Consiglio
dell'Unione europea

Bruxelles, 29 giugno 2020
(OR. en)

9180/20
ADD 1

DATAPROTECT 57
JAI 536
FREMP 41
DIGIT 50
RELEX 482

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto della Segretaria generale della Commissione europea
Data:	25 giugno 2020
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	SWD(2020) 115 final
Oggetto:	DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE […] che accompagna il documento 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**

Si trasmette in allegato, per le delegazioni, il documento SWD(2020) 115 final.

All: SWD(2020) 115 final

COMMISSIONE
EUROPEA

Bruxelles, 24.6.2020
SWD(2020) 115 final

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

[…]

che accompagna il documento

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

{COM(2020) 264 final}

Indice

1 Contesto 3

2 Applicazione del regolamento generale sulla protezione dei dati e funzionamento dei meccanismi di cooperazione e coerenza 4

2.1 Esercizio di poteri rafforzati da parte delle autorità di protezione dei dati 5

Questioni specifiche per il settore pubblico 6

Cooperazione con altre autorità di regolamentazione 6

2.2 Il meccanismo di cooperazione e coerenza 7

Sportello unico 8

Assistenza reciproca 9

Meccanismo di coerenza 9

Sfide da affrontare 10

2.3 Consulenza e orientamenti 11

Attività di sensibilizzazione e consulenza da parte delle autorità di protezione dei dati 11

Orientamenti del comitato europeo per la protezione dei dati 13

2.4 Risorse delle autorità di protezione dei dati 14

3 Norme armonizzate, tuttavia persiste un certo grado di frammentazione e approcci divergenti 16

3.1 Attuazione del regolamento generale sulla protezione dei dati da parte degli Stati membri 16

Principali questioni relative all'attuazione nazionale 17

Conciliazione del diritto alla protezione dei dati personali con la libertà di espressione e di informazione 18

3.2 Clausole di specificazione facoltative e loro limiti 20

Frammentazione legata all'uso di clausole di specificazione facoltative 20

4 Dare alle persone gli strumenti d'azione per controllare i propri dati 23

5 Opportunità e sfide per le organizzazioni, in particolare per le piccole e medie imprese 27

Insieme di strumenti per le imprese 30

6 Applicazione del regolamento generale sulla protezione dei dati alle nuove tecnologie 32

7 Trasferimenti internazionali e cooperazione globale 34

7.1 Tutela dei dati personali: una questione avente natura globale 34

7.2 Gli strumenti del regolamento generale sulla protezione dei dati relativi ai trasferimenti 36

Decisioni di adeguatezza 38

Garanzie adeguate 43
Deroghe 50
Decisioni da parte di organi giurisdizionali o autorità stranieri: non costituiscono motivo di trasferimento 51
7.3 Cooperazione internazionale nel settore della protezione dei dati 53
La dimensione bilaterale 53
La dimensione multilaterale 55

Allegato I: clausole di specificazione facoltative stabilite dalla legislazione nazionale
Allegato II: panoramica delle risorse delle autorità di protezione dei dati

1 CONTESTO

Il regolamento generale sulla protezione dei dati[1] è il risultato di otto anni di preparazione, redazione e negoziati interistituzionali ed è entrato in vigore il 25 maggio 2018 dopo un periodo transitorio di due anni (maggio 2016 - maggio 2018). L'articolo 97 del regolamento generale sulla protezione dei dati impone alla Commissione di riferire in merito alla valutazione e al riesame del regolamento stesso, a partire da una prima relazione dopo due anni di applicazione e successivamente ogni quattro anni.

Tale valutazione rientra anche nel contesto di un approccio multidisciplinare che la Commissione ha già seguito prima dell'entrata in vigore del regolamento e ha continuato ad attuare in maniera attiva da allora. Nel quadro di tale approccio, la Commissione si è impegnata in dialoghi bilaterali attualmente in corso con gli Stati membri in merito alla conformità della legislazione nazionale rispetto al regolamento generale sulla protezione dei dati, ha contribuito attivamente ai lavori del comitato europeo per la protezione dei dati (di seguito "il comitato") mettendo a disposizione le proprie esperienze e competenze, ha sostenuto le autorità di protezione dei dati e mantenuto stretti contatti con un'ampia serie di parti interessate sull'applicazione pratica del regolamento.

La valutazione si basa sull'esercizio di valutazione svolto dalla Commissione nel primo anno di applicazione del regolamento, riepilogato nella comunicazione pubblicata nel luglio del 2019[2]. Essa dà inoltre seguito alla comunicazione sull'applicazione del regolamento generale sulla protezione dei dati, pubblicata nel gennaio del 2018[3]. La Commissione ha inoltre adottato le linee guida sull'uso dei dati personali nel contesto elettorale, pubblicate nel settembre del 2018, e le linee guida sulle app a sostegno della lotta alla pandemia di Covid-19, pubblicate nell'aprile del 2020.

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 valutazione adotta un approccio di più ampio respiro per affrontare anche questioni sollevate da vari soggetti nel corso degli ultimi due anni.

Per preparare la valutazione, la Commissione ha tenuto conto dei contributi:

- del Consiglio[4];

---

[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] 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.

[3] 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]

[4] Posizione e conclusioni del Consiglio in merito all'applicazione del regolamento generale sulla protezione dei dati – 14994/2/19 Rev. 2, 15.01.2020:

- del Parlamento europeo (commissione per le libertà civili, la giustizia e gli affari interni)[5];
- del comitato[6] e delle singole autorità di protezione dei dati[7], sulla base di un questionario inviato dalla Commissione;
- del riscontro ottenuto dai membri del gruppo multilaterale di esperti a sostegno dell'applicazione del regolamento generale sulla protezione dei dati[8], anch'esso basato su un questionario inviato dalla Commissione;
- dei contributi ad hoc ricevuti dalle parti interessate.

2 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 e ha creato le fondamenta per una cultura autenticamente europea della protezione dei dati, che mira a garantire non soltanto un'interpretazione armonizzata, ma anche un'applicazione e un controllo armonizzati delle norme in materia di protezione dei dati. I suoi pilastri sono costituiti dalle autorità indipendenti nazionali di protezione dei dati e dal comitato di nuova costituzione.

Dato che le autorità di protezione dei dati sono fondamentali per il funzionamento dell'intero sistema di protezione dei dati dell'UE, la Commissione sta monitorando attentamente la loro effettiva indipendenza, anche per quanto riguarda l'adeguatezza delle risorse finanziarie, umane e tecniche.

È ancora troppo presto per valutare appieno il funzionamento dei meccanismi di cooperazione e coerenza, data la breve esperienza acquisita fino a questo momento[9]. Inoltre le autorità di protezione dei dati non hanno ancora utilizzato tutti gli strumenti previsti dal regolamento generale sulla protezione dei dati a sostegno del rafforzamento ulteriormente della loro cooperazione.

---

https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/it/pdf.

[5] 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.

[6] 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.

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

[8] Il gruppo multilaterale di esperti sul regolamento generale sulla protezione dei dati 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.
La relazione del gruppo multilaterale è disponibile al seguente indirizzo: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=21356&Lang=IT.

[9] Questo fatto è evidenziato in particolare anche dal Consiglio nel documento sulla sua posizione e sulle sue conclusioni in merito all'applicazione del regolamento generale sulla protezione dei dati e dal Comitato nel suo contributo alla valutazione.

2.1 Esercizio di poteri rafforzati da parte delle autorità di protezione dei dati

Il regolamento generale sulla protezione dei dati istituisce autorità di protezione dei dati indipendenti conferisce loro poteri di esecuzione armonizzati e rafforzati. Sin da quando si applica il regolamento generale sulla protezione dei dati, tali autorità stanno esercitando un'ampia serie di poteri correttivi previsti nel regolamento generale sulla protezione dei dati, quali sanzioni amministrative (22 autorità UE/SEE)[10], avvertimenti e ammonimenti (23), provvedimenti che intimano di ottemperare alle richieste dell'interessato (26), provvedimenti che intimano di conformare i trattamenti alle disposizioni del regolamento generale sulla protezione dei dati (27) nonché provvedimenti che intimano la rettifica, la cancellazione di dati personali o la limitazione del trattamento (17). Circa la metà delle autorità di protezione dei dati (13) ha imposto limitazioni provvisorie o definitive al trattamento, inclusi divieti di trattamento. Ciò dimostra un uso consapevole di tutte le misure correttive previste nel regolamento generale sulla protezione dei dati; le autorità di protezione dei dati non hanno esitato ad imporre sanzioni amministrative pecuniarie in aggiunta o in sostituzione di altre misure correttive, a seconda delle circostanze dei singoli casi.

Sanzioni amministrative pecuniarie

Tra il 25 maggio 2018 e il 30 novembre 2019 sono state 22 le autorità di protezione dei dati dell'UE/del SEE che hanno inflitto approssimativamente 785 sanzioni pecuniarie. Soltanto un numero esiguo di autorità non ha ancora imposto sanzioni amministrative pecuniarie, anche se i procedimenti attualmente in corso potrebbero comportare tali sanzioni. La maggior parte delle sanzioni pecuniarie ha riguardato violazioni in relazione ai seguenti aspetti: il principio di liceità; il consenso valido; la protezione di dati sensibili; l'obbligo di trasparenza, i diritti degli interessati; nonché violazioni dei dati.

Esempi di sanzioni pecuniarie imposte dalle autorità di protezione dei dati comprendono[11]:

- 200 000 EUR per il mancato rispetto del diritto di opposizione alla commercializzazione diretta in Grecia;
- 220 000 EUR nei confronti di un'impresa di intermediario di dati in Polonia per non aver informato le persone fisiche del trattamento in corso dei loro dati;
- 250 000 EUR nei confronti del campionato di calcio spagnolo LaLiga, per mancanza di trasparenza nella progettazione della sua applicazione per smartphone;
- 14,5 milioni di EUR per la violazione di principi di protezione dei dati, in particolare per la conservazione illecita da parte di una società immobiliare tedesca;
- 18 milioni di EUR per il trattamento illecito di categorie particolari di dati da parte dei servizi postali austriaci;

[10] I dati tra parentesi indicano il numero di autorità di protezione dei dati dell'UE/del SEE che hanno esercitato i poteri elencati tra il mese di maggio del 2018 e la fine di novembre del 2019. Cfr. contributo del comitato alle pagine 32 e 33.

[11] Numerose delle decisioni che hanno inflitto sanzioni pecuniarie sono ancora soggette a controllo giurisdizionale.

- 50 milioni di EUR nei confronti di Google in Francia, in ragione delle condizioni per l'ottenimento del consenso degli utenti.

Il buon esito del regolamento generale sulla protezione dei dati non dovrebbe essere misurato attraverso il numero di sanzioni pecuniarie imposte, dato che tale regolamento prevede una gamma più ampia di poteri correttivi. A seconda delle circostanze, l'effetto deterrente di un divieto di trattamento o della sospensione di flussi di dati può essere ad esempio molto più rilevante.

Questioni specifiche per il settore pubblico

Il regolamento generale sulla protezione dei dati consente agli Stati membri di stabilire se e in quale misura possano essere imposte sanzioni amministrative pecuniarie alle autorità e agli organismi pubblici. Qualora gli Stati membri si avvalgano di tale possibilità, ciò non priva le autorità di protezione dei dati della possibilità di esercitare tutti gli altri poteri correttivi nei confronti di autorità ed organismi pubblici[12].

Un'ulteriore questione specifica è il controllo degli organi giurisdizionali: sebbene il regolamento generale sulla protezione dei dati si applichi anche alle attività degli organi giurisdizionali, questi ultimi sono esonerati dal controllo da parte delle autorità di protezione dei dati nell'esercizio delle loro funzioni giurisdizionali. Tuttavia la Carta e il TFUE impongono agli Stati membri l'obbligo di incaricare un organismo indipendente all'interno dei loro rispettivi sistemi giudiziari affinché vigilino in merito a tali operazioni di trattamento[13].

