Consiglio
dell'Unione europea

Bruxelles, 29 luglio 2019
(OR. en)

11535/19

JAI 851
DAPIX 252
DATAPROTECT 190
RELEX 753
FREMP 106
DIGIT 129

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	25 luglio 2019
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2019) 374 final
Oggetto:	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

Si trasmette in allegato, per le delegazioni, il documento COM(2019) 374 final.

All.: COM(2019) 374 final

COMMISSIONE
EUROPEA

Bruxelles, 24.7.2019
COM(2019) 374 final

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

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

I. Introduzione

Il regolamento generale sulla protezione dei dati[1] (in appresso "regolamento") si applica in tutta l'Unione europea da oltre un anno. È al centro di un quadro dell'UE coerente e modernizzato in materia di protezione dei dati, che comprende anche la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie[2] e il regolamento sulla protezione dei dati per le istituzioni e gli organi dell'UE[3]. Tale quadro sarà completato dal regolamento sulla vita privata e le comunicazioni elettroniche, attualmente in iter legislativo.

Per garantire il diritto fondamentale alla protezione dei dati personali sono indispensabili norme rigorose in materia di protezione dei dati. Tali norme sono essenziali in una società democratica[4] e costituiscono una componente importante di un'economia sempre più basata sui dati. L'UE aspira a cogliere le numerose opportunità offerte dalla trasformazione digitale in termini di servizi, posti di lavoro e innovazione, affrontando al tempo stesso le sfide che esse comportano. Il furto di identità, la fuga di dati sensibili, la discriminazione di persone, le distorsioni intrinseche, la condivisione di contenuti illegali e lo sviluppo di strumenti di sorveglianza intrusivi sono soltanto alcuni esempi di problematiche che sono sempre più presenti nel dibattito pubblico e in relazione alle quali è evidente che le persone si aspettano che i loro dati siano protetti.

La protezione dei dati è diventata una questione realmente globale, dato che in tutto il mondo le persone tengono in gran conto e apprezzano sempre di più la protezione e la sicurezza dei loro dati. Numerosi paesi hanno adottato o stanno per adottare norme esaustive in materia di

---

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 (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1): https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679.

2 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): https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=celex:32016L0680. Il termine per il recepimento della direttiva da parte degli Stati membri è scaduto il 6 maggio 2018. Le relazioni sull'Unione della sicurezza illustrano lo stato di avanzamento del recepimento.

3 Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39): https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32018R1725. Il regolamento è entrato in vigore l'11 dicembre 2018.

4 La Corte suprema indiana, in una sentenza storica del 24 agosto 2017, ha riconosciuto la tutela della vita privata come un diritto fondamentale, un "aspetto essenziale della dignità dell'essere umano".

protezione dei dati basate su principi analoghi a quelli del regolamento, circostanza questa che ha portato a una convergenza globale delle norme di protezione dei dati. Ciò offre nuove opportunità per facilitare i flussi di dati, tra operatori commerciali o autorità pubbliche, migliorando al tempo stesso il livello di protezione dei dati personali nell'UE e in tutto il mondo.

La protezione dei dati è presa sul serio come mai prima d'ora e ha un impatto di ampia portata sulle varie parti interessate e sui vari settori. La Commissione è determinata a guidare l'UE verso un'attuazione efficace del nuovo regime di protezione dei dati e a sostenere tutti gli aspetti per la sua piena operatività. La presente comunicazione fa il punto sui risultati conseguiti finora per quanto riguarda l'attuazione coerente delle norme sulla protezione dei dati in tutta l'UE, il funzionamento del nuovo sistema di governance, l'impatto sui cittadini e sulle imprese e gli sforzi dell'UE per promuovere la convergenza globale dei regimi di protezione dei dati. Dà inoltre seguito alla comunicazione del gennaio 2018 sull'applicazione del regolamento[5] e si basa sui lavori del gruppo multilaterale[6], in particolare sul contributo all'esercizio di valutazione sull'anno trascorso e sulle discussioni svoltesi in occasione dell'evento di valutazione organizzato dalla Commissione il 13 giugno 2019[7]. La presente comunicazione intende essere altresì un contributo al riesame che la Commissione prevede di effettuare entro maggio 2020 [8].

Il quadro legislativo dell'UE in materia di protezione dei dati è un elemento cardine dell'approccio europeo antropocentrico all'innovazione. Sta diventando parte integrante della base di regolamentazione di una serie sempre più ampia di politiche, tra le quali quelle in materia di sanità e ricerca, intelligenza artificiale, trasporti, energia, concorrenza e applicazione della legge. La Commissione ha sottolineato costantemente l'importanza di una corretta attuazione e applicazione delle nuove norme sulla protezione dei dati, come sottolineato nella comunicazione del gennaio 2018 sull'applicazione del regolamento e negli orientamenti del settembre 2018 sull'uso dei dati personali nel contesto elettorale[9]. Al momento della stesura della presente comunicazione sono stati compiuti notevoli progressi a favore del conseguimento di questo obiettivo, sebbene siano certamente necessari ulteriori sforzi affinché il regolamento diventi pienamente operativo.

---

5 Comunicazione della Commissione al Parlamento europeo e al Consiglio, "Maggiore protezione, nuove opportunità – Orientamenti della Commissione per l'applicazione diretta del regolamento generale sulla protezione dei dati a partire dal 25 maggio 2018", COM(2018) 43 final: https://eur-lex.europa.eu/legal-content/IT/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043.

6 Il gruppo multilaterale sul regolamento istituito dalla Commissione coinvolge rappresentanti della società civile e delle imprese, studiosi e professionisti: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&Lang=IT.

7 http://europa.eu/rapid/press-release_IP-19-2956_it.htm.

8 Articolo 97 del regolamento.

9 "Orientamenti della Commissione sull'applicazione del diritto dell'Unione in materia di protezione dei dati nel contesto elettorale", COM(2018) 638 final: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52018DC0638&qid=1551268194885&from=IT.

II. Un continente, una legge: il quadro per la protezione dei dati è applicabile negli Stati membri

Uno degli obiettivi principali del regolamento era quello di eliminare il panorama frammentato di 28 diverse legislazioni nazionali esistente nell'ambito della precedente direttiva sulla protezione dei dati[10] e di garantire la certezza del diritto per le persone fisiche e giuridiche in tutta l'UE. Tale obiettivo è stato ampiamente conseguito.

L'armonizzazione del quadro giuridico

Il regolamento, pur essendo direttamente applicabile negli Stati membri, li ha obbligati ad adottare una serie di misure giuridiche a livello nazionale, in particolare per istituire e attribuire competenze alle autorità nazionali di protezione dei dati[11], stabilire norme su questioni specifiche, quali la conciliazione della protezione dei dati personali con la libertà di espressione e di informazione, nonché per modificare o abrogare la legislazione settoriale in considerazione di aspetti relativi alla protezione dei dati. Al momento della stesura della presente comunicazione, tutti gli Stati membri, eccetto tre[12], avevano aggiornato la loro legislazione nazionale in materia di protezione dei dati. I lavori di adeguamento delle leggi settoriali sono ancora in corso a livello nazionale. In seguito alla sua integrazione nell'accordo sullo Spazio economico europeo, l'applicazione del regolamento è stata estesa a Norvegia, Islanda e Liechtenstein, i quali hanno adottato anch'essi le rispettive legislazioni nazionali in materia di protezione dei dati.

