo di aiutarle a dimostrare la conformità, ad esempio codici di condotta, meccanismi di certificazione e clausole contrattuali tipo. Tale insieme di strumenti dovrebbe essere sfruttato appieno. Le PMI sottolineano in particolare l'importanza e l'utilità dei codici di condotta adattati alla loro situazione e che non comportano costi sproporzionati. Per quanto concerne i sistemi di certificazione, la sicurezza (compresa la cibersicurezza) e la protezione dei dati fin dalla progettazione, si tratta di elementi chiave da considerare nel quadro del regolamento generale sulla protezione dei dati che trarrebbero vantaggio da un approccio comune e ambizioso in tutta l'UE. La Commissione sta attualmente lavorando a clausole contrattuali tipo tra i titolari del trattamento e i responsabili del trattamento[51], sulla base dei lavori in corso per la modernizzazione delle clausole contrattuali tipo per i trasferimenti internazionali[52].

Applicazione del regolamento generale sulla protezione dei dati alle nuove tecnologie

Il regolamento generale sulla protezione dei dati, essendo stato concepito in modo tecnologicamente neutro, si basa su principi ed è pertanto progettato per coprire le nuove tecnologie man mano che si sviluppano.

È considerato uno strumento essenziale e flessibile per garantire che lo sviluppo di tecnologie nuove sia conforme ai diritti fondamentali. Il quadro legislativo in materia di protezione dei dati e di tutela della vita privata ha dimostrato la propria importanza e la propria flessibilità durante la crisi del Covid-19, in particolare per quanto concerne la progettazione delle applicazioni di tracciamento e altre soluzioni tecnologiche per contrastare la pandemia. Si prospettano sfide future per chiarire come applicare i principi comprovati a tecnologie specifiche quali l'intelligenza artificiale, la blockchain, l'Internet delle cose o il riconoscimento facciale, che richiedono un monitoraggio continuo. Il Libro bianco della Commissione sull'intelligenza artificiale[53] ha aperto ad esempio un dibattito pubblico sulle eventuali

[50] La Commissione ha fornito sostegno finanziario attraverso tre ondate di sovvenzioni, per un importo totale di 5 milioni di EUR, nel contesto delle quali le due più recenti sono state specificamente destinate a sostenere le autorità nazionali di protezione dei dati nei loro sforzi per raggiungere le persone fisiche e le piccole e medie imprese: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_it. Nel 2020 sarà stanziato un ulteriore milione di EUR.

[51] Ai sensi dell'articolo 28 del regolamento generale sulla protezione dei dati.

[52] Ai sensi dell'articolo 46 del regolamento generale sulla protezione dei dati.

[53] Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia, COM(2020) 65 final.

circostanze specifiche che potrebbero giustificare il ricorso all'intelligenza artificiale per finalità di identificazione biometrica a distanza (quali il riconoscimento facciale) nei luoghi pubblici, nonché sulle garanzie comuni. A tale riguardo, le autorità di protezione dei dati dovrebbero essere pronte ad accompagnare i processi tecnici di progettazione in una fase precoce.

Inoltre, l'applicazione rigorosa ed efficace del regolamento generale sulla protezione dei dati nei confronti delle piattaforme digitali e delle imprese integrate di grandi dimensioni, anche in settori quali la pubblicità online e il micro-targeting, è un aspetto essenziale ai fini della protezione delle persone fisiche.

Sviluppare un insieme di strumenti moderni per il trasferimento internazionale di dati

Il regolamento generale sulla protezione dei dati mette a disposizione una serie di strumenti modernizzati per facilitare il trasferimento di dati personali dall'UE verso un paese terzo o un'organizzazione internazionale, garantendo nel contempo che i dati continuino a beneficiare di un livello elevato di protezione. Negli ultimi due anni la Commissione ha intensificato i propri sforzi per sfruttare appieno il potenziale degli strumenti disponibili nel quadro del regolamento generale sulla protezione dei dati.

Ciò ha incluso partecipare attivamente al dialogo con i principali partner al fine di giungere a una "decisione di adeguatezza". L'effetto di tale decisione è consentire la libera circolazione sicura dei dati personali verso il paese terzo in questione senza che l'esportatore dei dati debba fornire ulteriori garanzie o ottenere alcuna autorizzazione. In particolare, le decisioni di adeguatezza reciproca UE-Giappone, che sono entrate in vigore nel febbraio 2019, hanno creato il più grande spazio al mondo per flussi di dati liberi e sicuri. Inoltre il processo di adeguatezza con la Repubblica di Corea è in fase avanzata, mentre sono in corso colloqui esplorativi con altri importanti partner in Asia e in America latina.