Cooperazione con altre autorità di regolamentazione

Come annunciato nella propria comunicazione del luglio del 2019, la Commissione sostiene l'interazione con altre autorità di regolamentazione, nel pieno rispetto delle rispettive competenze. Settori promettenti di cooperazione comprendono la tutela dei consumatori e la concorrenza. Il comitato ha espresso la propria intenzione di collaborare con altre autorità di regolamentazione, in particolare per quanto riguarda la concentrazione nei mercati digitali[14]. La Commissione ha riconosciuto l'importanza della protezione della vita privata e dei dati come parametro qualitativo della concorrenza[15]. I membri del comitato hanno partecipato a seminari congiunti con la rete di cooperazione per la tutela dei consumatori in materia di cooperazione per una migliore applicazione della legislazione dell'UE in materia di protezione dei dati e tutela dei consumatori. Tale approccio sarà perseguito per promuovere una comprensione comune e sviluppare modalità pratiche per affrontare problemi concreti incontrati dai consumatori, in particolare nell'economia digitale.

---

12 Articolo 83, paragrafo 7, del regolamento generale sulla protezione dei dati.

13 Articolo 8, paragrafo 3, della Carta; Articolo 16, paragrafo 2, TFUE; considerando 20 del regolamento generale sulla protezione dei dati.

14 Cfr. la dichiarazione del comitato europeo per la protezione dei dati in merito alle ripercussioni delle concentrazioni economiche sulla protezione dei dati , https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_it.pdf.

15 Cfr. il caso COMP M. 8124 Microsoft/LinkedIn.

Al fine di garantire un approccio coerente alla tutela della vita privata e alla protezione dei dati, e in attesa dell'adozione del regolamento sulla vita privata e le comunicazioni elettroniche, è indispensabile una stretta cooperazione con le autorità competenti per l'applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche[16], la lex specialis nel settore delle comunicazioni elettroniche. Una cooperazione più stretta con le autorità competenti ai sensi della direttiva NIS[17] e del gruppo di cooperazione NIS sarebbe reciprocamente vantaggiosa per tali autorità e le autorità di protezione dei dati.

2.2 Il meccanismo di cooperazione e coerenza

Il regolamento generale sulla protezione dei dati ha creato il meccanismo di cooperazione (un sistema di sportello unico per gli operatori, operazioni congiunte e assistenza reciproca tra le autorità di protezione dei dati) e il meccanismo di coerenza al fine di promuovere un'applicazione uniforme delle norme in materia di protezione dei dati, attraverso un'interpretazione coerente e la risoluzione di un eventuale disaccordo tra le autorità ad opera del comitato.

Il comitato, che riunisce tutte le autorità di protezione dei dati, è stato istituito come organismo dell'UE dotato di personalità giuridica ed è pienamente operativo, sostenuto da un segretariato[18] ed è fondamentale per il funzionamento dei due meccanismi di cui sopra. Entro la fine del 2019 il comitato aveva adottato 67 documenti tra i quali 10 orientamenti[19] e 43 pareri[2021] nuovi.

Il ruolo importante del comitato è emerso nel caso in cui era necessario fornire rapidamente un'interpretazione coerente del regolamento generale sulla protezione dei dati e trovare soluzioni immediatamente applicabili a livello UE. Ad esempio, nel contesto della pandemia di Covid-19, nel marzo 2020 il comitato ha adottato una dichiarazione sul trattamento dei dati personali che tratta, tra l'altro, della liceità del trattamento e dell'uso dei dati mobili relativi all'ubicazione in tale contesto[22], mentre nell'aprile del 2020 ha adottato linee guida sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al Covid-19 [23] nonché

---

16 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).

17 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

18 Cfr. dettagli sulle attività del segretariato nel contributo del comitato, pagg. 24-26.

19 In aggiunta ai 10 orientamenti adottati dal gruppo di lavoro Articolo 29 durante il periodo antecedente l'inizio del periodo di applicazione del regolamento generale sulla protezione dei dati e approvati dal comitato. Inoltre il comitato ha adottato 4 orientamenti supplementari tra gennaio e la fine di maggio del 2020 e ha aggiornato una versione esistente.

20 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.

21 Cfr. contributo del comitato, pagg. 18-23, per una panoramica completa delle attività del comitato.

22 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

23 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_it.

linee-guida sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al Covid-19[24]. Il comitato ha inoltre contribuito in maniera significativa alla progettazione dell'approccio dell'UE alle applicazioni di tracciamento da parte della Commissione e degli Stati membri.

La cooperazione quotidiana tra le autorità di protezione dei dati, indipendentemente dal fatto che esse agiscano a proprio nome o in veste di membri del comitato, si basa su scambi di informazioni e notifiche di casi aperti dalle autorità. Al fine di agevolare la comunicazione tra le autorità, la Commissione ha fornito un sostegno significativo mettendo a loro disposizione un sistema di scambio di informazioni[25]. La maggior parte delle autorità lo considera adeguato alle esigenze dei meccanismi di cooperazione e coerenza, anche se potrebbe essere ulteriormente perfezionato ad esempio rendendolo più semplice da utilizzare.

Sebbene sia ancora presto, è già possibile individuare diversi risultati e una serie di sfide che sono presentati in appresso. Tali aspetti dimostrano che, finora, le autorità garanti della protezione dei dati hanno fatto un uso efficace degli strumenti di cooperazione, privilegiando soluzioni più flessibili.

Sportello unico

Come norma generale, nei casi transfrontalieri, l'autorità di protezione dei dati di uno Stato membro può essere coinvolta: i) in quanto autorità capofila quando lo stabilimento principale dell'operatore è ubicato in tale Stato membro; oppure ii) come autorità coinvolta quando l'operatore ha uno stabilimento nel territorio di tale Stato membro, quando le persone fisiche in tale Stato membro sono interessate in maniera sostanziale o quando è stato promosso un reclamo presso tale autorità.

Tale stretta cooperazione è diventata una pratica quotidiana: dalla data di applicazione del regolamento generale sulla protezione dei dati, le autorità di protezione dei dati in tutti gli Stati membri ad un certo punto, sono state individuate come autorità capofila o come autorità interessate nel contesto di casi transfrontalieri, anche se in misura diversa.

Dal maggio 2018 fino alla fine del 2019, l'autorità irlandese di protezione dei dati ha agito in qualità di autorità capofila nel maggior numero di casi transfrontalieri (127), seguita da Germania (92), Lussemburgo (87), Francia (64) e Paesi Bassi (45). Tale classificazione riflette in particolare la situazione specifica dell'Irlanda e del Lussemburgo, che ospitano diverse imprese multinazionali di grandi dimensioni appartenenti al settore tecnologico.

La classificazione varia per quanto concerne il coinvolgimento in veste di autorità di protezione dei dati; l'autorità che risulta essere coinvolta nel maggior numero di casi (435) è infatti quella tedesca, seguita da quella spagnola (337), da quella danese (327), da quella francese (332) e da quella italiana (306)[26].

[24] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_it.pdf.

[25] Sistema di informazione del mercato interno ("IMI").

[26] Cfr. contributo del comitato, pag. 8.

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. Alla data di pubblicazione della presente relazione, sono in corso varie decisioni importanti aventi una dimensione transfrontaliera e soggette al meccanismo dello sportello unico. Tra queste, alcune riguardano imprese multinazionali di grandi dimensioni appartenenti al settore tecnologico[27]. Si prevede che forniscano chiarimenti e contribuiscano a una maggiore armonizzazione nell'interpretazione del regolamento generale sulla protezione dei dati.

Assistenza reciproca

Le autorità di protezione dei dati hanno fatto ampio uso dello strumento di assistenza reciproca.

Alla fine del 2019 risultavano essere state istituite 115 procedure di assistenza reciproca[28], in particolare per lo svolgimento di indagini, la maggior parte delle quali condotte da autorità di protezione dei dati di Spagna (26), Germania (20), Danimarca (13), Polonia (12) e Repubblica ceca (10). L'Irlanda (19), la Francia (11), l'Austria (10), la Germania (10) e il Lussemburgo (9) hanno invece ricevuto la maggior parte delle richieste[29].

La grande maggioranza delle autorità ritiene che l'assistenza reciproca sia uno strumento molto utile per la cooperazione e non ha incontrato particolari ostacoli all'applicazione della procedura di assistenza reciproca. Lo strumento cui le autorità hanno fatto ricorso con maggiore frequenza (ossia in 2 427 procedure) è lo scambio volontario di assistenza reciproca, che non prevede un termine legale o un obbligo rigoroso di risposta. L'autorità di protezione dei dati dell'Irlanda ha inviato e ricevuto il maggior numero di richieste di assistenza reciproca (527 inviate e 359 ricevute), seguita dalle autorità tedesche (260 inviate/356 ricevute).

Al contrario, non sono ancora state condotte operazioni congiunte[30] che consentirebbero alle autorità di protezione dei dati di Stati membri diversi di essere coinvolte già nella fase di indagine in merito a casi transfrontalieri. È in corso una riflessione in seno al comitato sull'attuazione pratica di questo strumento e su come promuoverne l'uso.

Meccanismo di coerenza

Finora è stata utilizzata soltanto la prima parte del meccanismo di coerenza, ossia l'adozione di pareri del comitato[31]. Non è stata invece ancora avviata alcuna procedura di risoluzione delle controversie a livello di comitato[32] o procedura d'urgenza[33].

---

27 Ad esempio, il 22 maggio 2020, l'autorità irlandese di protezione dei dati ha presentato un progetto di decisione ad altre autorità interessate, conformemente all'articolo 60 del regolamento, in merito a un'indagine su Twitter International Company concernente una notifica di violazione dei dati. Lo stesso giorno l'autorità irlandese di protezione dei dati ha altresì annunciato che era in preparazione un progetto di decisione su WhatsApp Ireland Limited per la presentazione di cui all'articolo 60, in materia di trasparenza, anche in relazione alla trasparenza circa le informazioni condivise con Facebook.

28 Articolo 61 del regolamento generale sulla protezione dei dati.

29 Cfr. contributo del comitato, pagg. 12-14.

30 Articolo 62 del regolamento generale sulla protezione dei dati.

31 Sulla base dell'articolo 64 del regolamento generale sulla protezione dei dati.

Tra il 25 maggio 2018 e il 31 dicembre 2019, il comitato ha emesso 36 pareri nel contesto dell'adozione di misure da parte di uno dei suoi membri[34]. La maggior parte di tali pareri (31) riguardava l'adozione di elenchi nazionali di trattamenti che richiedono una valutazione d'impatto sulla protezione dei dati. Due pareri riguardavano le norme vincolanti d'impresa, altri due riguardavano progetti di criteri per l'accreditamento per un organismo di monitoraggio del codice e uno riguardava le clausole contrattuali tipo[35].

Inoltre, il comitato ha adottato sei pareri[36], su richiesta. Tre di tali pareri riguardavano elenchi nazionali che identificavano trattamenti che non richiedevano una valutazione d'impatto sulla protezione dei dati. Gli altri riguardavano rispettivamente, un accordo amministrativo per il trasferimento di dati personali tra autorità di controllo finanziario del SEE e non appartenenti al SEE, l'interazione tra la direttiva relativa alla vita privata e alle comunicazioni elettroniche e il regolamento generale sulla protezione dei dati nonché la competenza di un'autorità di controllo in caso di mutamento delle circostanze relative allo stabilimento principale o unico[37].

Sfide da affrontare

Sebbene le autorità di protezione dei dati collaborino attivamente in seno al comitato e utilizzino già in modo intensivo lo strumento di cooperazione dell'assistenza reciproca, la creazione di una cultura comune veramente incentrata sulla protezione dei dati è ancora un processo in corso.

In particolare la gestione dei casi transfrontalieri richiede un approccio maggiormente efficiente e armonizzato nonché l'uso efficace di tutti gli strumenti di cooperazione previsti dal regolamento generale sulla protezione dei dati. Esiste un ampio consenso su questo aspetto dal momento che è stato sollevato in modi diversi dal Parlamento europeo, dal Consiglio, dal garante europeo della protezione dei dati, dalle parti interessate (all'interno del gruppo multilaterale e più in generale) e dalle autorità di protezione dei dati.