Tuttavia, le parti interessate chiedono un livello di armonizzazione ancora più elevato in taluni settori[13]. In effetti, il regolamento consente agli Stati membri una certa discrezionalità nello specificare ulteriormente la sua applicazione in taluni settori quali l'età del consenso da parte di minori per i servizi online[14] o il trattamento di dati personali in settori quali la medicina e la sanità pubblica. In questo caso, l'azione degli Stati membri è inquadrata da due elementi:

i) qualsiasi legge nazionale volta a precisare tali aspetti deve soddisfare le prescrizioni di cui alla Carta dei diritti fondamentali[15] (e non andare oltre i limiti fissati dal regolamento, che si fonda sulla Carta);
ii) non deve ostacolare la libera circolazione di dati personali all'interno dell'UE[16].

---

[10] 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): https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:31995L0046.

[11] Quali la facoltà di imporre sanzioni amministrative pecuniarie.

[12] Al 23 luglio 2019, Grecia, Portogallo e Slovenia erano ancora in fase di adozione del diritto nazionale.

[13] Cfr. relazione del gruppo multilaterale sul regolamento pubblicata il 13 giugno 2019: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670.

[14] 13 anni per Belgio, Danimarca, Estonia, Finlandia, Lettonia, Malta, Svezia e Regno Unito; 14 anni per Austria, Bulgaria, Cipro, Spagna, Italia e Lituania; 15 anni per Cechia e Francia; 16 anni per Germania, Ungheria, Croazia, Irlanda, Lussemburgo, Paesi Bassi, Polonia, Romania e Slovacchia.

[15] Articolo 8.

[16] Conformemente all'articolo 16, paragrafo 2, del trattato sul funzionamento dell'Unione europea.

In alcuni casi, gli Stati membri hanno introdotto prescrizioni nazionali in aggiunta a quelle del regolamento, in particolare attraverso numerose leggi settoriali, il che comporta una frammentazione e crea oneri inutili. Un esempio di prescrizione supplementare introdotta dagli Stati membri in aggiunta a quelle del regolamento è l'obbligo previsto dalla legislazione tedesca di designare un responsabile della protezione dei dati nelle imprese con almeno 20 dipendenti permanentemente coinvolte nel trattamento automatizzato di dati personali.

Prosecuzione degli sforzi a sostegno di una maggiore armonizzazione

La Commissione intrattiene dialoghi bilaterali con le autorità nazionali, nel contesto dei quali presta particolare attenzione alle misure nazionali in relazione a:

- l'effettiva indipendenza delle autorità di protezione dei dati, anche attraverso adeguate risorse finanziarie, umane e tecniche;
- il modo in cui le legislazioni nazionali limitano i diritti degli interessati;
- il fatto che la legislazione nazionale non dovrebbe introdurre prescrizioni che vadano oltre quelle del regolamento quando non vi è margine di specificazione, come nel caso di condizioni supplementari per il trattamento;
- l'adempimento dell'obbligo di conciliare il diritto alla protezione dei dati personali con la libertà di espressione e di informazione, tenendo conto del fatto che tale obbligo non dovrebbe essere utilizzato in modo improprio per creare un effetto dissuasivo sull'attività giornalistica.

Il lavoro delle autorità di protezione dei dati, che cooperano nel contesto del comitato europeo per la protezione dei dati ("il comitato"), è un fattore trainante chiave per un'applicazione coerente delle nuove norme: le azioni di esecuzione che interessano diversi Stati membri passano attraverso il meccanismo di cooperazione e coerenza[17] previsto in seno al comitato e gli orientamenti adottati dal comitato contribuiscono ad un'interpretazione armonizzata del regolamento. Le parti interessate si aspettano tuttavia che le autorità di protezione dei dati si spingano oltre in questa direzione.

Anche il lavoro degli organi giurisdizionali nazionali e della Corte di giustizia dell'Unione europea contribuisce a creare un'interpretazione coerente delle norme in materia di protezione dei dati. Gli organi giurisdizionali hanno recentemente emesso sentenze che annullano disposizioni del diritto interno che si discostano dal regolamento[18].

---

[17] L'articolo 60 del regolamento prevede una cooperazione tra autorità di protezione dei dati affinché si applichi un'unica interpretazione del regolamento in casi concreti. L'articolo 64 prevede che il comitato emetta pareri in determinati casi, in modo da garantire un'applicazione coerente del regolamento. Infine, al comitato è conferito il potere di adottare decisioni vincolanti indirizzate alle autorità di protezione dei dati in caso di disaccordo tra di esse.

[18] Ciò è avvenuto in Germania e in Spagna.

III. Tutti gli elementi del nuovo sistema di governance stanno iniziando ad avere un senso

Il regolamento ha creato una nuova struttura di governance, al centro della quale vi sono le autorità nazionali indipendenti di protezione dei dati, in veste di soggetti preposti all'applicazione del regolamento e primi punti di contatto per le parti interessate. Sebbene nell'ultimo anno la maggior parte delle autorità di protezione dei dati abbia beneficiato di maggiori risorse, permangono ancora notevoli differenze tra gli Stati membri[19].

Le autorità di protezione dei dati si avvalgono dei loro nuovi poteri

Il regolamento conferisce alle autorità di protezione dei dati poteri rafforzati di esecuzione. Contrariamente ai timori espressi da alcune parti interessate prima del maggio 2018, le autorità nazionali di protezione dei dati hanno adottato un approccio equilibrato ai poteri di esecuzione. Tali autorità si sono concentrate sul dialogo piuttosto che su sanzioni, in particolare per gli operatori di dimensioni più piccole che non trattano dati personali come attività principale. Allo stesso tempo, non hanno evitato di utilizzare efficacemente i loro nuovi poteri ogniqualvolta ciò fosse necessario, anche avviando indagini nel settore dei media sociali[20] e imponendo sanzioni amministrative pecuniarie di valore compreso tra poche migliaia di EUR a diversi milioni di EUR, a seconda della gravità delle violazioni delle norme in materia di protezione dei dati.

Esempi di sanzioni pecuniarie imposte dalle autorità di protezione dei dati[21]:

- 5 000 EUR a un bar di scommesse sportive in Austria, per sorveglianza video illecita;
- 220 000 EUR a una società di intermediazione dati in Polonia per non aver informato le persone fisiche del trattamento dei loro dati;
- 250 000 EUR al campionato di calcio spagnolo LaLiga, per mancanza di trasparenza nella progettazione della sua applicazione per smartphone;
- 50 milioni di EUR a Google in Francia, in ragione delle condizioni per l'ottenimento del consenso degli utenti.

Nel condurre le indagini, è essenziale che le autorità di protezione dei dati raccolgano le prove pertinenti, rispettino tutte le fasi procedurali previste dalla legislazione nazionale e garantiscano un giusto processo in relazione a casi spesso complessi. Ciò richiede tempo e un lavoro notevole, il che spiega perché la maggior parte delle indagini avviate in seguito all'entrata in vigore del regolamento è ancora in corso.

---

19 https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf.

20 Ad esempio, la commissione irlandese per la protezione dei dati ha avviato 15 indagini formali in relazione al rispetto del regolamento da parte di società tecnologiche multinazionali. Cfr. pag. 49 della relazione annuale 2018 della commissione irlandese per la protezione dei dati: https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018.

21 Numerose delle decisioni che impongono sanzioni pecuniarie sono ancora soggette a controllo giurisdizionale.

Detto questo, il successo del regolamento non deve essere misurato in base al numero di sanzioni pecuniarie imposte, bensì ai cambiamenti rilevati nella cultura e nel comportamento di tutte le parti interessate. In questo contesto, le autorità di protezione dei dati dispongono di altri strumenti quali l'imposizione di una limitazione provvisoria o definitiva al trattamento, inclusi il divieto di trattamento o la sospensione di flussi di dati verso un destinatario in un paese terzo[22].