Anche l'adeguatezza svolge un ruolo importante nel contesto delle future relazioni con il Regno Unito, purché siano soddisfatte le condizioni applicabili. Costituisce un fattore abilitante per il commercio, compreso il commercio digitale, e costituisce un presupposto essenziale per una cooperazione stretta e ambiziosa nel settore dell'applicazione della legge e della sicurezza. Inoltre un grado elevato di convergenza nella protezione dei dati costituisce un aspetto importante per garantire parità di condizioni tra due economie fortemente integrate. In linea con la dichiarazione politica sulle relazioni future tra l'UE e il Regno Unito, la Commissione sta attualmente effettuando una valutazione dell'adeguatezza a norma del regolamento generale sulla protezione dei dati e della direttiva sulla protezione dei dati riguardo al trattamento da parte delle autorità di contrasto[54].

Nel quadro della prima valutazione del regolamento generale sulla protezione dei dati, la Commissione è altresì tenuta a riesaminare le decisioni di adeguatezza adottate in

[54] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

conformità con la normativa precedente[55]. I servizi della Commissione hanno avviato un dialogo intenso con ciascuno degli 11 territori e paesi terzi interessati[56] al fine di valutare in che modo i loro sistemi di protezione dei dati si sono evoluti dall'adozione della decisione di adeguatezza e se soddisfano le prescrizioni stabilite dal regolamento generale sulla protezione dei dati. La necessità di garantire la continuità di tali decisioni, quale strumento fondamentale per il commercio e la cooperazione internazionale, è uno dei fattori che hanno spinto numerosi di tali paesi e territori a modernizzare e rafforzare la loro legislazione in materia di tutela della vita privata. Ulteriori garanzie sono in fase di discussione con taluni di questi paesi e territori per affrontare le differenze di protezione pertinenti. Tuttavia dato che, in una sentenza che sarà pronunciata il 16 luglio, la Corte di giustizia può fornire chiarimenti che potrebbero essere pertinenti per determinati aspetti del criterio di adeguatezza, la Commissione riferirà separatamente sulla valutazione delle decisioni di adeguatezza esistenti in seguito alla pronuncia della sentenza della Corte di giustizia in tale causa[57].

Oltre al suo lavoro sull'adeguatezza, la Commissione sta lavorando a una modernizzazione globale delle clausole contrattuali tipo, al fine di aggiornarle alla luce delle nuove prescrizioni introdotte dal regolamento generale sulla protezione dei dati. L'obiettivo è rispecchiare meglio le realtà dei trattamenti nell'economia digitale moderna e considerare l'eventuale necessità di chiarire ulteriormente talune garanzie, anche alla luce dell'imminente giurisprudenza della Corte di giustizia[58]. Tali clausole rappresentano il meccanismo di trasferimento dei dati di gran lunga più diffuso, con migliaia di imprese europee che fanno affidamento su di esse al fine di fornire un'ampia gamma di servizi ai propri clienti, fornitori, partner e dipendenti.

Il comitato ha inoltre svolto un ruolo attivo nello sviluppo degli aspetti internazionali del regolamento generale sulla protezione dei dati. Rientra in tale contesto l'aggiornamento degli orientamenti sui meccanismi di trasferimento esistenti, quali le norme vincolanti d'impresa e le cosiddette "deroghe", nonché lo sviluppo dell'infrastruttura giuridica per l'uso di nuovi strumenti introdotti dal regolamento generale sulla protezione dei dati, ossia i codici di condotta e la certificazione.

Al fine di consentire alle parti interessate di avvalersi appieno dell'insieme degli strumenti di trasferimento messi a disposizione dal regolamento generale sulla protezione dei dati, è importante che il comitato intensifichi i lavori in corso sui vari meccanismi di trasferimento, anche semplificando ulteriormente il processo di approvazione delle norme vincolanti d'impresa, mettendo a punto gli orientamenti sui codici di condotta e di certificazione come strumenti per i trasferimenti, e chiarendo l'interazione tra le norme sui trasferimenti internazionali di dati (capo V) e l'ambito di

---

[55] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

[56] Tali paesi e territorio sono: Andorra, Argentina, Canada, Isole Fær Øer, Guernsey, Jersey, Isola di Man, Israele, Nuova Zelanda, Svizzera e Uruguay.