Le principali questioni da affrontare in tale contesto comprendono differenze in relazione a:

- procedure amministrative nazionali riguardanti in particolare: 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, il momento della procedura in cui è concesso il diritto di essere ascoltati o di informazione e la partecipazione, durante il procedimento;
- interpretazioni di concetti relativi al meccanismo di cooperazione, quali le informazioni pertinenti, i concetti di "senza indugio" e "reclamo", il documento che è definito come il "progetto di decisione" dell'autorità di protezione dei dati

---

32 Articolo 65 del regolamento generale sulla protezione dei dati.
33 Articolo 66 del regolamento generale sulla protezione dei dati.
34 Ai sensi dell'articolo 64, paragrafo 1, del regolamento generale sulla protezione dei dati.
35 Articolo 28, paragrafo 8, del regolamento generale sulla protezione dei dati.
36 Ai sensi dell'articolo 64, paragrafo 2, del regolamento generale sulla protezione dei dati.
37 Cfr. contributo del comitato, pag. 15.

capofila, la composizione amichevole (in particolare la procedura per giungere a una composizione amichevole e la forma giuridica di tale composizione); e

- l'approccio in merito al momento per l'avvio della procedura di cooperazione, per il coinvolgimento delle autorità di protezione dei dati competenti e per la comunicazione di informazioni a tali autorità. I reclamanti non dispongono di chiarezza in merito alle modalità di gestione dei loro casi in situazioni transfrontaliere, come è stato sottolineato da diversi membri del gruppo multilaterale. Inoltre le imprese indicano che in alcuni casi le autorità nazionali di protezione dei dati non hanno deferito i casi all'autorità di protezione dei dati capofila, ma li hanno gestiti come casi locali.

La Commissione accoglie con favore l'annuncio del comitato nel quale informa di aver avviato una riflessione su come affrontare tali preoccupazioni. Il comitato ha indicato in particolare che chiarirà le fasi procedurali previste dalla cooperazione tra l'autorità di protezione dei dati capofila e le autorità di protezione dei dati coinvolte, analizzerà il diritto processuale amministrativo nazionale, si adopererà per definire un'interpretazione comune dei concetti fondamentali e rafforzerà la comunicazione e la cooperazione (comprese le operazioni congiunte). La riflessione e l'analisi del comitato dovrebbero condurre all'elaborazione di modalità di lavoro più efficienti nei casi transfrontalieri[38], anche basandosi sulle competenze dei suoi membri e rafforzando la partecipazione del suo segretariato. Occorre inoltre osservare che l'incarico affidato al comitato di garantire un'interpretazione coerente del regolamento generale sulla protezione dei dati non può essere soddisfatto semplicemente individuando il denominatore comune più basso.

Infine, trattandosi di un organismo dell'UE, il comitato deve applicare il diritto amministrativo dell'UE e garantire la trasparenza del processo decisionale.

2.3 Consulenza e orientamenti

Attività di sensibilizzazione e consulenza da parte delle autorità di protezione dei dati

Diverse autorità di protezione dei dati hanno creato strumenti nuovi, quali linee telefoniche di assistenza dedicate alle persone fisiche e alle imprese nonché strumentari per le imprese[39]. Numerosi operatori accolgono con favore il pragmatismo dimostrato da tali autorità nel fornire assistenza nell'applicazione del regolamento generale sulla protezione dei dati. In particolare numerose di tali autorità hanno collaborato e comunicato attivamente e strettamente con i responsabili della protezione dei dati, anche attraverso associazioni di responsabili della protezione dei dati. Numerose autorità hanno inoltre pubblicato orientamenti riguardanti il ruolo e gli obblighi dei responsabili della protezione dei dati a sostegno di questi ultimi durante le loro attività quotidiane e hanno organizzato seminari specificamente concepiti per loro. Tuttavia ciò non vale per tutte le autorità di protezione dei dati.

I riscontri ricevuti dalle parti interessate richiamano l'attenzione anche su una serie di questioni riguardanti gli orientamenti e la consulenza:

---

[38] Come sottolineato anche nella posizione e nelle conclusioni del Consiglio.
[39] Cfr. punto 7 in appresso.

- la mancanza di un approccio e di orientamenti coerenti tra le autorità nazionali di protezione dei dati su talune questioni (ad esempio in materia di cookie[40], applicazione dell'interesse legittimo, notifiche di violazioni dei dati o valutazioni d'impatto sulla protezione dei dati) o anche tra autorità di protezione dei dati all'interno di uno stesso Stato membro (ad esempio in Germania sui concetti di titolare del trattamento e responsabile del trattamento);
- l'incoerenza degli orientamenti adottati a livello nazionale rispetto a quelli adottati dal comitato;
- l'assenza di consultazioni pubbliche su determinati orientamenti adottati a livello nazionale;
- livelli diversi di coinvolgimento con le parti interessate tra le autorità di protezione dei dati;
- ritardi nella ricezione di risposte a richieste di informazioni;
- difficoltà nell'ottenere una consulenza pratica e preziosa da parte delle autorità di protezione dei dati;
- la necessità di aumentare il livello delle competenze settoriali presso talune autorità di protezione dei dati (ad esempio nel settore sanitario e in quello farmaceutico).

Numerose di queste questioni sono legate anche alla mancanza di risorse presso diverse autorità di protezione dei dati (cfr. in appresso).

Prassi divergenti per quanto concerne la notifica di violazioni dei dati[41]

Sebbene il comitato sottolinei l'onere causato da tali notifiche, vi sono notevoli discrepanze nelle notifiche tra gli Stati membri: sebbene da maggio 2018 a fine novembre 2019 nella maggior parte degli Stati membri il numero totale di notifiche di violazioni dei dati sia stato inferiore a 2 000 e in 7 Stati membri compreso tra il 2 000 e 10 000, le autorità di protezione dei dati di Paesi Bassi e Germania hanno riferito rispettivamente 37 400 e 45 600 notifiche[42].

Ciò potrebbe indicare una mancanza di coerenza nell'interpretazione e nell'attuazione, nonostante l'esistenza di orientamenti a livello UE in materia di notifiche delle violazioni dei dati.

[40] In attesa dell'adozione del regolamento sulla vita privata e le comunicazioni elettroniche, è necessaria una stretta cooperazione con le autorità competenti responsabili dell'applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche negli Stati membri. Conformemente a tale direttiva, in taluni Stati membri le autorità competenti per l'applicazione dell'articolo 5, paragrafo 3, della direttiva relativa alla vita privata e alle comunicazioni elettroniche (che stabiliscono le condizioni in base alle quali possono essere installati i "cookie" e che hanno accesso alle apparecchiature terminali di un utente) non sono le stesse delle autorità di controllo del regolamento generale sulla protezione dei dati.

[41] Articolo 33 del regolamento generale sulla protezione dei dati.

[42] Cfr. contributo del comitato, pag. 35.

Orientamenti del comitato europeo per la protezione dei dati

Ad oggi il comitato ha adottato più di 20 orientamenti riguardanti aspetti fondamentali del regolamento generale sulla protezione dei dati[43]. Gli orientamenti costituiscono uno strumento essenziale per un'applicazione coerente del regolamento generale sulla protezione dei dati e sono stati pertanto accolti in larga misura con favore dalle parti interessate. Le parti interessate hanno apprezzato la consultazione pubblica sistematica (da 6 a 8 settimane), chiedono tuttavia un dialogo più intenso con il comitato. In tale contesto la pratica di organizzare seminari su temi mirati prima di redigere orientamenti dovrebbe essere proseguita e ampliata per garantire la trasparenza, l'inclusività e la pertinenza dei lavori del comitato. Le parti interessate chiedono inoltre che l'interpretazione delle questioni più controverse sia affrontata negli orientamenti, dal momento che sono oggetto di una consultazione pubblica, e non nel contesto di pareri di cui all'articolo 64, paragrafo 2, del regolamento generale sulla protezione dei dati. Talune parti interessate chiedono inoltre orientamenti più pratici che specifichino l'applicazione di concetti e disposizioni del regolamento generale sulla protezione dei dati[44]. I membri del gruppo multilaterale sottolineano la necessità di fornire esempi più concreti in maniera da ridurre il più possibile le interpretazioni divergenti tra autorità di protezione dei dati. Allo stesso tempo, le richieste di chiarimenti in merito alle modalità di applicazione del regolamento generale sulla protezione dei dati e di fornitura di certezza giuridica non dovrebbero comportare prescrizioni aggiuntive o ridurre i vantaggi dell'approccio basato sul rischio e del principio di responsabilizzazione.

I temi sui quali le parti interessate auspicano ulteriori orientamenti del comitato comprendono: la portata dei diritti degli interessati (anche nei rapporti di lavoro); aggiornamenti in merito al parere sul trattamento basato sull'interesse legittimo; i concetti di titolare del trattamento, contitolari del trattamento e responsabile del trattamento nonché gli accordi necessari tra le parti[45]; l'applicazione del regolamento generale sulla protezione dei dati alle nuove tecnologie (quali la blockchain e l'intelligenza artificiale); il trattamento nel contesto della ricerca scientifica (anche in relazione alla collaborazione internazionale); il trattamento di dati relativi a minori; la pseudonimizzazione e l'anonimizzazione; nonché il trattamento di dati relativi alla salute.

Il comitato ha già riferito che pubblicherà orientamenti su numerosi di questi temi e che i lavori sono già stati avviati in relazione a numerosi di essi (ad esempio sull'applicazione dell'interesse legittimo come base giuridica per il trattamento).

Le parti interessate chiedono al comitato di aggiornare e rivedere gli orientamenti esistenti, se del caso, tenendo conto dell'esperienza acquisita dalla loro pubblicazione e cogliendo l'opportunità per approfondirli se necessario.

---

[43] Lavori sugli orientamenti già avviati prima dell'entrata in vigore del regolamento generale sulla protezione dei dati il 25 maggio 2018 nel contesto del Gruppo di lavoro Articolo 29. Cfr. elenco completo degli orientamenti all'indirizzo: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_it.

[44] Tale aspetto è stato sottolineato anche dal Parlamento europeo e dal Consiglio.

[45] Il comitato sta attualmente preparando orientamenti in materia di titolari del trattamento e responsabili del trattamento.

2.4 Risorse delle autorità di protezione dei dati

Fornire a ciascuna autorità di protezione dei dati le risorse umane, tecniche e finanziarie, nonché i locali e le infrastrutture necessari costituisce un presupposto per l'efficace svolgimento dei loro compiti e l'esercizio dei loro poteri e rappresenta di conseguenza una condizione essenziale per la loro indipendenza[46].

La maggior parte delle autorità di protezione dei dati ha beneficiato di un aumento del personale e delle risorse dall'entrata in vigore del regolamento generale sulla protezione dei dati nel 2016[47]. Tuttavia numerose di esse segnalano ancora di non disporre di risorse sufficienti[48].

Numero di membri del personale che lavorano per le autorità nazionali di protezione dei dati

Tra il 2016 e il 2019 il numero totale di dipendenti delle autorità di protezione dei dati del SEE considerate congiuntamente è aumentato del 42 % (del 62 % se si considerano le previsioni del 2020).

Il numero di membri del personale è aumentato nella maggior parte delle autorità durante questo periodo e il maggior incremento (in percentuale) è stato registrato per le autorità di Irlanda (+ 169 %), Paesi Bassi (+ 145 %), Islanda (+ 143 %), Lussemburgo (+ 126 %) e Finlandia (+ 114 %). Al contrario il personale è diminuito presso diverse autorità di protezione dei dati e le diminuzioni più marcate sono state osservate in Grecia (- 15 %), Bulgaria (- 14 %), Estonia (- 11 %), Lettonia (- 10 %) e Lituania (- 8 %). Presso talune autorità la diminuzione del personale è dovuta anche al fatto che gli esperti in materia di protezione dei dati hanno lasciato le autorità preferendo il settore privato che offre loro condizioni più interessanti.

In generale le previsioni per il 2020 prevedono un aumento del personale rispetto al 2019, fatta eccezione per le autorità di Austria, Bulgaria, Italia, Svezia e Islanda (presso le quali il personale dovrebbe rimanere stabile), Cipro e Danimarca (presso le quali è prevista una riduzione del personale).

Le autorità di protezione dei dati tedesche[49] presentano congiuntamente il numero più elevato di membri del personale (888 nel 2019/previsione di 1002 nel 2020), seguite dalle autorità di protezione dei dati in Polonia (238/260), Francia (215/225), Spagna (170/220), Paesi Bassi (179/188), Italia (170/170) e Irlanda (140/176).

Le autorità di protezione dei dati con il minor numero di membri del personale sono quelle di Cipro (24/22), Lettonia (19/31), Islanda (17/17), Estonia (16/18) e Malta (13/15).

---

[46] Cfr. l'articolo 52, paragrafo 4, del regolamento generale sulla protezione dei dati.

[47] Il regolamento è entrato in vigore nel maggio del 2016 e si applica dal maggio del 2018, dopo un periodo transitorio di 2 anni.

[48] Cfr. contributo del comitato, pagg. 26-30.