Alcune autorità di protezione dei dati hanno creato strumenti nuovi, quali linee di assistenza e strumenti per le imprese, mentre altre hanno sviluppato approcci nuovi, quali ambienti isolati di regolamentazione (*sandbox*)[23] destinati a fornire assistenza alle imprese nei loro sforzi relativi al rispetto delle norme. Tuttavia, numerose parti interessate ritengono ancora di non aver ricevuto sufficiente sostegno e informazioni, in particolare le piccole e medie imprese in alcuni Stati membri[24]. Al fine di contribuire a porre rimedio a questa situazione, la Commissione concede sovvenzioni alle autorità di protezione dei dati affinché queste ultime possano raggiungere le parti interessate, in particolare le persone fisiche e le piccole e medie imprese[25].

Il comitato europeo per la protezione dei dati è operativo

Le autorità di protezione dei dati hanno intensificato il loro lavoro in seno al comitato europeo per la protezione dei dati[26]. Questo intenso lavoro ha consentito al comitato di adottare circa 20 orientamenti in merito ad aspetti chiave del regolamento[27]. I settori futuri di lavoro del comitato sono presentati in un programma biennale[28] come richiesto dal regolamento.

Nei casi transfrontalieri, ciascuna autorità di protezione dei dati non agisce più semplicemente come un'autorità nazionale, bensì fa parte di un processo veramente europeo in tutte le fasi, dall'indagine alla decisione. Tale stretta cooperazione è diventata una pratica quotidiana: a fine giugno del 2019 erano 516 i casi transfrontalieri gestiti attraverso il meccanismo di cooperazione.

---

22 Articolo 58, paragrafo 2, lettere f) e j).

23 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/.

24 Cfr. relazione del gruppo multilaterale sul regolamento generale sulla protezione dei dati: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670.

25 2 milioni di EUR assegnati a nove autorità di protezione dei dati nel 2018 per attività nel 2018-2019: Belgio, Bulgaria, Danimarca, Ungheria, Lituania, Lettonia, Paesi Bassi, Slovenia e Islanda: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017;
1 milione di EUR da assegnare nel 2019: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019.

26 Il comitato ha personalità giuridica ed è composto dai capi delle autorità nazionali di controllo della protezione dei dati e dal garante europeo della protezione dei dati.

27 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_it.

28 https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_it.

La Commissione contribuisce attivamente ai lavori del comitato[29] nel promuovere la lettera e lo spirito del regolamento e ricorda i principi generali del diritto dell'Unione[30].

Verso la creazione di una cultura europea della protezione dei dati

Il nuovo sistema di governance deve ancora realizzare appieno il suo potenziale. È importante che il comitato renda ulteriormente più efficace il suo processo decisionale e sviluppi una cultura comune dell'UE in materia di protezione dei dati tra i suoi membri. Le possibilità delle quali dispongono le autorità di protezione dei dati di unire i loro sforzi[31] su questioni che interessano più di uno Stato membro, ad esempio lo svolgimento di indagini e misure di contrasto congiunte, può contribuire al raggiungimento di tale obiettivo attenuando nel contempo i vincoli in termini di risorse.

Numerose parti interessate auspicano una cooperazione ancora maggiore e un approccio uniforme da parte delle autorità nazionali di protezione dei dati[32] e chiedono inoltre una maggiore coerenza nella consulenza fornita da tali autorità[33], oltre a un pieno allineamento degli orientamenti nazionali a quelli del comitato. Alcune parti interessate si aspettano anche ulteriori chiarimenti di concetti chiave del regolamento, quali l'approccio basato sul rischio, tenendo conto in particolare delle preoccupazioni delle piccole e medie imprese.

In questo contesto, è essenziale consentire alle parti interessate di contribuire meglio ai lavori del comitato. Per questo motivo la Commissione accoglie con favore la consultazione pubblica sistematica organizzata dal comitato in merito agli orientamenti. Questa pratica, associata all'organizzazione di seminari per le parti interessate su temi specifici in una fase iniziale della riflessione, dovrebbe essere proseguita e ampliata in maniera da garantire la trasparenza, l'inclusione e la pertinenza dei lavori del comitato.

IV. Le persone esercitano i loro diritti, tuttavia occorre che la sensibilizzazione continui

Un altro obiettivo chiave del regolamento era il rafforzamento dei diritti delle persone fisiche. Il regolamento è considerato ampiamente dalle associazioni dei diritti civili e dalle organizzazioni dei consumatori come un importante contributo ad una società digitale equa, fondata sulla fiducia reciproca.

---

29 In veste di partecipante senza diritto di voto.

30 La Commissione ha inoltre contribuito ad agevolare l'istituzione del comitato e ne sostiene il funzionamento fornendo il suo sistema di comunicazione.

31 Articolo 62 del regolamento.

32 Cfr. relazione del gruppo multilaterale sul regolamento: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670. Ad esempio, le imprese ritengono che gli elenchi nazionali dei tipi di trattamento che richiedono una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del regolamento avrebbero potuto essere armonizzati in maniera migliore.

33 Anche tra le varie autorità degli Stati federali.

Una maggiore sensibilizzazione del pubblico in materia di diritti di protezione dei dati

Le persone fisiche dell'UE sono sempre più consapevoli delle norme in materia di protezione dei dati e dei loro diritti: il 67 % dei rispondenti a un'indagine Eurobarometro del maggio 2019[34] è a conoscenza del regolamento e il 57 % sa che esiste un'autorità nazionale per la protezione dei dati alla quale rivolgersi per informazioni o per presentare reclami. Il 73 % ha sentito parlare di almeno uno dei diritti riconosciuti dal regolamento. Tuttavia, un numero considerevole di persone nell'UE non adotta ancora misure attive per proteggere i propri dati personali durante la navigazione online. Ad esempio, il 44 % delle persone non ha modificato le impostazioni predefinite in materia di tutela della vita privata nelle reti sociali.

Le persone esercitano sempre più spesso i loro diritti

Questa maggiore consapevolezza in merito ai diritti ha indotto le persone a esercitarli più intensamente attraverso richieste di informazioni di clienti e rivolgendosi più spesso alle autorità di protezione dei dati per chiedere informazioni o presentare reclami[35]. Anche le imprese riferiscono che le richieste di accesso ai dati personali sono aumentate in diversi settori, come quello bancario e delle telecomunicazioni. Le persone hanno inoltre revocato più spesso il loro consenso ed esercitato il loro diritto di opposizione alle comunicazioni commerciali[36].

Tuttavia, alcuni operatori hanno segnalato malintesi di interpretazione da parte di persone riguardo alle norme sulla protezione dei dati, quali la convinzione che esse dovrebbero acconsentire a tutti i trattamenti o che il diritto alla cancellazione sia assoluto (mentre, ad esempio, i dati personali devono talvolta essere conservati dagli operatori in ragione di obblighi giuridici)[37]. Da parte loro, le organizzazioni della società civile lamentano i lunghi tempi di risposta da parte di alcune imprese e autorità di protezione dei dati.

È importante osservare che, su mandato di singoli individui, sono state avviate diverse azioni collettive da parte di organizzazioni non governative avvalendosi della nuova possibilità prevista dal regolamento[38]. Il ricorso alle azioni collettive sarebbe stato più semplice se un maggior numero di Stati membri si fosse avvalso della possibilità, prevista dal regolamento, di consentire alle organizzazioni non governative di avviare azioni senza mandato[39].