[57] Cfr. causa C-311/18, *Garante per la protezione dei dati personali/Facebook Ireland Limited, Maximillian Schrems* ("Schrems II"), che riguarda una domanda di pronuncia pregiudiziale sulle cosiddette clausole contrattuali tipo. Tuttavia la Corte potrà chiarire ulteriormente anche taluni aspetti del criterio di adeguatezza.

[58] Cfr. causa Schrems II.

applicazione territoriale (articolo 3) del regolamento generale sulla protezione dei dati.

Un altro aspetto importante della dimensione internazionale delle norme dell'UE in materia di protezione dei dati è l'ambito di applicazione territoriale di maggiore portata del regolamento generale sulla protezione dei dati che comprende anche le attività di trattamento di operatori stranieri attivi sul mercato dell'UE. Al fine di garantire l'effettivo rispetto del regolamento generale sulla protezione dei dati e una reale parità di condizioni, è essenziale che tale ampliamento di portata si rifletta adeguatamente nelle azioni di esecuzione attuate dalle autorità di protezione dei dati. In particolare, ove necessario, tali autorità dovrebbero coinvolgere il titolare del trattamento o il responsabile del trattamento nell'UE, al quale ci si può rivolgere in aggiunta o in sostituzione dell'impresa con sede al di fuori dell'UE. Tale approccio dovrebbe essere perseguito con maggiore vigore al fine di inviare un messaggio chiaro che la mancanza di uno stabilimento nell'UE non esonera gli operatori stranieri dalle loro responsabilità ai sensi del regolamento generale sulla protezione dei dati.

Promozione della convergenza e cooperazione internazionale in materia di protezione dei dati

Il regolamento generale sulla protezione dei dati si è già rivelato un punto di riferimento fondamentale a livello internazionale e ha svolto un ruolo di catalizzatore per numerosi paesi in tutto il mondo al fine di prendere in considerazione l'introduzione di norme moderne sulla tutela della vita privata. Tale tendenza verso la convergenza globale è uno sviluppo molto positivo che offre nuove opportunità per proteggere meglio le persone fisiche nell'UE quando i loro dati vengono trasferiti all'estero, facilitando nel contempo i flussi di dati.

Sulla base di tale tendenza, la Commissione ha intensificato il proprio dialogo in una serie di consessi bilaterali, regionali e multilaterali al fine di promuovere una cultura globale di rispetto della vita privata e di sviluppare elementi di convergenza tra sistemi diversi di tutela della vita privata. Nei suoi sforzi, la Commissione si è basata e continuerà a fare affidamento sul sostegno attivo del servizio europeo per l'azione esterna e della rete delle delegazioni dell'UE in paesi terzi e delle missioni presso organizzazioni internazionali. Ciò ha consentito inoltre una maggiore coerenza e complementarità tra i diversi aspetti della dimensione esterna delle politiche dell'UE, dal commercio al nuovo partenariato UE-Africa. Anche il G20 e il G7 hanno recentemente riconosciuto il contributo della protezione dei dati alla fiducia nell'economia digitale e ai flussi di dati, in particolare attraverso il concetto di "*Data Free Flow with Trust*" (libera circolazione dei dati con fiducia), originariamente proposto dalla presidenza giapponese del G20[59]. La strategia in materia di dati mette in evidenza l'intenzione della Commissione di continuare a promuovere la condivisione dei dati con partner di fiducia, contrastando nel contempo gli abusi quali un accesso sproporzionato delle autorità pubbliche (straniere) ai dati personali.

Pur promuovendo la convergenza delle norme in materia di protezione dei dati a livello internazionale, in modo da facilitare i flussi di dati e, di conseguenza, gli

[59] Cfr. ad es. testo della dichiarazione dei leader del G20 di Osaka: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

scambi, la Commissione è anche determinata ad affrontare il protezionismo digitale, come recentemente sottolineato nella strategia in materia di dati[60]. A tal fine, ha messo a punto disposizioni specifiche sui flussi di dati e sulla protezione dei dati negli accordi commerciali[61] che presenta sistematicamente nei suoi negoziati bilaterali (più recentemente con Australia, Nuova Zelanda e Regno Unito) e multilaterali come nel caso degli attuali colloqui sul commercio elettronico dell'OMC[62]. Tali disposizioni orizzontali escludono restrizioni ingiustificate, quali le prescrizioni che impongono la localizzazione forzata dei dati, preservando nel contempo l'autonomia di regolamentazione delle parti al fine di tutelare il diritto fondamentale alla protezione dei dati.