[49] In Germania vi sono 18 autorità, una delle quali è un'autorità federale e 17 autorità regionali (di cui due in Baviera).

Bilancio delle autorità nazionali di protezione dei dati

Tra il 2016 e il 2019 il bilancio totale delle autorità di protezione dei dati del SEE considerate congiuntamente è aumentato del 49 % (del 64 % se si considerano le previsioni del 2020).

Il bilancio della maggior parte delle autorità è aumentato durante questo periodo, facendo registrare il maggior incremento (in percentuale) per le autorità di Irlanda (+ 223 %), Islanda (+ 167 %), Lussemburgo (+ 165 %), Paesi Bassi (+ 130 %) e Cipro (+ 114 %). Al contrario alcune autorità hanno registrato soltanto un lieve aumento del bilancio e tra di esse gli aumenti di entità minore sono stati registrati per le autorità di protezione dei dati di Estonia (7 %), Lettonia (4 %), Romania (3 %) e Belgio (1 %), mentre in Francia l'autorità ha registrato una diminuzione (- 2 %).

In generale le previsioni per il 2020 prevedono un aumento del bilancio rispetto al 2019, fatta eccezione per le autorità di Austria, Bulgaria, Estonia e Paesi Bassi (i cui bilanci dovrebbero rimanere stabili).

Le autorità di protezione dei dati che presentano il bilancio più elevato sono quelle di Germania (76,6 milioni di EUR nel 2019/85,8 milioni di EUR nelle previsioni per il 2020), Italia (29,1/30,1), Paesi Bassi (18,6/18,6), Francia (18,5/20,1) e Irlanda (15,2/16,9).

Le autorità con il bilancio più basso sono quelle di Croazia (1,2 milioni di EUR nel 2019/1,4 milioni di EUR nel 2020), Romania (1,1/1,3), Lettonia (0,6/1,2), Cipro (0,5/0,5) e Malta (0,5/0,6).

La tabella di cui all'allegato II fornisce una panoramica delle risorse umane e di bilancio delle autorità nazionali di protezione dei dati.

Oltre a incidere sulla loro capacità di applicare le norme a livello nazionale, la mancanza di risorse limita anche la capacità delle autorità di protezione dei dati di partecipare e contribuire ai meccanismi di cooperazione e coerenza, nonché al lavoro svolto in seno al comitato. Come sottolineato dal comitato, il successo del meccanismo dello sportello unico dipende dal tempo e dallo sforzo che le autorità di protezione dei dati possono dedicare al trattamento e alla cooperazione di singoli casi transfrontalieri. La questione delle risorse è aggravata dal maggiore ruolo svolto dalle autorità nel controllo di sistemi informatici su larga scala attualmente in fase di sviluppo. Le autorità di protezione dei dati in Irlanda e Lussemburgo necessitano altresì di risorse specifiche, dato il loro ruolo di autorità capofila per l'applicazione del regolamento generale sulla protezione dei dati nei confronti di imprese tecnologiche di grandi dimensioni ubicate principalmente in tali Stati membri.

Sebbene il comitato menzioni l'impatto del meccanismo di cooperazione e le sue scadenze per quanto concerne il lavoro delle autorità di protezione dei dati[50], il regolamento generale sulla protezione dei dati impone agli Stati membri di fornire alle autorità nazionali di protezione dei dati risorse umane, finanziarie e tecniche adeguate[51].

[50] Articolo 60 del regolamento generale sulla protezione dei dati.
[51] Articolo 52, paragrafo 4, del regolamento generale sulla protezione dei dati.

La segreteria del comitato, fornita dal garante europeo della protezione dei dati[52], è attualmente composta da 20 persone, tra cui esperti giuridici, informatici e di comunicazione. Occorre valutare se tale dato debba evolvere in futuro alla luce dell'effettivo adempimento della sua funzione di sostegno analitico, amministrativo e logistico al comitato e ai suoi sottogruppi, anche attraverso la gestione del sistema di scambio di informazioni.

3 NORME ARMONIZZATE, TUTTAVIA PERSISTE UN CERTO GRADO DI FRAMMENTAZIONE E APPROCCI DIVERGENTI

Il regolamento generale sulla protezione dei dati definisce un approccio coerente alle norme in materia di protezione dei dati in tutta l'UE, che sostituisce i diversi regimi nazionali esistenti ai sensi della direttiva del 1995 sulla protezione dei dati.

3.1 Attuazione del regolamento generale sulla protezione dei dati da parte degli Stati membri

Il regolamento generale sulla protezione dei dati è direttamente applicabile in tutti gli Stati membri dal 25 maggio 2018. Ha imposto agli Stati membri di legiferare in particolare per istituire autorità nazionali di protezione dei dati e definire le condizioni generali per i loro membri, al fine di garantire che ciascuna autorità agisca in maniera pienamente indipendente nello svolgimento dei suoi compiti e nell'esercizio dei suoi poteri conformemente al regolamento generale sulla protezione dei dati. Gli obblighi giuridici e i compiti pubblici possono costituire una base giuridica per il trattamento di dati personali soltanto se sono previsti dal diritto (dell'Unione o) nazionale. Inoltre gli Stati membri devono stabilire norme in materia di sanzioni, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie e devono conciliare il diritto alla protezione dei dati personali con il diritto alla libertà di espressione e di informazione. Il diritto nazionale può oltre prevedere una base giuridica per l'esenzione dal divieto generale di trattare categorie speciali di dati personali ad esempio per motivi di interesse pubblico rilevante nel settore della sanità pubblica, compresa la protezione da gravi minacce per la salute a carattere transfrontaliero. Inoltre gli Stati membri devono garantire l'accreditamento degli organismi di certificazione.

La Commissione sta monitorando l'attuazione del regolamento generale sulla protezione dei dati nella legislazione nazionale. Al momento della stesura della presente relazione, tutti gli Stati membri fatta eccezione per la Slovenia, hanno adottato una nuova legislazione in materia di protezione dei dati o hanno adattato la propria legislazione in questo settore. La Commissione ha pertanto chiesto alla Slovenia di fornire chiarimenti sui progressi compiuti finora e la ha esortata a portare a termine tale processo[53].

---

[52] Articolo 75 del regolamento generale sulla protezione dei dati.

[53] 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.

Inoltre la conformità della normativa nazionale rispetto alle norme in materia di protezione dei dati per quanto riguarda l'*acquis* di Schengen è valutata anche nel contesto del meccanismo di valutazione Schengen coordinato dalla Commissione. La Commissione e gli Stati membri valutano congiuntamente le modalità con cui i paesi attuano e applicano l'*acquis* di Schengen in numerosi settori; per la protezione dei dati, ciò riguarda sistemi informatici di larga scala quali il sistema d'informazione Schengen e il sistema informativo Via e comprende il ruolo delle autorità di protezione dei dati nel controllo del trattamento di dati personali nel contesto di tali sistemi.

I lavori per l'adeguamento delle normative settoriali sono ancora in corso a livello nazionale. In seguito all'integrazione del regolamento generale sulla protezione dei dati nell'accordo sullo Spazio economico europeo, la sua applicazione è stata estesa alla Norvegia, all'Islanda e al Liechtenstein. Anche tali paesi hanno adottato le proprie normative nazionali in materia di protezione dei dati.

La Commissione utilizzerà 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.

Principali questioni relative all'attuazione nazionale

Le principali questioni individuate finora nel quadro della valutazione in corso della legislazione nazionale e degli scambi bilaterali con gli Stati membri comprendono:

- restrizioni all'applicazione del regolamento generale sulla protezione dei dati: taluni Stati membri escludono ad esempio del tutto le attività del parlamento nazionale;
- differenze nell'applicabilità delle normative nazionali specifiche. Taluni Stati membri collegano l'applicabilità del loro diritto nazionale al luogo in cui i beni o i servizi sono offerti, altri al luogo di stabilimento del titolare del trattamento o del responsabile del trattamento. Ciò è in contrasto con l'obiettivo di armonizzazione perseguito dal regolamento generale sulla protezione dei dati;
- normative nazionali che sollevano interrogativi sulla proporzionalità dell'ingerenza nel diritto alla protezione dei dati. La Commissione ad esempio ha avviato una procedura di infrazione nei confronti di uno Stato membro che aveva adottato una normativa che imponeva ai giudici di divulgare informazioni specifiche sulle loro attività non professionali, una circostanza incompatibile con il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali[54];
- l'assenza di un organismo indipendente per il controllo del trattamento dei dati da parte degli organi giurisdizionali che agiscono nell'esercizio delle loro funzioni giurisdizionali[55];

[54] La procedura di infrazione riguarda la legge polacca del 20 dicembre 2019 sulla magistratura che incide sull'indipendenza dei giudici e riguarda, tra l'altro, la divulgazione del coinvolgimento dei giudici in attività non professionali: https://ec.europa.eu/commission/presscorner/detail/it/ip_20_772.

[55] Cfr. articolo 8, paragrafo 3, della Carta; articolo 16 TFUE; considerando 20 del regolamento generale sulla protezione dei dati.

- la legislazione in settori pienamente regolamentati dal regolamento generale sulla protezione dei dati al di là del margine per specificazioni o limitazioni. Si tratta, in particolare, del caso in cui le disposizioni nazionali stabiliscono condizioni per il trattamento sulla base di un interesse legittimo, prevedendo la definizione di un equilibrio tra i rispettivi interessi del titolare del trattamento e delle persone fisiche interessate, mentre il regolamento generale sulla protezione dei dati impone a ciascun titolare del trattamento di definire tale equilibrio caso per caso e di avvalersi di tale base giuridica;
- specifiche e prescrizioni aggiuntive che vanno al di là del trattamento per il rispetto di un obbligo giuridico o dell'adempimento di una funzione pubblica (ad esempio per la videosorveglianza nel settore privato o per il marketing diretto); nonché per i concetti utilizzati nel regolamento generale sulla protezione dei dati (ad esempio "su larga scala" o "cancellazione").

Talune di queste questioni possono essere chiarite dalla Corte di giustizia in casi ancora pendenti[56].

Conciliazione del diritto alla protezione dei dati personali con la libertà di espressione e di informazione

Una questione specifica riguarda l'attuazione dell'obbligo per gli Stati membri di conciliare, per legge, il diritto alla protezione dei dati personali con la libertà di espressione e di informazione[57]. La questione è molto complessa in quanto una valutazione dell'equilibrio tra tali diritti fondamentali deve tenere conto anche delle disposizioni e delle garanzie previste dalla normativa in materia di stampa e mezzi d'informazione.

La valutazione della legislazione degli Stati membri mostra approcci diversi alla conciliazione del diritto alla protezione dei dati personali con quello alla libertà di espressione e di informazione:

- taluni Stati membri stabiliscono il principio del primato della libertà di espressione o esentano in linea di principio dall'applicazione di interi capi di cui all'articolo 85, paragrafo 2, del regolamento generale sulla protezione dei dati in caso di trattamento per finalità giornalistiche e di espressione accademica, artistica e letteraria. In una certa misura la normativa sui media prevede alcune garanzie per quanto riguarda i diritti degli interessati;
- taluni Stati membri 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;
- 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.

[56] Ad esempio l'esenzione di una commissione parlamentare dall'applicazione del regolamento generale sulla protezione dei dati è oggetto di una causa pendente per una pronuncia pregiudiziale (C-272/19).

[57] Articolo 85 del regolamento generale sulla protezione dei dati.

La Commissione proseguirà la propria valutazione della legislazione nazionale sulla base delle prescrizioni di cui alla Carta. La conciliazione deve essere prevista dalla legge, rispettare il contenuto essenziale di tali diritti fondamentali ed essere proporzionata e necessaria (articolo 52, paragrafo 1, della Carta). Le norme in materia di protezione dei dati non dovrebbero pregiudicare l'esercizio della libertà di espressione e di informazione, in particolare creando un effetto dissuasivo o essendo interpretate come un modo per esercitare pressioni sui giornalisti affinché divulghino le loro fonti.

3.2 Clausole di specificazione facoltative e loro limiti

Il regolamento generale sulla protezione dei dati lascia agli Stati membri la possibilità di specificare ulteriormente la sua applicazione in un numero limitato di settori. Tale margine per la legislazione nazionale deve essere distinto dall'obbligo di attuare talune altre disposizioni del regolamento generale sulla protezione dei dati di cui sopra. Le clausole di specificazione facoltative sono elencate nell'allegato I.