La necessità di proseguire gli sforzi di sensibilizzazione

Il dialogo e gli sforzi di sensibilizzazione incentrati sul pubblico generale devono pertanto proseguire a livello nazionale e di Unione europea. A tal fine, nel luglio 2019 la Commissione ha lanciato una nuova campagna online[40] destinata a incoraggiare le persone a leggere le

---

34 http://europa.eu/rapid/press-release_IP-19-2956_it.htm.
35 https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf.
36 Cfr. relazione del gruppo multilaterale sul regolamento generale sulla protezione dei dati.
37 Cfr. relazione del gruppo multilaterale sul regolamento generale sulla protezione dei dati.
38 Articolo 80, paragrafo 1, del regolamento.
39 Articolo 80, paragrafo 2, del regolamento.
40 Tale campagna fa seguito alla precedente destinata alla diffusione di materiale informativo per le persone fisiche e giuridiche, disponibile all'indirizzo: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_it.

dichiarazioni in materia di tutela della vita privata e ad ottimizzare le proprie impostazioni a riguardo.

V. Le imprese stanno adattando le loro prassi

Il regolamento mira a sostenere le imprese dell'economia digitale offrendo soluzioni a prova di futuro. In generale, le imprese accolgono con favore il principio di responsabilizzazione del regolamento, che si allontana dal precedente approccio oneroso ex ante (l'eliminazione degli obblighi di notifica, la scalabilità degli obblighi e la flessibilità della protezione dei dati fin dalla progettazione e della protezione per impostazione predefinita consentono la concorrenza sulla base di soluzioni rispettose della vita privata). Allo stesso tempo, alcuni chiedono alle autorità di protezione dei dati una maggiore certezza del diritto e orientamenti aggiuntivi o più chiari[41].

Gestione affidabile dei dati

Mentre le imprese segnalano una serie di sfide nell'adeguarsi alle nuove norme[42], molti sottolineano che questa è stata anche un'occasione per portare la questione della protezione dei dati all'attenzione dei consigli di amministrazione delle imprese, per mettere ordine all'interno dell'impresa per quanto concerne i dati detenuti, per migliorare la sicurezza, essere meglio preparati agli incidenti, ridurre l'esposizione a rischi inutili e costruire rapporti di maggiore fiducia con i propri clienti e partner commerciali. Per quanto concerne la trasparenza, le organizzazioni della società civile e di imprese menzionano il delicato equilibrio da raggiungere tra il fornire alle persone tutte le informazioni richieste dal regolamento e l'uso di un linguaggio chiaro e semplice e di una forma che le persone possano comprendere. Gli operatori stanno sviluppando soluzioni innovative in questa direzione.

In generale, le imprese hanno indicato di essere in grado di dare attuazione ai nuovi diritti riconosciuti agli interessati, anche se talvolta è stato difficile rispettare le scadenze in ragione di un aumento del numero di richieste e del loro carattere più ampio[43] oppure della necessità di verificare l'identità della persona che presenta la richiesta.

Impatto sull'innovazione

Il regolamento non solo consente, ma incoraggia anche lo sviluppo di nuove tecnologie nel rispetto del diritto fondamentale alla protezione dei dati personali. È il caso di settori quali l'intelligenza artificiale.

Le imprese hanno iniziato a sviluppare la loro offerta di nuovi servizi più rispettosi della vita privata. Ad esempio, i motori di ricerca che non tengono traccia degli utenti o che non utilizzano la pubblicità comportamentale stanno progressivamente guadagnando quote di

---

41 Cfr. relazione del gruppo multilaterale sul regolamento.

42 L'aggiornamento del sistema informatico è spesso citato come una delle principali sfide, in particolare per quanto riguarda l'attuazione dei principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, il diritto alla cancellazione nelle copie di riserva, ecc.

43 Le imprese chiedono inoltre al comitato di fornire orientamenti in merito a richieste infondate ed eccessive.

mercato in taluni Stati membri. Altre imprese stanno sviluppando servizi che si basano su nuovi diritti concessi agli interessati, quali la portabilità dei loro dati personali. Un numero crescente di imprese ha promosso il rispetto dei dati personali come elemento di differenziazione concorrenziale e punto di forza nelle vendite. Questi sviluppi non si limitano all'UE, ma riguardano anche economie estere molto innovative[44].

La situazione specifica delle microimprese e delle piccole imprese a "basso rischio"

Sebbene la situazione vari da uno Stato membro all'altro, le microimprese e le piccole imprese[45] che non trattano dati personali come loro attività principale sono state tra le parti interessate che hanno presentato il maggior numero di domande sull'applicazione del regolamento. Pur sembrando in parte dovute a una scarsa consapevolezza delle norme in materia di protezione dei dati, le loro preoccupazioni sono talvolta esacerbate anche da campagne di società di consulenza che cercano di fornire consulenza a pagamento, dalla diffusione di informazioni errate, ad esempio sulla necessità di ottenere sistematicamente il consenso da parte delle persone fisiche[46] e da requisiti supplementari imposti a livello nazionale.

In questo contesto, le microimprese e le piccole imprese chiedono orientamenti che siano adeguati alla loro situazione specifica e che forniscano informazioni molto pratiche. Alcune autorità di protezione dei dati lo hanno già fatto a livello nazionale[47]. A complemento delle iniziative nazionali, la Commissione ha pubblicato materiale informativo per aiutare tali imprese a conformarsi alle nuove norme attraverso una serie di misure pratiche[48].

Utilizzo degli strumenti messi a disposizione dal regolamento

Il regolamento prevede strumenti per dimostrare la conformità, quali le clausole contrattuali tipo, i codici di condotta e i meccanismi di certificazione di recente introduzione.

Le clausole contrattuali tipo sono clausole modello che possono essere inserite su base volontaria in un contratto, ad esempio tra un titolare del trattamento e un responsabile del trattamento, e che stabiliscono gli obblighi delle parti contraenti ai sensi del regolamento. Il regolamento amplia le possibilità di utilizzare clausole contrattuali tipo tanto per i trasferimenti internazionali quanto all'interno dell'UE[49]. Nel settore dei trasferimenti

---

44 Ad esempio, secondo una relazione pubblicata dall'associazione israeliana del settore della sicurezza informatica, nel 2018 il sottosettore "protezione dei dati e tutela della vita privata" della sicurezza informatica è stato quello che ha registrato la più rapida crescita a seguito dell'entrata in vigore del regolamento generale sulla protezione dei dati.

45 Come definito nella definizione di PMI, disponibile all'indirizzo: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_it.

46 Il regolamento, infatti, non si fonda soltanto sul consenso, ma prevede diverse basi giuridiche per il trattamento dei dati personali.

47 Ad esempio, la guida elaborata dall'autorità francese per la protezione dei dati: https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement.

48 https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-en-n.pdf.

49 Cfr. articolo 28 del regolamento. Le clausole contrattuali tipo adottate dalla Commissione hanno validità in tutta l'UE. Al contrario, quelle adottate ai sensi dell'articolo 28, paragrafo 8, da un'autorità di protezione dei dati vincolano soltanto l'autorità che le ha adottate e possono quindi essere utilizzate come clausole contrattuali tipo per i trattamenti che rientrano nella competenza di tale autorità, ai sensi degli articoli 55 e 56.

internazionali, il loro ampio utilizzo indica[50] che sono molto utili alle imprese nei loro sforzi di conformità e particolarmente vantaggiose per le imprese che non dispongono di risorse per negoziare contratti individuali con ciascuno dei loro contraenti di trattamento dei dati.

Numerosi settori ritengono inoltre che l'adozione di clausole contrattuali tipo rappresenti uno strumento utile per favorire l'armonizzazione, in particolare quando è la Commissione ad adottarle. La Commissione collaborerà con le parti interessate per sfruttare le possibilità offerte dal regolamento e per aggiornare le clausole esistenti.