Occorre pertanto esplorare ulteriormente le sinergie tra gli strumenti per il commercio e quelli per la protezione dei dati al fine di garantire flussi internazionali di dati liberi e sicuri che sono essenziali per le attività commerciali, la competitività e la crescita delle imprese europee, comprese le PMI, in un'economia sempre più digitalizzata.

Analogamente è importante garantire che, se invitate a condividere dati per finalità di contrasto sulla base di una richiesta legittima, le imprese attive nel mercato europeo possano farlo senza dover affrontare conflitti di legge e nel pieno rispetto dei diritti fondamentali dell'UE. Per questo motivo la Commissione è impegnata a sviluppare quadri giuridici appropriati con i suoi partner internazionali al fine di evitare conflitti di legge e sostenere tali forme efficaci di cooperazione, in particolare prevedendo le necessarie garanzie in materia di protezione dei dati, contribuendo così a una lotta maggiormente efficace contro la criminalità.

Infine, in un momento in cui le questioni relative al rispetto della vita privata o a incidenti di sicurezza relativi ai dati possono colpire un gran numero di persone fisiche contemporaneamente in più giurisdizioni, è opportuno rafforzare ulteriormente la cooperazione "sul campo" tra le autorità di regolamentazione europee e internazionali. In particolare, ciò richiede lo sviluppo di strumenti giuridici adeguati per consentire forme più strette di cooperazione e di assistenza reciproca, anche consentendo gli scambi di informazioni necessari nel contesto delle indagini. È sempre in tale spirito che la Commissione sta istituendo una "Accademia sulla protezione dei dati", una piattaforma nella quale le autorità di protezione dei dati dell'UE e straniere possano condividere conoscenze, esperienze e migliori pratiche con l'obiettivo di facilitare e sostenere la cooperazione tra le autorità preposte a far rispettare le norme in materia di tutela della vita privata.

---

[60] Strategia in materia di dati, pag. 23.

[61] Cfr. testo delle disposizioni orizzontali per i flussi di dati transfrontalieri e per la protezione dei dati personali (negli accordi commerciali e di investimento dell'UE): https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf.

[62] 84 membri dell'OMC sono attualmente impegnati in negoziati plurilaterali sul commercio elettronico, a seguito di una dichiarazione congiunta adottata dai ministri il 25 gennaio 2019 a Davos. Nel contesto di tale processo, il 3 maggio 2019 l'UE ha presentato la propria proposta di testo sulle norme e sugli obblighi futuri in materia di commercio elettronico. La proposta comprende disposizioni orizzontali sui flussi di dati e sulla protezione dei dati personali: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

3 AZIONI FUTURE

Al fine di realizzare il pieno potenziale del regolamento generale sulla protezione dei dati, è importante creare un approccio armonizzato e una cultura europea comune della protezione dei dati, nonché promuovere una gestione maggiormente efficiente ed armonizzata dei casi transfrontalieri. Ciò rientra nelle aspettative di persone e imprese e costituisce un obiettivo essenziale della riforma delle norme dell'UE in materia di protezione dei dati. È altrettanto importante assicurare che tutti gli strumenti disponibili nel regolamento generale sulla protezione dei dati siano utilizzati appieno al fine di garantire un'applicazione efficace per le persone fisiche e le imprese.

La Commissione proseguirà i propri scambi bilaterali con gli Stati membri sull'attuazione del regolamento generale sulla protezione dei dati e, se necessario, continuerà a utilizzare tutti gli strumenti a sua disposizione per promuovere il rispetto da parte degli Stati membri degli obblighi loro imposti dal regolamento generale sulla protezione dei dati.

Data la valutazione in corso della legislazione nazionale, il breve periodo di esperienza pratica dall'inizio dell'applicazione del regolamento generale sulla protezione dei dati e il fatto che la legislazione settoriale è ancora in fase di riesame in numerosi Stati membri, è ancora troppo presto per trarre conclusioni definitive sull'attuale livello di frammentazione. Per quanto concerne il possibile conflitto di legge dovuto all'attuazione da parte degli Stati membri di clausole di specificazione, è innanzitutto necessario comprendere meglio le conseguenze per i titolari e i responsabili del trattamento[63].