I margini per il diritto degli Stati membri sono soggetti alle condizioni e ai limiti stabiliti dal regolamento generale sulla protezione dei dati e non consentono un regime nazionale parallelo di protezione dei dati[58]. Gli Stati membri sono tenuti a modificare o abrogare le leggi nazionali in materia di protezione dei dati, compresa la legislazione settoriale contenente aspetti relativi alla protezione dei dati.

Inoltre il diritto nazionale degli Stati membri in materia non deve includere disposizioni che potrebbero creare confusione per quanto riguarda l'applicazione diretta del regolamento generale sulla protezione dei dati. Di conseguenza laddove il regolamento generale sulla protezione dei dati preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, questi ultimi possono integrare nel loro diritto nazionale elementi di tale regolamento, nella misura necessaria a garantire la coerenza e rendere le disposizioni nazionali comprensibili per le persone alle quali esse si applicano[59].

Le parti interessate ritengono che gli Stati membri dovrebbero ridurre o astenersi dall'utilizzare clausole di specificazione facoltative, in quanto non contribuiscono all'armonizzazione. Le divergenze nazionali nell'attuazione delle normative e nella loro interpretazione da parte delle autorità di protezione dei dati aumentano notevolmente il costo della conformità giuridica in tutta l'UE.

Frammentazione legata all'uso di clausole di specificazione facoltative

- Limiti di età per il consenso da parte di minori per servizi della società dell'informazione

Taluni Stati membri si sono avvalsi della possibilità di prevedere un'età inferiore a 16 anni per il consenso in relazione ai servizi della società dell'informazione (articolo 8, paragrafo 1, del regolamento generale sulla protezione dei dati). Mentre nove Stati membri applicano il limite di 16 anni, otto Stati membri hanno optato per 13 anni, sei per 14 anni e tre per 15 anni[60].

Di conseguenza un'impresa che fornisce servizi della società dell'informazione a minori in tutta l'UE deve distinguere tra i limiti di età dei potenziali utenti, a seconda dello Stato membro in cui risiedono. Ciò è in contrasto con l'obiettivo fondamentale

---

[58] Il termine ampiamente utilizzato di "clausole di apertura" per indicare le clausole di specificazione è fuorviante, in quanto potrebbe dare l'impressione che gli Stati membri abbiano margini di manovra che vanno oltre le disposizioni del regolamento.

[59] Considerando 8 del regolamento generale sulla protezione dei dati.

[60] 13 anni per Belgio, Danimarca, Estonia, Finlandia, Lettonia, Malta, Portogallo e Svezia; 14 anni per Austria, Bulgaria, Cipro, Spagna, Italia e Lituania; 15 anni per Repubblica ceca, Grecia e Francia; 16 anni per Germania, Ungheria, Croazia, Irlanda, Lussemburgo, Paesi Bassi, Polonia, Romania e Slovacchia.

del regolamento generale sulla protezione dei dati di garantire un livello omogeneo di protezione alle persone fisiche e di opportunità commerciali in tutti gli Stati membri.

Tali differenze determinano situazioni nelle quali lo Stato membro in cui è stabilito il titolare del trattamento prevede un limite di età diverso dagli Stati membri nei quali risiedono gli interessati.

- Salute e ricerca

Nell'applicare deroghe al divieto generale di trattare categorie particolari di dati personali[61], la legislazione degli Stati membri segue approcci diversi per quanto concerne il livello di specificazione e le garanzie, anche per finalità sanitarie e di ricerca. La maggior parte degli Stati membri ha introdotto o mantenuto ulteriori condizioni per il trattamento di dati genetici, biometrici o relativi alla salute. Ciò è vero anche per le deroghe relative ai diritti degli interessati per finalità di ricerca[62], per quanto concerne tanto la portata delle deroghe quanto le relative garanzie.

Gli orientamenti futuri del comitato sull'uso dei dati personali nel settore della ricerca scientifica contribuiranno a un approccio armonizzato in tale contesto. 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 effettivi che le sono pervenute dalla comunità scientifica. Sarebbe utile che tali orientamenti possano essere adottati prima dell'avvio del programma quadro Orizzonte Europa al fine di armonizzare le pratiche di protezione dei dati e facilitare la condivisione dei dati in merito ai progressi della ricerca. Anche orientamenti del comitato in merito al trattamento di dati personali nel settore della salute potrebbero essere utili.

Il regolamento generale sulla protezione dei dati prevede un quadro solido per la legislazione nazionale nel settore della sanità pubblica e include esplicitamente le minacce sanitarie transfrontaliere e il controllo delle epidemie e della loro diffusione[63], un aspetto rilevante nel contesto della lotta contro la pandemia di Covid-19.

A livello UE, l'8 aprile 2020 la Commissione ha adottato una raccomandazione relativa a un insieme di strumenti per l'uso di tecnologia e dati in questo contesto, comprese le applicazioni mobili e l'uso di dati di mobilità resi anonimi[64], mentre il 16 aprile 2020 ha pubblicato orientamenti sulle app a sostegno della lotta alla pandemia di Covid-19 relativamente alla protezione dei dati[65]. Il comitato ha pubblicato una dichiarazione sul trattamento di dati in tale contesto il 19 marzo 2020[66], seguita il 21 aprile 2020 da linee guida sul trattamento di dati per finalità di ricerca e sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti in tale contesto[67]. Tali raccomandazioni e linee guida chiariscono in che modo i principi e le norme in materia di protezione dei dati personali si applicano nel contesto della lotta alla pandemia.

---

61 Articolo 9 del regolamento generale sulla protezione dei dati.

62 Articolo 89, paragrafo 2, del regolamento generale sulla protezione dei dati.

63 Cfr. articolo 9, paragrafo 2, lettera i), del regolamento generale sulla protezione dei dati e il considerando 46 dello stesso.

64 https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.

65 https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=IT.

66 https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_it.

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

- Limitazioni di ampia portata dei diritti dell'interessato

La maggior parte delle normative nazionali in materia di protezione dei dati che limitano i diritti degli interessati non specificano gli obiettivi di interesse pubblico generale tutelati da tali limitazioni e/o non soddisfano in misura sufficiente le condizioni e le garanzie richieste dall'articolo 23, paragrafo 2, del regolamento generale sulla protezione dei dati[68]. Diversi Stati membri non lasciano spazio per la verifica della proporzionalità o estendono le limitazioni persino oltre l'ambito di applicazione dell'articolo 23, paragrafo 1, del regolamento generale sulla protezione dei dati. Talune normative nazionali negano il diritto di accesso per motivi di sforzo sproporzionato da parte del titolare del trattamento per dati personali conservati sulla base di un obbligo di conservazione o connessi allo svolgimento di compiti di servizio pubblico senza circoscrivere tale limitazione agli obiettivi di interesse pubblico generale.

- Prescrizioni aggiuntive per le imprese

Sebbene l'obbligo di disporre di un responsabile della protezione dei dati si basi sull'approccio basato sul rischio[69], uno Stato membro[70] lo ha esteso sulla base di criteri quantitativi, obbligando le imprese che hanno 20 o più dipendenti, coinvolte in maniera permanente nel trattamento automatizzato di dati personali, a designare tale figura, indipendentemente dai rischi connessi alle attività di trattamento[71]. Ciò ha determinato oneri aggiuntivi.

4 DARE ALLE PERSONE GLI STRUMENTI D'AZIONE PER CONTROLLARE I PROPRI DATI

Il regolamento generale sulla protezione dei dati rende efficaci i diritti fondamentali, in particolare il diritto alla protezione dei dati personali, ma anche gli altri diritti fondamentali riconosciuti dalla Carta, tra i quali il rispetto della vita privata e della vita familiare, la libertà di espressione e di informazione, la non discriminazione, la libertà di pensiero, di coscienza e di religione, nonché la libertà d'impresa e il diritto a un ricorso effettivo. Tali diritti devono essere esercitati in maniera equilibrata tra loro conformemente al principio della proporzionalità[72].

Il regolamento generale sulla protezione dei dati fornisce alle persone fisiche diritti azionabili, quali il diritto di accesso, rettifica, cancellazione, opposizione, portabilità e maggiore trasparenza; conferisce altresì alle persone fisiche il diritto di proporre reclamo presso un'autorità di protezione dei dati, anche mediante azioni rappresentative, e il diritto al ricorso giurisdizionale.

---

[68] Ad esempio perché ripetono semplicemente la formulazione dell'articolo 23, paragrafo 1, del regolamento generale sulla protezione dei dati.

[69] Articolo 37, paragrafo 1, del regolamento generale sulla protezione dei dati.

[70] Germania.

[71] Facendo ricorso alla clausola di specificazione di cui all'articolo 37, paragrafo 4, del regolamento generale sulla protezione dei dati.

[72] Cfr. considerando 4 del regolamento generale sulla protezione dei dati.

Le persone fisiche sono sempre più consapevoli dei loro diritti, come dimostrato dai risultati dell'Eurobarometro[73] del luglio 2019 e dall'indagine condotta dall'Agenzia dell'Unione europea per i diritti fondamentali[74].

Secondo l'indagine sui diritti fondamentali condotta dall'Agenzia dell'Unione europea per i diritti fondamentali:

- il 69 % della popolazione di età pari o superiore a 16 anni nell'UE ha sentito parlare del regolamento generale sulla protezione dei dati;
- il 71 % dei partecipanti nell'UE ha sentito parlare della propria autorità nazionale di protezione dei dati; tale dato varia dal 90 % della Repubblica ceca al 44 % del Belgio;
- il 60 % dei partecipanti nell'UE è a conoscenza di una legge che consente loro di accedere ai propri dati personali detenuti dalla pubblica amministrazione; tale percentuale scende tuttavia al 51 % per le imprese private;
- più di un partecipante su cinque (23 %) nell'UE non vuole condividere dati personali (quali indirizzo, cittadinanza o data di nascita) con la pubblica amministrazione, mentre il 41 % non vuole condividere tali dati con imprese private.

Le persone fisiche esercitano sempre più spesso il loro diritto di proporre reclamo presso le autorità di protezione dei dati, individualmente o tramite azioni rappresentative[75]. Soltanto alcuni Stati membri hanno consentito alle organizzazioni non governative di avviare azioni senza un mandato, in linea con la possibilità prevista dal regolamento generale sulla protezione dei dati. Una volta adottata, la proposta di direttiva sulle azioni rappresentative a tutela degli interessi collettivi dei consumatori[76] dovrebbe rafforzare il quadro per le azioni rappresentative anche nel settore della protezione dei dati.

Reclami

Il numero totale di reclami promossi tra il mese di maggio del 2018 e la fine di novembre del 2019, come riferito dal comitato, si attesta a circa 275 000[77]. Tuttavia tale dato va considerato con molta cautela, dato che la definizione di reclamo non coincide esattamente tra le autorità. Il numero assoluto di reclami ricevuti dalle autorità di protezione dei dati[78] è molto diverso da uno Stato membro all'altro. I numeri più elevati di reclami sono stati registrati in Germania (67 000), nei Paesi Bassi (37 000), in Spagna e in Francia (18 000 ciascuno), in Italia (14 000), in Polonia e in Irlanda (12 000 ciascuno). Due terzi delle autorità hanno segnalato un numero di reclami compreso tra 8 000 e 600. I numeri più bassi di reclami sono stati registrati in Estonia e in Belgio (circa 500), a Malta e in Islanda (meno di 200 ciascuno).

---

[73] https://ec.europa.eu/commission/presscorner/detail/it/IP_19_2956.

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

[75] Articolo 80 del regolamento generale sulla protezione dei dati.

[76] COM(2018) 184 final - 2018/089 (COD).

[77] Entrambi a norma degli articoli 77 e 80 del regolamento generale sulla protezione dei dati.

[78] Cfr. contributo del comitato, pagg. 31-32.

Il numero di reclami non è necessariamente correlato alle dimensioni della popolazione o al PIL, ad esempio in Germania è stato registrato un numero di reclami pari a quasi il doppio di quello nei Paesi Bassi e a quasi il quadruplo rispetto a Spagna e Francia.

Dal riscontro ricevuto dal gruppo multilaterale emerge che le organizzazioni hanno messo in atto una serie di misure volte a facilitare l'esercizio dei diritti degli interessati, compresi processi di attuazione che garantiscono il riesame individuale delle richieste e una risposta da parte del titolare del trattamento, l'uso di canali diversi (posta, indirizzo di posta elettronica dedicato, sito web, ecc.), politiche e procedure interne aggiornate in materia di trattamento interno tempestivo delle richieste nonché la formazione del personale. Talune imprese hanno messo in atto portali digitali accessibili tramite il sito web dell'impresa (o l'intranet aziendale per i dipendenti) per facilitare l'esercizio dei diritti da parte degli interessati.