L'adesione a codici di condotta è un altro strumento operativo e pratico a disposizione dell'industria per facilitare la dimostrazione del rispetto del regolamento[51]. Tali codici dovrebbero essere elaborati da associazioni di categoria od organismi che rappresentano categorie di titolari del trattamento e responsabili del trattamento e dovrebbero descrivere le modalità di attuazione delle norme di protezione dei dati in un settore specifico. Calibrando gli obblighi in funzione dei rischi[52], tali codici possono inoltre rivelarsi un mezzo molto utile ed economico per consentire alle piccole e medie imprese di ottemperare ai loro obblighi.

Infine, anche la certificazione può essere uno strumento utile per dimostrare la conformità a requisiti specifici del regolamento. Può aumentare la certezza del diritto per le imprese e promuovere il regolamento a livello mondiale. Le linee guida per la certificazione e l'accreditamento[53] recentemente adottate dal comitato europeo per la protezione dei dati consentiranno lo sviluppo di sistemi di certificazione nell'UE. La Commissione seguirà questi sviluppi e, se del caso, si avvarrà dei poteri conferiti dal regolamento per definire i requisiti per la certificazione. La Commissione può inoltre presentare una richiesta di normalizzazione agli organismi di normalizzazione dell'UE su aspetti rilevanti ai fini del regolamento.

VI. La convergenza verso l'alto sta progredendo a livello internazionale

L'esigenza di proteggere i dati personali non si limita all'Unione europea. Come dimostrato da una recente indagine globale sulla sicurezza di Internet, a livello mondiale si registra un aumento della mancanza di fiducia che induce le persone a cambiare il modo in cui si comportano online[54]. Un numero crescente di imprese risponde a queste preoccupazioni

---

50 Esse costituiscono in realtà il principale strumento su cui le imprese fanno affidamento per le loro esportazioni di dati.

51 Il 4 giugno 2019 il comitato europeo per la protezione dei dati ha adottato orientamenti sui codici di condotta. Tali orientamenti chiariscono le procedure e le norme relative alla presentazione, all'approvazione e alla pubblicazione di codici a livello tanto nazionale quanto UE.

52 Considerando 98 del regolamento.

53 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_it; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_it;

54 Cfr. l'indagine globale CIGI-Ipsos 2019 sulla sicurezza di Internet e la fiducia nei suoi confronti. Secondo tale indagine, il 78 % dei rispondenti è preoccupato della tutela della propria vita privata online, il 49 % afferma che la sfiducia li ha indotti a divulgare meno informazioni personali online, il 43 % ha invece riferito di prestare maggiore attenzione alla protezione del proprio dispositivo e il 39 % ha risposto di utilizzare Internet in modo più selettivo, tra le altre precauzioni. L'indagine è stata condotta in 25 economie: Australia, Brasile, Canada, Cina, Egitto, Francia, Germania, Giappone, Gran Bretagna, Hong Kong, India, Indonesia, Italia, Kenya, Messico, Nigeria, Pakistan, Polonia, Russia, Repubblica di Corea, Stati Uniti, Sud Africa, Svezia, Tunisia e Turchia.

estendendo di propria iniziativa i diritti riconosciuti dal regolamento ai loro clienti non residenti nell'UE.

Inoltre, poiché i paesi di tutto il mondo affrontano sempre più spesso sfide analoghe, si stanno dotando di nuove norme di protezione dei dati o modernizzando quelle esistenti. Spesso tali leggi presentano una serie di caratteristiche comuni condivise dal regime di protezione dei dati dell'UE, come una legislazione di ampia portata piuttosto che norme settoriali, diritti individuali applicabili e un'autorità di controllo indipendente. Questa tendenza è veramente globale, dalla Corea del Sud al Brasile, dal Cile alla Thailandia, dall'India all'Indonesia. La partecipazione sempre più universale alla "Convenzione 108" del Consiglio d'Europa[55], recentemente modernizzata[56] con un contributo significativo della Commissione, è un altro evidente indizio di questa tendenza alla convergenza verso l'alto.

Promuovere flussi di dati sicuri e liberi attraverso decisioni di adeguatezza e con altri mezzi

Questa convergenza che si sta sviluppando offre nuove opportunità per facilitare i flussi di dati e, di conseguenza, gli scambi commerciali, nonché la cooperazione tra autorità pubbliche, migliorando nel contempo il livello di protezione dei dati delle persone fisiche nell'UE quando tali dati vengono trasferiti all'estero.

Nell'attuare la strategia definita nella sua comunicazione del 2017 sullo scambio e sulla protezione di dati personali in un mondo globalizzato[57], la Commissione ha intensificato il suo impegno nei confronti di paesi terzi e altri partner internazionali basandosi su elementi di convergenza tra i sistemi di tutela della vita privata e sviluppandoli ulteriormente. Ciò ha incluso la valutazione della possibilità di adottare accertamenti di adeguatezza in relazione a paesi terzi selezionati[58]. Questo lavoro ha prodotto risultati importanti, in particolare l'entrata in vigore, nel febbraio del 2019, dell'accordo di mutua adeguatezza UE-Giappone che ha creato lo spazio più grande al mondo di flussi di dati liberi e sicuri. I negoziati sull'adeguatezza con la Corea del Sud sono in fase avanzata e sono in corso lavori esplorativi che mirano ad avviare colloqui sull'adeguatezza con diversi paesi dell'America latina, quali il Cile o il Brasile, in funzione del completamento dei processi legislativi in corso. Gli sviluppi sono promettenti anche in alcune parti dell'Asia, come ad esempio in India, Indonesia e

---

55 Convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STE N. 108) e protocollo addizionale del 2001 alla convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri (STE N. 181). Si tratta dell'unico strumento multilaterale vincolante nel settore della protezione dei dati. Gli ultimi paesi che hanno ratificato la convenzione sono l'Argentina, il Messico, Capo Verde e il Marocco.

56 Protocollo che modifica la convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STE N. 108), come convenuto nella 128ª seduta del comitato dei ministri tenutasi ad Elsinora, Danimarca, il 17 e 18 maggio 2018. Il testo consolidato della convenzione 108 aggiornata è disponibile al seguente indirizzo: https://rm.coe.int/16808ade9d.

57 Comunicazione della Commissione al Parlamento europeo e al Consiglio, "Scambio e protezione dei dati personali in un mondo globalizzato", COM/2017/07 final.

58 Il regolamento ha inoltre creato la possibilità di accertamenti di adeguatezza anche in relazione ad organizzazioni internazionali, nel contesto degli sforzi dell'UE per facilitare gli scambi di dati con tali soggetti.

Taiwan, nonché nei paesi del vicinato europeo orientale e meridionale, che potrebbero consentire future decisioni di adeguatezza.

Allo stesso tempo, la Commissione accoglie con favore il fatto che altri paesi che hanno messo in atto strumenti di trasferimento analoghi all'adeguatezza del regolamento abbiano riconosciuto che l'UE e i paesi riconosciuti "adeguati" dall'UE garantiscono il livello di protezione richiesto[59]. In questo modo si può creare una rete di paesi nel contesto della quale i dati possono circolare liberamente.

Parallelamente a ciò, è in corso un intenso lavoro con altri paesi terzi, quali il Canada, la Nuova Zelanda, l'Argentina e Israele, che mira a garantire la continuità, ai sensi del regolamento, delle decisioni di adeguatezza adottate sulla base della direttiva del 1995 sulla protezione dei dati. Nel frattempo, lo scudo UE-USA per la privacy si è dimostrato uno strumento utile per garantire flussi di dati transatlantici basati su un livello elevato di protezione, con oltre 4 700 imprese partecipanti[60]. Il suo riesame annuale garantisce che il corretto funzionamento del quadro sia verificato regolarmente e che nuove questioni possano essere affrontate in tempo utile.