Nel dare seguito a tali questioni, la giurisprudenza pertinente degli organi giurisdizionali nazionali e della Corte di giustizia contribuisce a creare un'interpretazione coerente delle norme in materia di protezione dei dati. Gli organi giurisdizionali nazionali hanno recentemente emesso sentenze che annullano le disposizioni contenute nelle legislazioni nazionali che si discostano dal regolamento generale sulla protezione dei dati[64].

Per quanto concerne la dimensione internazionale, la Commissione continuerà a concentrarsi sulla promozione della convergenza delle norme in materia di protezione dei dati al fine di garantire flussi di dati sicuri. Ciò comprende varie forme di lavoro "a monte", ad esempio nel contesto delle riforme in corso per definire leggi nuove o aggiornate in materia di protezione dei dati oppure la spinta a sostegno del concetto di "*Data Free Flow with Trust*" nei consessi multilaterali. Riguarda inoltre numerosi dialoghi in materia di adeguatezza e la modernizzazione e l'ampliamento dell'insieme di strumenti dell'UE per il trasferimento attraverso l'aggiornamento delle clausole contrattuali tipo e la creazione di basi per meccanismi di certificazione. Tale lavoro comprende anche i negoziati internazionali, ad esempio nel settore dell'accesso transfrontaliero alle prove elettroniche, al fine di garantire che i trasferimenti di dati avvengano con adeguate garanzie in materia di protezione dei dati. Infine,

[63] Cfr. posizione e conclusioni del Consiglio relative all'applicazione del regolamento generale sulla protezione dei dati.
[64] Ciò è avvenuto in Germania e in Spagna, oppure in Austria, colmando una lacuna nella legislazione nazionale.

nell'impegnarsi in negoziati sulla cooperazione internazionale e sull'assistenza reciproca tra autorità preposte a far rispettare le norme in materia di protezione dei dati, la Commissione si adopererà per realizzare la convergenza "dalla teoria alla pratica".

Sulla base di tale valutazione dell'applicazione del regolamento generale sulla protezione dei dati dal maggio 2018, le azioni elencate in appresso sono state ritenute necessarie per sostenerne l'applicazione. La Commissione ne monitorerà l'attuazione anche in vista della prossima relazione di valutazione del 2024.

Attuazione e integrazione del quadro giuridico

Gli Stati membri dovrebbero:

- completare l'allineamento delle rispettive leggi settoriali al regolamento generale sulla protezione dei dati;
- prendere in considerazione la possibilità di limitare l'uso di clausole di specificazione che potrebbero creare frammentazione e compromettere la libera circolazione dei dati all'interno dell'UE;
- valutare se il diritto nazionale che attua il regolamento generale sulla protezione dei dati rientri sempre all'interno dei margini previsti dalla legislazione degli Stati membri.

La Commissione intende:

- proseguire gli scambi bilaterali con gli Stati membri in materia di conformità delle legislazioni nazionali rispetto al regolamento generale sulla protezione dei dati, nonché in materia di indipendenza e risorse delle autorità nazionali di protezione dei dati; utilizzare tutti gli strumenti a sua disposizione, comprese le procedure di infrazione, per garantire che gli Stati membri rispettino il regolamento generale sulla protezione dei dati;
- sostenere ulteriori scambi di opinioni e pratiche nazionali tra Stati membri su temi che sono soggetti a ulteriore specificazione a livello nazionale, come il trattamento di dati personali relativi alla salute e alla ricerca, in maniera da ridurre il livello di frammentazione del mercato unico, o che sono soggetti a un equilibrio con altri diritti, come ad esempio la libertà di espressione;
- 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;
- ricorrere al gruppo di esperti degli Stati membri del regolamento generale sulla protezione dei dati (istituito durante la fase transitoria prima che il regolamento diventasse applicabile) con l'obiettivo di agevolare il dibattito e la condivisione di esperienze tra gli Stati membri e con la Commissione;
- valutare se, alla luce di ulteriori esperienze e della giurisprudenza pertinente, potrebbe essere opportuno proporre modifiche future mirate a talune disposizioni del regolamento generale sulla protezione dei dati, in particolare per quanto riguarda i registri delle attività di trattamento da parte delle PMI per le quali il trattamento dei dati personali non costituisce l'attività principale

(basso rischio)[65] e per quanto concerne la possibile armonizzazione dell'età del consenso dei minori in relazione ai servizi della società dell'informazione.