Sono necessari tuttavia ulteriori progressi in merito ai seguenti aspetti:

- non tutti i titolari del trattamento sono tenuti a rispettare l'obbligo di agevolare l'esercizio dei diritti degli interessati[79]. Devono garantire che gli interessati dispongano di un punto di contatto efficace cui possano spiegare i loro problemi. Può trattarsi del responsabile della protezione dei dati, i cui recapiti devono essere forniti proattivamente all'interessato[80]. Le modalità di contatto non devono limitarsi alla posta elettronica, ma devono consentire all'interessato altresì di rivolgersi al titolare del trattamento con altri mezzi;
- le persone fisiche che chiedono di accedere ai loro dati continuano a incontrare difficoltà, ad esempio nel caso di piattaforme, intermediari di dati e imprese di tecnologie pubblicitarie;
- il diritto alla portabilità dei dati non viene sfruttato appieno. La strategia europea per la protezione dei dati (in appresso "la strategia in materia di dati")[81], adottata dalla Commissione il 19 febbraio 2020, ha sottolineato la necessità di agevolare tutti gli usi possibili di tale diritto [ad esempio mediante l'obbligo di installare interfacce tecniche e formati leggibili da un dispositivo automatico in maniera da consentire la portabilità dei dati (pressoché) in tempo quasi reale]. Gli operatori osservano che talvolta vi sono difficoltà nel fornire i dati in un formato strutturato, di uso comune e leggibile da un dispositivo automatico (a causa della mancanza di standard). Soltanto le organizzazioni di settori specifici, quali quello bancario, delle telecomunicazioni, dei contatori per l'acqua e il riscaldamento, segnalano di aver messo in atto le interfacce necessarie[82]. Sono stati sviluppati nuovi strumenti tecnologici per facilitare l'esercizio, da parte delle persone fisiche, dei loro diritti ai sensi del regolamento generale sulla protezione dei dati, non limitato alla portabilità dei dati (ad esempio spazi per la conservazione di dati personali e servizi di gestione di informazioni personali);

---

79 Articolo 12, paragrafo 2, del regolamento generale sulla protezione dei dati.

80 Articolo 13, paragrafo 1, lettera b), e articolo 14, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati.

81 https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0066&qid=1596810829005&from=IT.

82 Cfr. relazione del gruppo multilaterale.

- diritti dei minori: numerosi membri del gruppo multilaterale sottolineano la necessità di fornire informazioni ai minori e il fatto che numerose organizzazioni ignorano che i minori possono subire ripercussioni dal trattamento dei dati che li riguardano. Il Consiglio ha sottolineato che si potrebbe prestare particolare attenzione alla protezione dei minori in sede di elaborazione dei codici di condotta. La protezione dei minori è altresì una priorità delle autorità di protezione dei dati[83];
- diritto all'informazione: talune imprese hanno adottato un approccio molto legalistico, considerando un esercizio giuridico le notifiche in materia di protezione dei dati, fornendo informazioni piuttosto complesse, difficili da comprendere o incomplete, mentre il regolamento generale sulla protezione dei dati impone che le informazioni siano concise e impieghino un linguaggio semplice e chiaro[84]. Sembra che talune imprese non seguano le raccomandazioni del comitato, ad esempio per quanto riguarda l'elenco dei nomi delle entità con le quali condividono i dati;
- diversi Stati membri hanno limitato ampiamente i diritti degli interessati attraverso il diritto nazionale e per taluni si sono spinti persino oltre i margini di cui all'articolo 23 del regolamento generale sulla protezione dei dati;
- l'esercizio dei diritti delle persone fisiche è talvolta ostacolato dalle pratiche di pochi attori digitali importanti che rendono difficile a tali persone scegliere le impostazioni che tutelano maggiormente la loro vita privata (in violazione della prescrizione della protezione dei dati fin dalla progettazione e per impostazione predefinita[85])[86].

Le parti interessate attendono con impazienza orientamenti del comitato sui diritti degli interessati.

---

[83] Cfr. risultati di una consultazione pubblica sui diritti dei minori alla protezione dei dati svolta dall'autorità irlandese di protezione dei dati: https://www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf. Anche l'autorità francese di protezione dei dati ha avviato una consultazione pubblica nell'aprile del 2020: https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-sur-les-droits-des-mineurs-dans-lenvironnement-numerique.

[84] Articolo 12, paragrafo 1, del regolamento generale sulla protezione dei dati.

[85] Articolo 25 del regolamento generale sulla protezione dei dati.

[86] Cfr. relazione del consiglio norvegese dei consumatori "*Deceived by Design*" [Ingannati per progettazione], che ha messo in evidenza "modelli oscuri", le impostazioni predefinite e altre caratteristiche e tecniche utilizzate dalle imprese per incoraggiare gli utenti ad optare per opzioni intrusive: https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/.
Cfr. anche la ricerca pubblicata nel dicembre del 2019 dal dialogo transatlantico tra consumatori e dalla Heinrich-Böll-Stiftung Brussels European Union che analizza le pratiche delle tre principali piattaforme globali: https://eu.boell.org/en/2019/12/11/privacy-eu-and-us-consumer-experiences-across-three-global-platforms.

5 OPPORTUNITÀ E SFIDE PER LE ORGANIZZAZIONI, IN PARTICOLARE PER LE PICCOLE E MEDIE IMPRESE

Opportunità per le organizzazioni

Il regolamento generale sulla protezione dei dati promuove la concorrenza e l'innovazione. Unitamente al regolamento sulla libera circolazione dei dati non personali[87], il regolamento generale sulla protezione dei dati garantisce la libera circolazione dei dati all'interno dell'UE e crea parità di condizioni rispetto alle imprese non stabilite nell'UE. Creando un quadro armonizzato per la protezione dei dati personali, il regolamento generale sulla protezione dei dati garantisce che tutti gli attori del mercato interno siano vincolati dalle medesime norme e beneficino delle medesime opportunità, indipendentemente dal fatto che abbiano uno stabilimento e indipendentemente dal luogo in cui avviene il trattamento. La neutralità tecnologica del regolamento generale sulla protezione dei dati fornisce il quadro per la protezione dei dati per quanto concerne i nuovi sviluppi tecnologici. I principi della protezione dei dati fin dalla progettazione e per impostazione predefinita incentivano soluzioni innovative che comprendono fin dall'inizio considerazioni concernenti la protezione dei dati e possono ridurre i costi del rispetto delle norme in tale contesto.

Inoltre la tutela della vita privata diventa un importante parametro competitivo che le persone fisiche tengono sempre più in considerazione nella scelta dei loro servizi. Coloro che sono più informati e sensibili alle considerazioni in materia di protezione dei dati cercano prodotti e servizi che garantiscono un'efficace protezione dei dati personali. L'attuazione del diritto alla portabilità dei dati può ridurre gli ostacoli all'ingresso per le imprese che offrono servizi innovativi e rispettosi della protezione dei dati. Occorre monitorare gli effetti di un uso potenzialmente più ampio di tale diritto sul mercato in diversi settori. Il rispetto delle norme in materia di protezione dei dati e la loro applicazione trasparente creeranno fiducia nell'utilizzo dei dati personali delle persone e quindi nuove opportunità per le imprese.

Come tutti i regolamenti, le norme in materia di protezione dei dati comportano costi di conformità intrinseci per le imprese. Le opportunità e i vantaggi di una maggiore fiducia nell'innovazione digitale e i benefici sociali derivanti dal rispetto di un diritto fondamentale superano tuttavia tali costi. Garantendo parità di condizioni e dotando le autorità di protezione degli strumenti dei quali necessitano per applicare le norme in maniera efficace, il regolamento generale sulla protezione dei dati impedisce alle imprese non conformi di trarre profitto dalla fiducia sviluppata da coloro che rispettano le norme.

Sfide specifiche per le piccole e medie imprese (PMI)

Le parti interessate, ma anche il Parlamento europeo, il Consiglio e le autorità di protezione dei dati, condividono una percezione generale secondo la quale l'applicazione del regolamento generale sulla protezione dei dati è particolarmente complicata in particolare per le microimprese, le piccole e medie imprese e le piccole organizzazioni di volontariato e di beneficenza.

---

[87] 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).

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. L'approccio basato sul rischio associa la flessibilità a una protezione efficace. Tiene conto delle esigenze delle PMI per le quali il trattamento dei dati non costituisce la loro attività principale e ne calibra gli obblighi in particolare in base alla probabilità e alla gravità dei rischi connessi allo specifico trattamento da loro svolto[88].

I trattamenti di piccole dimensioni e a basso rischio non dovrebbero essere trattati allo stesso modo dei trattamenti ad alto rischio e svolti di frequente, indipendentemente dalle dimensioni dell'impresa che li effettua. Di conseguenza, come concluso dal comitato, "in ogni caso, l'approccio basato sul rischio promosso dal legislatore nel testo dovrebbe essere mantenuto, dato che i rischi per gli interessati non dipendono dalle dimensioni dei titolari del trattamento"[89]. Le autorità di protezione dei dati dovrebbero tenere pienamente conto di tale principio in sede di applicazione del regolamento generale sulla protezione dei dati, preferibilmente nell'ambito di un approccio europeo comune, al fine di non creare ostacoli al mercato unico.

Le autorità di protezione dei dati hanno sviluppato diversi strumenti e hanno sottolineato la loro intenzione di migliorarli ulteriormente. Talune autorità hanno avviato campagne di sensibilizzazione e organizzano persino eventi di formazione sul regolamento generale sulla protezione dei dati rivolti alle PMI.

Esempi di orientamenti e strumenti forniti dalle autorità di protezione dei dati in particolare a favore delle PMI

- pubblicazione di informazioni rivolte alle PMI;
- seminari per i responsabili della protezione dei dati ed eventi rivolti alle PMI che non sono tenute a designare un responsabile della protezione dei dati;
- guide interattive per fornire assistenza alle PMI;
- linee telefoniche dirette per consultazioni;
- modelli di contratti per il trattamento e registri dei trattamenti.

Una descrizione delle attività svolte dalle autorità di protezione dei dati è presentata nel contributo del comitato[90].

Numerose delle azioni che sostengono in maniera specifica le PMI hanno ricevuto finanziamenti dell'UE. 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 PMI. Di conseguenza, nel 2018, sono stati assegnati 2 milioni di EUR a nove autorità di protezione dei dati per attività da svolgere nel periodo 2018-2019 (Belgio,

88 Articolo 24, paragrafo 1, del regolamento generale sulla protezione dei dati.
89 Cfr. contributo del comitato, pag. 35.
90 Cfr. contributo del comitato, pagg. 35-45.

Bulgaria, Danimarca, Ungheria, Lituania, Lettonia, Paesi Bassi, Slovenia e Islanda)[91]; mentre nel 2019 è stato assegnato 1 milione di EUR a quattro autorità di protezione dei dati per attività da svolgere nel 2020 (Belgio, Malta, Slovenia e Croazia in collaborazione con l'Irlanda)92. Nel 2020 sarà stanziato un ulteriore milione di EUR.

Nonostante queste iniziative, le PMI e le start-up segnalano spesso di incontrare difficoltà in relazione all'attuazione del principio di responsabilizzazione previsto dal regolamento generale sulla protezione dei dati[93]. Tali soggetti riferiscono in particolare di non ottenere sempre orientamenti e consulenza pratici sufficienti da parte delle autorità nazionali di protezione dei dati o che i tempi necessari per ottenere tali orientamenti e tale consulenza sono troppo lunghi. Vi sono stati anche casi nei quali le autorità si sono dimostrate restie a farsi coinvolgere in merito a questioni giuridiche. Di fronte a situazioni di questo tipo, spesso le PMI si rivolgono a consulenti e avvocati esterni per gestire l'attuazione del principio di responsabilizzazione e dell'approccio basato sul rischio (nonché delle prescrizioni in materia di trasparenza, registri dei trattamenti e notifiche di violazioni dei dati). Ciò può altresì comportare ulteriori costi per tali soggetti.