Poiché non esiste una soluzione sempre valida per i flussi di dati, la Commissione sta inoltre collaborando con le parti interessate e il comitato per sfruttare appieno il potenziale degli strumenti del regolamento per i trasferimenti internazionali. Si tratta di strumenti quali le clausole contrattuali tipo, lo sviluppo di sistemi di certificazione, codici di condotta o accordi amministrativi per gli enti pubblici. A tale riguardo, la Commissione è interessata allo scambio di esperienze e migliori prassi con altri sistemi che possono aver sviluppato una competenza specifica in relazione ad alcuni di questi strumenti. La Commissione valuterà la possibilità di avvalersi dei poteri ad essa conferiti dal regolamento per quanto riguarda tali strumenti di trasferimento, in particolare le clausole contrattuali tipo.

Oltre agli strumenti puramente bilaterali, potrebbe anche essere utile valutare se i paesi che la pensano allo stesso modo siano in grado di definire un quadro multinazionale in questo settore in un momento in cui i flussi di dati costituiscono una componente sempre più cruciale degli scambi commerciali, delle comunicazioni e delle interazioni sociali. Tale strumento consentirebbe la libera circolazione di dati tra le parti contraenti, garantendo al tempo stesso il livello di protezione richiesto sulla base di valori condivisi e di sistemi convergenti. Tale strumento potrebbe essere sviluppato, ad esempio, basandosi sulla convenzione 108 aggiornata oppure ispirandosi all'iniziativa "*Data Free Flows with Trust*" lanciata dal Giappone all'inizio di quest'anno.

Sviluppo di sinergie nuove tra il commercio e gli strumenti di protezione dei dati

Nel promuovere la convergenza delle norme in materia di protezione dei dati a livello internazionale, la Commissione è altresì determinata ad affrontare la questione del protezionismo digitale. A tal fine, ha sviluppato disposizioni specifiche sui flussi di dati e

---

[59] Questo è l'approccio adottato, ad esempio, da Argentina, Colombia, Israele e Svizzera.

[60] Ciò significa che nei suoi primi tre anni di esistenza, lo scudo per la privacy ha registrato più aziende partecipanti rispetto al suo predecessore, l'"Approdo sicuro", dopo 13 anni di funzionamento.

sulla protezione dei dati negli accordi commerciali che presenta sistematicamente nei suoi negoziati bilaterali e multilaterali, come ad esempio negli attuali colloqui dell'OMC sul commercio elettronico. Tali disposizioni orizzontali escludono misure puramente protezionistiche, quali i requisiti di localizzazione forzata dei dati, pur preservando l'autonomia normativa delle parti per tutelare il diritto fondamentale alla protezione dei dati.

Sebbene tali dialoghi in materia di protezione dei dati e i negoziati commerciali debbano seguire percorsi separati, essi possono completarsi a vicenda: l'accordo sulla mutua adeguatezza UE-Giappone è l'esempio migliore di tali sinergie che facilitano ulteriormente gli scambi commerciali e amplificano in tal modo i vantaggi dell'accordo di partenariato economico. In effetti, questo tipo di convergenza, basato su valori condivisi e standard elevati e sostenuto da un'applicazione efficace, fornisce la base più solida per lo scambio di dati personali, un aspetto sempre più riconosciuto dai nostri partner internazionali[61]. Dato che le imprese operano sempre più spesso a livello transfrontaliero e preferiscono applicare norme analoghe in tutte le loro operazioni commerciali a livello mondiale, tale convergenza contribuisce a creare un ambiente favorevole agli investimenti diretti, facilitando gli scambi commerciali e migliorando la fiducia tra partner commerciali.

Facilitazione dello scambio di informazioni per contrastare la criminalità e il terrorismo sulla base di garanzie adeguate

Una maggiore compatibilità tra i regimi di protezione dei dati può inoltre facilitare notevolmente gli scambi di informazioni particolarmente necessari tra le autorità di regolamentazione, di polizia e giudiziarie dell'UE e quelle straniere, contribuendo in tal modo ad una cooperazione più efficace e rapida in materia di contrasto[62]. A tal fine, la Commissione intende avvalersi della possibilità di adottare decisioni di adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie con l'obiettivo di approfondire la sua cooperazione con i principali partner nella lotta contro la criminalità e il terrorismo. Inoltre, l'"accordo quadro" UE-USA[63], entrato in vigore nel mese di febbraio del 2017, può essere utilizzato come modello per accordi analoghi con altri importanti partner in materia di sicurezza.

Altri esempi che sottolineano l'importanza di livelli elevati di protezione dei dati come base per una cooperazione stabile con paesi terzi in materia di contrasto sono il trasferimento di

---

61 Come si evince, ad esempio, dal riferimento al concetto di "*Data Free Flow with Trust*" nella dichiarazione dei leader del G20 di Osaka: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

62 Cfr. comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, "Agenda europea sulla sicurezza", COM(2015) 185 final.

63 Accordo fra l'UE e gli USA sulla protezione dei dati personali trasferiti e trattati ai fini di prevenzione, indagine, accertamento o perseguimento di reati, anche di terrorismo, nel quadro della cooperazione di polizia e della cooperazione giudiziaria in materia penale: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:22016A1210(01) (l'"accordo quadro"). L'accordo quadro costituisce il primo accordo internazionale bilaterale nel settore dell'applicazione della legge che prevede un catalogo completo di diritti e obblighi in materia di protezione dei dati in linea con l'*acquis* dell'Unione. Si tratta di un esempio riuscito di come la cooperazione in materia di applicazione della legge con un importante partner internazionale possa essere rafforzata negoziando una solida serie di garanzie per la protezione dei dati.

dati concernenti il codice di prenotazione (*Passenger Name Record*, PNR)[64] e lo scambio di informazioni operative tra Europol e importanti partner internazionali. A questo proposito, sono attualmente in corso o sono in procinto di iniziare negoziati su accordi internazionali con diversi paesi del vicinato meridionale[65].

Solide garanzie in materia di protezione dei dati costituiranno inoltre una componente essenziale di qualsiasi futuro accordo sull'accesso transfrontaliero a prove elettroniche nelle indagini penali, a livello bilaterale (accordo UE-USA) o multilaterale (secondo protocollo aggiuntivo alla convenzione "Budapest" del Consiglio d'Europa sulla criminalità informatica)[66].

Promozione della cooperazione tra le autorità preposte all'applicazione delle norme in materia di protezione dei dati

In un momento in cui le questioni di rispetto della vita privata o gli incidenti di sicurezza possono interessare un gran numero di persone contemporaneamente in giurisdizioni diverse, forme più strette di cooperazione tra le autorità di controllo a livello internazionale possono contribuire a garantire tanto una protezione più efficace dei diritti individuali quanto un ambiente più stabile per gli operatori economici. In questo contesto e in stretto contatto con il comitato, la Commissione si adopererà per facilitare la cooperazione in materia di applicazione e l'assistenza reciproca tra le autorità di controllo dell'UE e straniere, anche avvalendosi dei nuovi poteri previsti in tale settore dal regolamento[67]. Ciò potrebbe riguardare diverse forme di cooperazione che spaziano dallo sviluppo di strumenti interpretativi o pratici comuni[68] allo scambio di informazioni su indagini in corso.

Infine, la Commissione intende altresì intensificare il dialogo con organizzazioni e reti regionali, quali l'Associazione delle nazioni del sud-est asiatico (ASEAN), l'Unione africana, il forum delle autorità di protezione dei dati Asia-Pacifico (APPA, *Asia Pacific Privacy Authorities forum*) o la rete per la protezione dei dati ibero-americana (*Ibero-American Data Protection Network*), che svolgono un ruolo sempre più importante nella definizione di norme comuni in materia di protezione dei dati, promuovendo lo scambio di migliori prassi e favorendo la cooperazione tra autorità di applicazione della normativa. Collaborerà inoltre con l'Organizzazione per la cooperazione e lo sviluppo economici e l'Organizzazione per la cooperazione economica Asia-Pacifico per sviluppare una convergenza verso un livello elevato di protezione dei dati.