Fare in modo che il nuovo sistema di governance realizzi appieno il proprio potenziale

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

- sviluppare accordi efficienti tra autorità di protezione dei dati per quanto riguarda il funzionamento del meccanismo di cooperazione e di coerenza, anche per quanto riguarda gli aspetti procedurali, basandosi sulle competenze dei suoi membri e rafforzando il coinvolgimento del segretariato del comitato;
- sostenere l'armonizzazione nell'applicazione e nell'esecuzione del regolamento generale sulla protezione dei dati utilizzando tutti i mezzi a loro disposizione, anche chiarendo ulteriormente i concetti chiave del regolamento generale sulla protezione dei dati, e garantendo che gli orientamenti nazionali siano pienamente in linea con quelli adottati dal comitato;
- incoraggiare l'uso di tutti gli strumenti previsti dal regolamento generale sulla protezione dei dati al fine di garantirne un'applicazione coerente;
- intensificare la cooperazione tra le autorità di protezione dei dati, ad esempio conducendo indagini congiunte.

La Commissione intende:

- continuare a monitorare attentamente l'indipendenza effettiva e assoluta delle autorità nazionali di protezione dei dati;
- incoraggiare la cooperazione tra le autorità di regolamentazione (in particolare in settori quali la concorrenza, le comunicazioni elettroniche, la sicurezza delle reti e dei sistemi informatici e la politica dei consumatori);
- sostenere la riflessione in seno al comitato in merito alle procedure applicate dalle autorità nazionali di protezione dei dati al fine di migliorare la cooperazione sui casi transfrontalieri.

Gli Stati membri:

- assegneranno alle autorità di protezione dei dati risorse sufficienti a consentire a queste ultime di svolgere i loro compiti.

Sostegno a favore delle parti interessate

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

- adottare ulteriori orientamenti pratici, di facile comprensione, e che forniscano risposte chiare nonché ad evitare ambiguità sulle questioni relative all'applicazione del regolamento generale sulla protezione dei dati, ad esempio in materia di trattamento di dati di minori e di diritti degli interessati,

[65] Articolo 30, paragrafo 5, del regolamento generale sulla protezione dei dati.

compreso l'esercizio del diritto di accesso e del diritto di cancellazione, consultando le parti interessate nel processo;

- riesaminare gli orientamenti qualora siano necessari ulteriori chiarimenti alla luce dell'esperienza e degli sviluppi, anche nella giurisprudenza della Corte di giustizia;
- sviluppare strumenti pratici, quali moduli armonizzati per le violazioni dei dati e registri semplificati delle attività di trattamento, in maniera da aiutare le PMI a basso rischio a soddisfare i propri obblighi.

La Commissione intende:

- mettere a disposizione clausole contrattuali tipo tanto per i trasferimenti internazionali quanto per il rapporto tra titolare e responsabile del trattamento;
- fornire strumenti per chiarire/sostenere l'applicazione delle norme in materia di protezione dei dati rispetto ai minori[66];
- in linea con la strategia in materia di dati, esplorare mezzi pratici per facilitare un maggiore uso del diritto alla portabilità da parte delle persone fisiche, conferendo loro ad esempio un maggiore controllo su chi può accedere ai dati generati automaticamente e utilizzarli;
- sostenere la standardizzazione/certificazione in particolare in merito ad aspetti di cibersicurezza attraverso la cooperazione tra l'agenzia dell'Unione europea per la cibersicurezza (ENISA), le autorità di protezione dei dati e il comitato;
- se del caso, avvalersi del proprio diritto di chiedere al comitato di redigere orientamenti e pareri su questioni specifiche di importanza per le parti interessate;
- se necessario, fornire orientamenti, nel pieno rispetto del ruolo del comitato;
- sostenere le attività delle autorità di protezione dei dati che facilitano l'attuazione degli obblighi del regolamento generale sulla protezione dei dati da parte delle PMI, attraverso il sostegno finanziario, in particolare per gli orientamenti pratici e gli strumenti digitali che possono essere replicati in altri Stati membri.