Una questione specifica è costituita dai registri delle attività di trattamento, considerati dalle PMI e dalle piccole associazioni un onere amministrativo gravoso. L'esenzione da tale obbligo di cui all'articolo 30, paragrafo 5, del regolamento generale sulla protezione dei dati è in effetti molto limitata. Tuttavia gli sforzi corrispondenti per rispettare tale obbligo non dovrebbero essere sovrastimati. Laddove l'attività principale delle PMI non comporti il trattamento di dati personali, tali registri possono essere semplici e non gravosi. Lo stesso vale per le associazioni di volontariato e di altro tipo. Tali registri semplificati sarebbero facilitati da modelli di registri, come già avviene nella pratica per talune autorità di protezione dei dati. In ogni caso tutti coloro che trattano dati personali dovrebbero disporre di un quadro generale del loro trattamento dei dati come requisito di base per il principio di responsabilizzazione.

Lo sviluppo di strumenti pratici a livello UE da parte del comitato, quali moduli armonizzati per le violazioni dei dati e registri semplificati delle attività di trattamento, possono aiutare le PMI e le piccole associazioni[94] le cui attività principali non si concentrano sul trattamento di dati personali ad adempiere ai loro obblighi.

Varie associazioni di categoria hanno compiuto sforzi per sensibilizzare e informare i propri membri ad esempio attraverso conferenze e seminari, fornendo alle imprese informazioni sugli orientamenti disponibili o sviluppando un servizio di assistenza in materia di protezione dei dati a favore dei loro membri. Tali associazioni segnalano altresì un numero crescente di seminari, riunioni ed eventi organizzati da gruppi di riflessione e associazioni di PMI su questioni relative al regolamento generale sulla protezione dei dati.

---

91 https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017.

92 https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_it.

93 Cfr. relazione del gruppo multilaterale.

94 Cfr. contributo del Consiglio.

Al fine di migliorare la libera circolazione di tutti i dati all'interno dell'UE e di istituire un'applicazione coerente del regolamento generale sulla protezione dei dati e il regolamento sulla libera circolazione dei dati non personali, la Commissione ha pubblicato altresì una guida pratica sulle norme che disciplinano il trattamento di serie miste di dati, composte da dati personali e non personali e rivolta in particolare alle PMI[95].

Insieme di strumenti per le imprese

Il regolamento generale sulla protezione dei dati prevede strumenti che contribuiscono a dimostrare la conformità, quali codici di condotta, meccanismi di certificazione e clausole contrattuali tipo.

- Codici di condotta

Il comitato ha emanato linee guida[96] volte a sostenere e agevolare i "titolari dei codici" nella redazione, nella modifica o nell'estensione di codici nonché a fornire orientamenti pratici e assistenza interpretativa. Tali linee guida chiariscono inoltre le procedure per la presentazione, l'approvazione e la pubblicazione dei codici a livello nazionale e UE stabilendo i criteri minimi richiesti.

Le parti interessate ritengono che i codici di condotta siano strumenti decisamente utili. Sebbene a livello nazionale siano attuati numerosi codici, molti codici di condotta a livello UE sono attualmente in fase di preparazione (ad esempio in materia di applicazioni mobili per la salute, ricerca sanitaria nel settore della genomica, cloud computing, marketing diretto, assicurazione, trattamento da parte di servizi di prevenzione e consulenza rivolti a minori)[97]. Gli operatori ritengono che i codici di condotta a livello UE debbano essere promossi in maniera più evidente in quanto favoriscono un'applicazione coerente del regolamento generale sulla protezione dei dati in tutti gli Stati membri.

Tuttavia i codici di condotta richiedono altresì tempo e investimenti da parte degli operatori tanto per il loro sviluppo quanto per la creazione degli organismi di controllo indipendenti richiesti. I rappresentanti delle PMI sottolineano l'importanza e l'utilità di codici di condotta adattati alla loro situazione e che non comportano costi sproporzionati.

Di conseguenza le associazioni di numerosi settori hanno attuato altri tipi di strumenti di autoregolamentazione, quali codici di buone pratiche od orientamenti. Sebbene tali strumenti possano fornire informazioni utili, non beneficiano dell'approvazione da parte delle autorità di protezione dei dati e non possono fungere da strumento per contribuire a dimostrare la conformità rispetto al regolamento generale sulla protezione dei dati.

Il Consiglio sottolinea che i codici di condotta devono prestare particolare attenzione al trattamento dei dati relativi a minori e dei dati sanitari. La Commissione sta

---

[95] Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, COM(2019) 250 final.

[96] https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_it.

[97] Cfr. relazione del gruppo multilaterale.

sostenendo i codici di condotta destinati ad armonizzare l'approccio in materia di sanità e ricerca e a facilitare il trattamento transfrontaliero di dati personali[98]. Il comitato sta per approvare un progetto di requisiti di accreditamento per i codici di condotta degli organismi di controllo, proposti da varie autorità di protezione dei dati[99]. Quando i codici di condotta transnazionali o UE sono pronti per essere sottoposti all'approvazione da parte delle autorità di protezione dei dati, vengono sottoposti a consultazione da parte del comitato. Fare in modo che i codici di condotta siano messi in atto rapidamente è particolarmente importante per i settori che comportano il trattamento di quantità significative di dati (ad esempio il cloud computing) o di dati sensibili (ad esempio, sanità/ricerca).

- Certificazione

La certificazione può essere uno strumento utile per dimostrare il rispetto di prescrizioni specifiche del regolamento generale sulla protezione dei dati. Può aumentare la certezza del diritto per le imprese e promuovere il regolamento generale sulla protezione dei dati a livello mondiale.

Come sottolineato nello studio sulla certificazione pubblicato nell'aprile del 2019[100], l'obiettivo dovrebbe essere quello di facilitare l'adozione di regimi pertinenti. Lo sviluppo di regimi di certificazione nell'UE sarà sostenuto dalle linee guida pubblicate dal comitato sui criteri di certificazione[101] e sull'accreditamento degli organismi di certificazione[102].

La sicurezza e la protezione dei dati fin dalla progettazione sono elementi chiave da considerare nei sistemi di certificazione nel quadro del regolamento generale sulla protezione dei dati che trarrebbero vantaggio da un approccio comune e ambizioso in tutta l'UE. La Commissione continuerà a sostenere i contatti attuali tra l'agenzia dell'Unione europea per la cibersicurezza (ENISA), le autorità di protezione dei dati e il comitato.

Per quanto riguarda la cibersicurezza, a seguito dell'adozione del regolamento sulla cibersicurezza, la Commissione ha chiesto all'ENISA di preparare due sistemi di certificazione, di cui uno per i servizi cloud[103]. Sono attualmente all'esame ulteriori sistemi riguardanti la cibersicurezza di servizi e prodotti destinati ai consumatori. Sebbene tali sistemi di certificazione istituiti a norma del regolamento sulla cibersicurezza non riguardino esplicitamente la protezione dei dati e la tutela della vita privata, contribuiscono ad accrescere la fiducia dei consumatori nei servizi e nei prodotti digitali. Tali sistemi possono comprovare il rispetto dei principi di sicurezza

---

98 Cfr. azioni annunciate nella strategia europea per i dati, pag. 30.

99 A norma dell'articolo 41, paragrafo 3, del regolamento generale sulla protezione dei dati. Cfr. i pareri del comitato europeo per la protezione dei dati all'indirizzo: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_it.

100 https://ec.europa.eu/info/study-data-protection-certification-mechanisms_it.

101 https://edpb.europa.eu/our-work-tools/our-documents/nasoki/guidelines-12018-certification-and-identifying-certification_it.

102 https://edpb.europa.eu/our-work-tools/our-documents/pokyny/guidelines-42018-accreditation-certification-bodies-under_it. Diverse autorità di controllo hanno già presentato i loro requisiti di accreditamento al comitato, tanto per gli organismi di controllo dei codici di condotta quanto per gli organismi di certificazione. Cfr. panoramica al seguente indirizzo: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_it.

103 https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe.

fin dalla progettazione e l'attuazione di misure tecniche e organizzative adeguate in materia di sicurezza del trattamento dei dati personali.

- Clausole contrattuali tipo

La Commissione sta lavorando a clausole contrattuali tipo tra i titolari del trattamento e i responsabili del trattamento[104], anche alla luce della modernizzazione delle clausole contrattuali tipo per i trasferimenti internazionali (cfr. sezione 7.2). Un atto dell'Unione, adottato dalla Commissione, avrà un effetto vincolante a livello UE e garantirà la piena armonizzazione e la certezza del diritto.

6 APPLICAZIONE DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI ALLE NUOVE TECNOLOGIE

Un quadro tecnologicamente neutro, aperto a tecnologie nuove

Il regolamento generale sulla protezione dei dati è neutro sul piano tecnologico, in grado di creare fiducia e basato sui principi[105]. Tali principi, compresi il trattamento lecito e trasparente, la limitazione della finalità e la minimizzazione dei dati, forniscono una base solida per la protezione dei dati personali, indipendentemente dai trattamenti e dalle tecniche applicate.

I membri del gruppo multilaterale segnalano che, nel complesso, il regolamento generale sulla protezione dei dati ha un impatto positivo sullo sviluppo di tecnologie nuove e fornisce una buona base per l'innovazione. È considerato uno strumento essenziale e flessibile per garantire che lo sviluppo di tecnologie nuove in conformità con i diritti fondamentali. L'attuazione dei suoi principi fondamentali è particolarmente importante per il trattamento intensivo di dati. L'approccio basato sul rischio e tecnologicamente neutro del regolamento generale sulla protezione dei dati garantisce un livello di protezione dei dati adeguato per far fronte al rischio del trattamento, anche utilizzando tecnologie emergenti.

Le parti interessate rilevano in particolare che i principi della limitazione della finalità e dell'ulteriore trattamento compatibile, della minimizzazione dei dati, della limitazione della conservazione, della trasparenza, della responsabilizzazione e le condizioni per il ricorso lecito in larga misura a processi decisionali automatizzati[106] rispondono alle preoccupazioni legate all'uso dell'intelligenza artificiale.

L'approccio basato sul rischio e a prova di futuro del regolamento generale sulla protezione dei dati sarà applicato anche nell'eventuale quadro futuro per l'intelligenza artificiale e nell'attuazione della strategia in materia di dati. Quest'ultima strategia mira a promuovere la disponibilità dei dati e la creazione di spazi comuni europei di dati sostenuti da servizi di infrastrutture cloud federati. Per quanto concerne i dati personali, il regolamento generale sulla protezione dei dati fornisce il quadro giuridico

---

[104] Articolo 28, paragrafo 7, del regolamento generale sulla protezione dei dati.

[105] Come ricordato dal Consiglio, dal Parlamento europeo e dal comitato nei loro contributi alla valutazione.

[106] Tuttavia le parti interessate osservano che non tutti i processi decisionali automatizzati in un contesto di intelligenza artificiale rientrano nell'ambito di applicazione dell'articolo 22 del regolamento generale sulla protezione dei dati.

principale entro il quale si possono elaborare soluzioni efficaci caso per caso in funzione della natura e del contenuto di ciascuno degli spazi di dati.

Il regolamento generale sulla protezione dei dati ha accresciuto la consapevolezza in merito alla protezione dei dati personali tanto all'interno quanto all'esterno dell'UE e ha indotto le imprese ad adattare le loro pratiche per tener conto dei principi di protezione dei dati nello svolgimento di attività innovative. Tuttavia le organizzazioni della società civile osservano che, sebbene l'impatto del regolamento generale sulla protezione dei dati sullo sviluppo di tecnologie nuove sembri positivo, le pratiche dei principali attori digitali non sono ancora cambiate radicalmente a favore di un trattamento maggiormente rispettoso della vita privata. 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.

La Commissione sta analizzando le questioni più generali relative ai comportamenti di mercato dei grandi attori digitali nel contesto del pacchetto relativo alla legge sui servizi digitali[107]. Per quanto concerne la ricerca nel settore dei media sociali, la Commissione ricorda che il regolamento generale sulla protezione dei dati non può essere utilizzato come scusa dalle piattaforme dei media sociali per limitare l'accesso da parte di ricercatori e verificatori di fatti a dati non personali, quali statistiche in merito a quali annunci mirati sono stati inviati a quali categorie di persone, i criteri per la definizione di tale attività mirata, informazioni su account falsi, ecc.

L'approccio tecnologicamente neutro e a prova di futuro del regolamento generale sulla protezione dei dati è stato sottoposto a prova durante la pandemia di Covid-19 e si è dimostrato efficace. Le sue norme basate su principi hanno sostenuto lo sviluppo di strumenti per contrastare e monitorare la diffusione del virus.