---

64 La risoluzione (SCR) 2396 del Consiglio di sicurezza delle Nazioni Unite del 21 dicembre 2017 invita tutti gli Stati membri delle Nazioni Unite a sviluppare la capacità di raccogliere, trattare e analizzare i dati PNR, nel pieno rispetto dei diritti umani e delle libertà fondamentali. Cfr. anche la comunicazione della Commissione "Agenda europea sulla sicurezza", COM(2015)185 final: http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52015DC0185&from=it.

65 https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en.

66 http://europa.eu/rapid/press-release_IP-19-2891_it.htm.

67 Cfr. articolo 50 del regolamento sulla cooperazione internazionale nel settore della protezione dei dati. Tale disposizione tratta un'ampia gamma di forme di cooperazione, dall'informazione sulla legislazione in materia di protezione dei dati al deferimento di reclami e all'assistenza nelle indagini.

68 Ad esempio, modelli comuni per le notifiche di violazioni.

VII. La legislazione in materia di protezione dei dati come parte integrante di un'ampia gamma di politiche

La protezione dei dati personali è garantita e integrata in diverse politiche dell'Unione.

Telecomunicazioni e servizi di comunicazione elettronica

Nel gennaio del 2017 la Commissione ha adottato la sua proposta di regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche (COM/2017/010 final)[69]. La proposta mira a tutelare la riservatezza delle comunicazioni, come previsto dalla Carta dei diritti fondamentali, ma anche a proteggere i dati personali che possono far parte di una comunicazione, nonché le apparecchiature terminali degli utenti finali.

La proposta di regolamento sulla vita privata e le comunicazioni elettroniche specifica e completa il regolamento stabilendo norme specifiche per tali finalità. Modernizza le attuali norme UE in materia di *e-privacy*[70] al fine di rispecchiare gli sviluppi tecnologici e giuridici. Rafforza la tutela della vita privata delle persone fisiche estendendo l'ambito di applicazione delle nuove norme al fine di includere anche i fornitori di servizi di comunicazione "*over-the-top*", creando così parità di condizioni per tutti i servizi di comunicazione elettronica. Sebbene il Parlamento europeo abbia adottato un mandato per l'avvio di triloghi nell'ottobre del 2017, il Consiglio non ha ancora concordato in merito a un approccio generale. La Commissione rimane pienamente impegnata a favore del regolamento sulla vita privata e le comunicazioni elettroniche e sosterrà i colegislatori nei loro sforzi per giungere a una rapida adozione del regolamento proposto.

Salute e ricerca

Agevolare gli scambi di dati sanitari, considerati dati sensibili ai sensi del regolamento, tra Stati membri sta diventando sempre più importante nel settore della sanità pubblica per motivi di interesse generale. Tra questi si annoverano la prestazione di assistenza sanitaria o di cure, la protezione contro gravi minacce transfrontaliere alla salute e la garanzia di elevati livelli di qualità e sicurezza dell'assistenza sanitaria e dei medicinali o dei dispositivi medici. Il regolamento stabilisce le norme che garantiscono un trattamento lecito e affidabile e gli scambi di dati sanitari in tutta l'UE. Tali norme si applicano anche all'accesso di terzi a dati medici dei pazienti, compresi i dati contenuti nelle cartelle cliniche elettroniche dei pazienti e nelle prescrizioni elettroniche e, nel lungo termine, a registrazioni sanitarie elettroniche complete e al loro utilizzo per finalità di ricerca scientifica. Nel settore specifico delle sperimentazioni cliniche, la Commissione ha inoltre preparato domande e risposte specifiche sull'interazione tra il regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio,

---

69 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52017PC0010.

70 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).

sulla sperimentazione clinica di medicinali per uso umano[71] e il regolamento generale sulla protezione dei dati[72].

Intelligenza artificiale (IA)

In considerazione della crescente importanza strategica dell'intelligenza artificiale, è essenziale definire norme globali per il suo sviluppo e utilizzo. Nel promuovere lo sviluppo e l'adozione dell'intelligenza artificiale, la Commissione ha optato per un approccio antropocentrico, nel senso che le applicazioni di intelligenza artificiale devono rispettare i diritti fondamentali[73]. In questo contesto, le norme stabilite dal regolamento forniscono un quadro generale e contengono obblighi e diritti specifici particolarmente rilevanti per il trattamento di dati personali nel contesto dell'intelligenza artificiale. Ad esempio, il regolamento comprende il diritto di non essere oggetto di una decisione basata unicamente sul trattamento automatizzato, tranne in determinate situazioni[74]. Comprende inoltre requisiti specifici in termini di trasparenza sull'uso di un processo decisionale automatizzato, in particolare l'obbligo di informare sull'esistenza di tali decisioni e di fornire informazioni significative e spiegare il significato e le conseguenze previste del trattamento per l'interessato[75]. Questi principi fondamentali del regolamento sono stati riconosciuti dal gruppo di esperti ad alto livello sull'intelligenza artificiale[76], dall'Organizzazione per la cooperazione e lo sviluppo economici[77] e dal G20[78] come particolarmente rilevanti per affrontare le sfide e le opportunità derivanti dall'intelligenza artificiale. Il comitato europeo per la protezione dei dati ha individuato nell'intelligenza artificiale uno dei possibili temi del suo programma di lavoro per il periodo 2019-2020[79].

Trasporti

Lo sviluppo di automobili connesse e città intelligenti si basa sempre più spesso sul trattamento e sullo scambio di grandi quantità di dati personali tra più parti, tra cui automobili, costruttori di automobili, fornitori di servizi telematici e autorità pubbliche

---

71 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32014R0536.

72 https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf.

73 Comunicazione della Commissione dell'8 aprile 2019, "Creare fiducia nell'intelligenza artificiale antropocentrica", (COM/2019/168 final): https://eur-lex.europa.eu/legal-content/IT/TXT/?qid=1566576396495&uri=CELEX:52019DC0168.
"Orientamenti etici per un'IA affidabile", presentato dal gruppo di esperti ad alto livello (HLEG) l'8 aprile 2019: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Cfr. anche la raccomandazione del Consiglio dell'OCSE sull'intelligenza artificiale: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, i Principi in materia di IA del G20 approvati nel contesto della dichiarazione dei leader del G20 di Osaka: https://www.g20.org/pdf/documents/en/annex_08.pdf e la dichiarazione dei ministri del G20 sul commercio e l'economia digitale: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

74 Articolo 22 del regolamento.

75 Articolo 13, paragrafo 2, lettera f), del regolamento.

76 https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence.

77 Raccomandazione del Consiglio sull'intelligenza artificiale: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

78 Dichiarazione dei ministri del G20 sul commercio e l'economia digitale: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

79 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_it.pdf.

competenti per le infrastrutture stradali. Questo ambiente multipartitico comporta una certa complessità per quanto concerne la ripartizione dei ruoli e delle responsabilità dei vari soggetti coinvolti nel trattamento di dati personali e su come garantire la liceità del trattamento da parte di tutti i soggetti. Il rispetto del regolamento e della legislazione in materia di *ePrivacy* è essenziale per l'utilizzo riuscito di sistemi di trasporto intelligenti nel contesto di tutti i modi di trasporto, nonché per la diffusione di strumenti e servizi digitali che consentono una maggiore mobilità delle persone e delle merci[80].