Incentivazione dell'innovazione

La Commissione intende:

- monitorare l'applicazione del regolamento generale sulla protezione dei dati alle nuove tecnologie, anche tenendo conto di eventuali future iniziative nel settore dell'intelligenza artificiale e nel contesto della strategia in materia di dati;

[66] Progetto della Commissione in materia di strumenti per l'identificazione dell'età – progetto pilota per la dimostrazione di un'infrastruttura tecnica interoperabile per la protezione dei minori, comprensivo di verifica dell'età e consenso da parte dei genitori. Si prevede che ciò sostenga l'attuazione dei meccanismi di protezione dei minori sulla base della legislazione vigente dell'UE in materia di protezione dei minori online.

- incoraggiare, anche attraverso il sostegno finanziario, la redazione di codici di condotta dell'UE in materia di salute e ricerca;
- seguire da vicino lo sviluppo e l'uso di app nel contesto della pandemia di Covid-19.

Il comitato è invitato a:

- pubblicare orientamenti sull'applicazione del regolamento generale sulla protezione dei dati nel settore della ricerca scientifica, dell'intelligenza artificiale, della blockchain e di eventuali altri sviluppi tecnologici;
- riesaminare gli orientamenti qualora siano necessari ulteriori chiarimenti alla luce degli sviluppi tecnologici.

Ulteriore sviluppo dell'insieme di strumenti per il trasferimento di dati

La Commissione intende:

- proseguire i dialoghi sull'adeguatezza con i paesi terzi interessati, in linea con la strategia illustrata nella sua comunicazione del 2017 intitolata "Scambio e protezione dei dati personali in un mondo globalizzato" anche, ove possibile, trattando i trasferimenti di dati ad autorità di contrasto in materia penale (ai sensi della direttiva sulla protezione dei dati riguardo al trattamento da parte delle autorità di contrasto) e altre autorità pubbliche; ciò comprende la finalizzazione il prima possibile del processo di adeguatezza con la Repubblica di Corea;
- finalizzare la valutazione in corso delle decisioni esistenti in materia di adeguatezza e riferire al Parlamento europeo e al Consiglio;
- portare a termine i lavori concernenti la modernizzazione delle clausole contrattuali tipo, al fine di aggiornarle alla luce del regolamento generale sulla protezione dei dati, in maniera da trattare tutti gli scenari di trasferimento pertinenti e rispecchiare meglio le pratiche commerciali moderne.

Il comitato è invitato a:

- chiarire ulteriormente l'interazione tra le norme sui trasferimenti internazionali di dati (capo V) con l'ambito di applicazione territoriale del regolamento generale sulla protezione dei dati (articolo 3);
- garantire l'effettiva applicazione nei confronti degli operatori stabiliti in paesi terzi che rientrano nell'ambito di applicazione territoriale del regolamento generale sulla protezione dei dati, anche per quanto riguarda la nomina di un rappresentante, se del caso (articolo 27);
- ottimizzare la valutazione e l'eventuale approvazione di norme vincolanti d'impresa al fine di accelerare il processo;
- completare i lavori sull'architettura, sulle procedure e sui criteri di valutazione per i codici di condotta e i meccanismi di certificazione come strumenti per i trasferimenti di dati.

Promozione della convergenza e sviluppo della cooperazione internazionale

La Commissione intende:

- sostenere i processi di riforma in corso nei paesi terzi su norme nuove o modernizzate in materia di protezione dei dati attraverso la condivisione di esperienze e migliori pratiche;
- avviare un dialogo con i partner africani per promuovere la convergenza normativa e sostenere lo sviluppo di capacità delle autorità di controllo nel contesto del capitolo digitale del nuovo partenariato UE-Africa;
- valutare le possibilità di agevolazione della cooperazione tra operatori privati e autorità di contrasto, anche negoziando quadri bilaterali e multilaterali per il trasferimento di dati nel contesto dell'accesso a prove elettroniche da parte di autorità straniere di contrasto in materia penale, in maniera da evitare conflitti di legge, assicurando nel contempo adeguate garanzie in materia di protezione dei dati;
- avviare un dialogo con organizzazioni internazionali e regionali quali l'OCSE, l'ASEAN o il G20 con l'obiettivo di promuovere flussi di dati affidabili basati su livelli elevati di protezione dei dati, anche nel contesto dell'iniziativa "*Data Flow with Trust*";
- istituire una "Accademia sulla protezione dei dati" per facilitare e sostenere gli scambi tra le autorità di regolamentazione europee e internazionali;
- promuovere la cooperazione internazionale in materia di applicazione tra le autorità di controllo, anche attraverso la negoziazione di accordi di cooperazione e di assistenza reciproca.