Energia

Lo sviluppo di soluzioni digitali nel settore energetico si basa sempre più spesso sul trattamento di dati personali. La legislazione adottata nel contesto del pacchetto "Energia pulita per tutti gli europei"[81] comprende disposizioni nuove che consentono la digitalizzazione del settore elettrico e norme sull'accesso ai dati, la gestione dei dati e l'interoperabilità che permettono il trattamento in tempo reale di dati dei consumatori per realizzare risparmi e incoraggiare l'autogenerazione e la partecipazione al mercato dell'energia. Di conseguenza, il rispetto delle norme in materia di protezione dei dati è di estrema importanza per la riuscita attuazione di tali disposizioni.

Concorrenza

Il trattamento dei dati personali rappresenta sempre più un elemento da considerare nella politica in materia di concorrenza[82]. Dato che le autorità di protezione dei dati sono le uniche incaricate di valutare una violazione delle norme sulla protezione dei dati, le autorità incaricate in materia di concorrenza, consumatori e protezione dei dati cooperano e continueranno a cooperare, se necessario, nel contesto dell'intersezione delle rispettive competenze. La Commissione promuoverà tale cooperazione e seguirà da vicino gli sviluppi.

Contesto elettorale

Nei suoi Orientamenti sull'uso dei dati personali nel contesto elettorale[83], pubblicato nel settembre 2018 nel contesto del pacchetto elettorale[84], la Commissione ha richiamato l'attenzione su norme di particolare importanza per i soggetti coinvolti nelle elezioni, comprese le questioni relative al *micro-targeting* degli elettori. Tali orientamenti sono stati ripresi in una dichiarazione del comitato europeo per la protezione dei dati[85] e diverse autorità per la protezione dei dati hanno emanato orientamenti a livello nazionale. Il pacchetto elettorale ha compreso inoltre un invito a ciascuno Stato membro a istituire una rete elettorale nazionale che coinvolgesse nelle attività online pertinenti per le elezioni le autorità nazionali competenti in materia elettorale e i responsabili del controllo e dell'applicazione delle norme,

---

80 Ad esempio, facilitando la pianificazione e l'uso dei vari mezzi di trasporto nel corso del viaggio.

81 In particolare la direttiva 2009/72/CE del Parlamento europeo e del Consiglio sull'energia elettrica: https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32009L0072.

82 Ad esempio, caso M.8788 (Apple/Shazam) e caso M.8124 (Microsoft/LinkedIn).

83 https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52018DC0638&qid=1551268194885&from=IT

84 http://europa.eu/rapid/press-release_IP-18-5681_it.htm.

85 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.

come quelle competenti per la protezione dei dati. Sono state inoltre adottate misure nuove per introdurre sanzioni in caso di violazioni delle norme in materia di protezione dei dati da parte di partiti politici e fondazioni europei. La Commissione ha raccomandato agli Stati membri di adottare il medesimo approccio a livello nazionale. La valutazione delle elezioni del Parlamento europeo del 2019, la cui pubblicazione è prevista per il mese di ottobre del 2019, terrà conto anche di aspetti concernenti la protezione dei dati.

Applicazione della legge

È possibile sviluppare un'Unione della sicurezza efficace ed autentica soltanto nel pieno rispetto dei diritti fondamentali sanciti dalla Carta dell'UE e dalla legislazione UE secondaria, comprese adeguate garanzie di protezione dei dati per consentire lo scambio sicuro di dati personali per finalità di contrasto. Qualsiasi restrizione del diritto fondamentale alla tutela della vita privata e alla protezione dei dati è soggetta a una verifica rigorosa della necessità e della proporzionalità.

VIII. Conclusioni

Sulla base delle informazioni finora disponibili e del dialogo con le parti interessate, secondo la valutazione preliminare della Commissione il primo anno di applicazione del regolamento è stato complessivamente positivo. Tuttavia, come indicato nella presente comunicazione, sono necessari ulteriori progressi in una serie di settori.

Attuazione e integrazione del quadro giuridico:

- i tre Stati membri che non hanno ancora aggiornato la legislazione nazionale in materia di protezione dei dati devono provvedere con urgenza. Tutti gli Stati membri dovrebbero completare l'allineamento della loro legislazione settoriale con i requisiti del regolamento;

- la Commissione si avvarrà di tutti gli strumenti a sua disposizione, comprese le procedure di infrazione, per garantire che gli Stati membri rispettino il regolamento e limitino l'eventuale frammentazione del quadro normativo in materia di protezione dei dati.

Fare in modo che il nuovo sistema di governance realizzi tutto il suo potenziale:

- gli Stati membri dovrebbero assegnare risorse umane, finanziarie e tecniche sufficienti alle autorità nazionali di protezione dei dati;

- le autorità di protezione dei dati dovrebbero intensificare la loro cooperazione, ad esempio conducendo indagini congiunte. Gli Stati membri dovrebbero agevolare lo svolgimento di tali indagini;

- il comitato dovrebbe sviluppare ulteriormente una cultura UE della protezione dei dati e avvalersi pienamente degli strumenti previsti dal regolamento per garantire un'applicazione armonizzata delle norme. Dovrebbe proseguire i lavori sugli orientamenti, in particolare quelli rivolti alle piccole e medie imprese;

- le competenze del segretariato del comitato dovrebbero essere rafforzate al fine di sostenere e guidare i lavori del comitato in maniera più efficace;

- la Commissione continuerà a sostenere le autorità di protezione dei dati e il comitato, in particolare partecipando attivamente ai lavori del comitato e richiamando la sua attenzione sui requisiti del diritto dell'UE nel corso dell'attuazione del regolamento;

- la Commissione sosterrà l'interazione tra le autorità di protezione dei dati e altre autorità, in particolare nel settore della concorrenza, nel pieno rispetto delle rispettive competenze.

Sostegno a favore delle parti interessate e loro coinvolgimento:

- il comitato dovrebbe migliorare il modo in cui coinvolge le parti interessate nei suoi lavori. La Commissione continuerà a sostenere finanziariamente le autorità di protezione dei dati per aiutarle a raggiungere le parti interessate;

- la Commissione continuerà le sue attività di sensibilizzazione e il lavoro con le parti interessate.

Promozione della convergenza internazionale:

- la Commissione intensificherà ulteriormente il suo dialogo sull'adeguatezza con i principali partner qualificati, anche nel settore dell'applicazione della legge. In particolare, intende concludere nei prossimi mesi i negoziati in corso con la Corea del Sud. Nel 2020 riferirà in merito al riesame delle 11 decisioni di adeguatezza adottate ai sensi della direttiva sulla protezione dei dati;
- la Commissione continuerà ad adoperarsi, anche attraverso l'assistenza tecnica, lo scambio di informazioni e migliori prassi, con i paesi interessati affinché siano adottate leggi moderne in materia di tutela della vita privata, e promuoverà la cooperazione con le autorità di controllo di paesi terzi ed organizzazioni regionali;
- la Commissione si impegnerà con le organizzazioni multilaterali e regionali nella promozione di livelli elevati di protezione dei dati in veste di soggetto facilitatore degli scambi e della cooperazione (ad esempio nel contesto dell'iniziativa "*Data Free Flow with Trust*" lanciata dal Giappone nel contesto del G20).

Il regolamento[86] impone alla Commissione di riferire in merito alla sua attuazione nel 2020. Sarà l'occasione per esaminare i progressi compiuti e valutare se, dopo due anni di applicazione, le varie componenti del nuovo regime di protezione dei dati saranno pienamente operative. A tal fine, la Commissione si impegnerà con il Parlamento europeo, il Consiglio, gli Stati membri, il comitato europeo per la protezione dei dati, le parti interessate e i cittadini.

[86] Articolo 97 del regolamento.