Sfide da affrontare

Lo sviluppo e l'applicazione di tecnologie nuove non mettono in discussione tali principi. Si prospettano sfide future per chiarire come applicare i principi comprovati all'uso di tecnologie specifiche quali l'intelligenza artificiale, la blockchain, l'Internet delle cose, il riconoscimento facciale o l'informatica quantistica.

In tale contesto il Parlamento europeo e il Consiglio hanno sottolineato la necessità di un monitoraggio continuo per chiarire in che modo il regolamento generale sulla protezione dei dati si applica alle nuove tecnologie e alle imprese tecnologiche di grandi dimensioni. Inoltre le parti interessate avvertono che anche la valutazione della continua adeguatezza del regolamento generale sulla protezione dei dati alle sue finalità richiede un monitoraggio costante.

Le parti interessate dell'industria sottolineano che l'innovazione richiede un'applicazione del regolamento generale sulla protezione dei dati basata su principi, in linea con la sua progettazione, piuttosto che in maniera rigida e formale. Ritengono che orientamenti del comitato in merito all'applicazione dei principi, dei concetti e delle norme del regolamento generale sulla protezione dei dati alle nuove tecnologie, quali l'intelligenza artificiale, la blockchain o l'Internet delle cose, che tengano conto

[107] https://ec.europa.eu/commission/presscorner/detail/it/ip_20_962.

dell'approccio basato sul rischio, contribuirebbero a fornire chiarimenti e una maggiore certezza del diritto. Tali strumenti normativi non vincolanti sono particolarmente idonei ad accompagnare l'applicazione del regolamento generale sulla protezione dei dati alle nuove tecnologie, in quanto garantiscono una maggiore certezza del diritto e possono essere rivisti in linea con gli sviluppi tecnologici. Talune parti interessate suggeriscono inoltre che potrebbe essere utile fornire orientamenti settoriali sulle modalità di applicazione del regolamento generale sulla protezione dei dati alle nuove tecnologie.

Il comitato ha dichiarato che continuerà a considerare l'impatto delle tecnologie emergenti sulla protezione dei dati personali.

Le parti interessate sottolineano inoltre l'importanza del fatto che le autorità di regolamentazione acquisiscano una conoscenza approfondita delle modalità di utilizzo della tecnologia e avviino un dialogo con il settore industriale sullo sviluppo delle tecnologie emergenti. Ritengono che un approccio che prevede "contesti di sperimentazione normativa", come mezzo per ottenere orientamenti sull'applicazione delle norme, potrebbe essere un'opzione interessante per testare le nuove tecnologie e aiutare le imprese ad applicare la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita nelle nuove tecnologie.

In termini di ulteriori azioni politiche, le parti interessate raccomandano che le future proposte politiche in materia di intelligenza artificiale si basino sui quadri giuridici esistenti e siano allineate con il regolamento generale sulla protezione dei dati. Occorre valutare con attenzione le potenziali questioni specifiche, sulla base di prove pertinenti, prima di proporre norme prescrittive nuove.

Il Libro bianco della Commissione sull'intelligenza artificiale presenta una serie di opzioni strategiche in merito alle quali sono stati richiesti i pareri delle parti interessate fino al 14 giugno 2020. Per quanto concerne il riconoscimento facciale, una tecnologia che può avere un impatto significativo sui diritti delle persone fisiche, il Libro bianco ha ricordato l'attuale quadro legislativo e ha aperto un dibattito pubblico sulle circostanze specifiche, se presenti, che potrebbero giustificare l'uso dell'intelligenza artificiale per finalità di riconoscimento facciale e per altre finalità di identificazione biometrica a distanza in luoghi pubblici, nonché sulle garanzie comuni.

7 TRASFERIMENTI INTERNAZIONALI E COOPERAZIONE GLOBALE

7.1 Tutela dei dati personali: una questione avente natura globale

La richiesta di protezione dei dati personali non conosce frontiere, dato che le persone fisiche in tutto il mondo tengono in gran conto e apprezzano sempre di più la tutela della vita privata e la sicurezza dei loro dati.

Nel contempo, l'importanza dei flussi di dati per le persone fisiche, i governi, le imprese e, più in generale, la società nel suo complesso, è inevitabile nel nostro mondo interconnesso. Tali flussi di dati costituiscono parte integrante del commercio, della cooperazione tra autorità pubbliche e delle interazioni sociali. A tale riguardo, l'attuale pandemia di Covid-19 evidenzia altresì la criticità del trasferimento e dello scambio di dati personali per numerose attività essenziali, tra le quali la garanzia della continuità delle operazioni governative e aziendali, consentendo il telelavoro e altre

soluzioni che si basano ampiamente sulle tecnologie dell'informazione e della comunicazione, sviluppando la cooperazione nella ricerca scientifica in materia di diagnostica, cure e vaccini nonché contrastando forme nuove di criminalità informatica, come ad esempio i sistemi di frode online che offrono medicinali contraffatti che si sostiene prevengano o curino la Covid-19.

In questo contesto, più che mai prima d'ora, tutelare la vita privata e facilitare i flussi di dati sono attività che devono procedere di pari passo. L'UE, con il suo sistema di protezione dei dati, che combina l'apertura ai trasferimenti internazionali a un elevato livello di protezione delle persone fisiche, si trova nella posizione ideale per promuovere flussi di dati sicuri e affidabili. Il regolamento generale sulla protezione dei dati si è già rivelato un punto di riferimento 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.

Si tratta di una tendenza realmente universale che, per menzionare soltanto alcuni esempi, va dal Cile alla Corea del Sud, dal Brasile al Giappone, dal Kenya all'India, dalla Tunisia all'Indonesia e dalla California a Taiwan. Tali sviluppi sono notevoli non soltanto da un punto di vista quantitativo, ma anche qualitativo: numerose delle leggi in materia di tutela della vita privata recentemente adottate o in fase di adozione si basano su un nucleo centrale di garanzie, diritti e meccanismi di attuazione comuni condivisi dall'UE. In un mondo troppo spesso caratterizzato da approcci normativi diversi, se non persino divergenti, tale tendenza alla convergenza globale costituisce uno sviluppo molto positivo che crea nuove opportunità per una maggiore protezione delle persone fisiche in Europa, facilitando nel contempo i flussi di dati e riducendo i costi di transazione per gli operatori economici.

Per cogliere tali opportunità e attuare la strategia illustrata nella sua comunicazione del 2017 dal titolo "Scambio e protezione dei dati personali in un mondo globalizzato"[108], la Commissione ha notevolmente intensificato i propri lavori sulla dimensione internazionale della tutela della vita privata sfruttando appieno gli strumenti di trasferimento disponibili, come spiegato in appresso. Ciò ha incluso la collaborazione attiva con partner importanti al fine di pervenire a un "accertamento di adeguatezza" e ha portato a risultati importanti, quali la creazione del più grande spazio al mondo di libera e sicura circolazione di dati tra l'UE e il Giappone.

Oltre alle proprie attività sull'adeguatezza, la Commissione ha lavorato in stretta collaborazione con le autorità di protezione dei dati in seno al comitato, nonché con altre parti interessate, per sfruttare appieno il potenziale offerto dalle norme flessibili del regolamento generale sulla protezione dei dati in materia di trasferimenti internazionali. Ciò riguarda la modernizzazione di strumenti quali le clausole contrattuali tipo, lo sviluppo di sistemi di certificazione, codici di condotta o accordi amministrativi per lo scambio di dati tra autorità pubbliche, nonché il chiarimento di concetti chiave relativi ad esempio all'ambito di applicazione territoriale delle norme dell'UE in materia di protezione dei dati o al ricorso alle cosiddette "deroghe" per il trasferimento di dati personali.

[108] Comunicazione della Commissione al Parlamento europeo e al Consiglio, Scambio e protezione dei dati personali in un mondo globalizzato [COM(2017) 7 final], 10.1.2017.

Infine 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 ha potuto 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 coerenza e una maggiore complementarità tra i diversi aspetti della dimensione esterna delle politiche dell'UE, dal commercio al nuovo partenariato Africa-UE.

7.2 Gli strumenti del regolamento generale sulla protezione dei dati relativi ai trasferimenti

Dato che sempre più operatori privati e pubblici si affidano a flussi internazionali di dati nel contesto delle loro operazioni abituali, vi è una crescente necessità di strumenti flessibili che possano essere adattati a settori modelli imprenditoriali e situazioni di trasferimento diversi. Rispecchiando tali esigenze, il regolamento generale sulla protezione dei dati mette a disposizione una serie di strumenti modernizzati che facilita 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. Tale continuità di protezione è importante, dato che nel contesto attuale i dati si muovono facilmente a livello transfrontaliero e che le tutele garantite dal regolamento generale sulla protezione dei dati sarebbero incomplete se fossero limitate al trattamento all'interno dell'UE.

Con il capo V del regolamento generale sulla protezione dei dati, il legislatore ha confermato l'architettura delle norme sui trasferimenti già esistente ai sensi della direttiva 95/46: i trasferimenti di dati possono avvenire qualora la Commissione abbia effettuato un accertamento di adeguatezza nei confronti di un paese terzo o di un'organizzazione internazionale oppure, in assenza di tale accertamento, qualora il titolare del trattamento o il responsabile del trattamento nell'UE ("esportatore di dati") abbia fornito garanzie adeguate, ad esempio mediante la stipula di un contratto con il destinatario ("importatore di dati"). Inoltre rimangono disponibili i presupposti di legge per i trasferimenti (le cosiddette deroghe) per situazioni specifiche per le quali il legislatore ha deciso che l'equilibrio degli interessi consente il trasferimento di dati a determinate condizioni. Nel contempo la riforma ha chiarito e semplificato le norme esistenti ad esempio stabilendo nel dettaglio le condizioni per un accertamento di adeguatezza o norme vincolanti d'impresa, limitando i requisiti di autorizzazione a pochissimi casi specifici e abolendo completamente gli obblighi di notifica. Sono stati inoltre introdotti nuovi strumenti di trasferimento, ad esempio codici di condotta o sistemi di certificazione, e sono state ampliate le possibilità di utilizzare gli strumenti esistenti (ad esempio clausole contrattuali tipo).

L'economia digitale odierna consente agli operatori stranieri di partecipare (a distanza ma) direttamente al mercato interno dell'UE e di competere per acquisire clienti europei e i loro dati personali. Quando si rivolgono specificamente ai cittadini europei mediante l'offerta di beni o servizi o il monitoraggio del loro comportamento, tali operatori stranieri sono tenuti a rispettare il diritto dell'UE allo stesso modo degli operatori dell'UE. Tale aspetto si riflette nell'articolo 3 del regolamento generale sulla protezione dei dati, che estende l'applicabilità diretta delle norme dell'UE in materia di

protezione dei dati a taluni trattamenti condotti da titolari e responsabili del trattamento al di fuori dell'UE. Ciò assicura le garanzie necessarie nonché parità di condizioni per tutte le imprese che operano sul mercato dell'UE.

La sua ampia portata è una delle ragioni per le quali gli effetti del regolamento generale sulla protezione dei dati sono stati avvertiti anche in altre parti del mondo. Gli orientamenti dettagliati emanati dal comitato sull'ambito di applicazione territoriale del regolamento generale sulla protezione dei dati, a seguito di una consultazione pubblica di ampio respiro, sono quindi importanti per aiutare gli operatori stranieri a stabilire se e quali trattamenti siano direttamente soggetti alle garanzie previste in tale atto legislativo, anche fornendo esempi concreti[109].

L'estensione dell'ambito di applicazione del diritto dell'UE in materia di protezione dei dati non è tuttavia di per sé sufficiente a garantirne il rispetto nella pratica. Come sottolineato anche dal Consiglio[110], è fondamentale garantire il rispetto delle norme da parte degli operatori stranieri così come un'applicazione rigorosa delle norme nei loro confronti. La nomina di un rappresentante nell'UE (articolo 27, paragrafi 1 e 2, del regolamento generale sulla protezione dei dati), al quale le persone fisiche e le autorità di controllo possono rivolgersi in aggiunta a o in sostituzione dell'impresa responsabile che agisce dall'estero[111], dovrebbe svolgere un ruolo chiave in tal senso. Tale approccio, adottato sempre più spesso anche in altri contesti[112], 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. Qualora tali operatori non rispettino l'obbligo di nominare un rappresentante[113], le autorità di controllo dovrebbero ricorrere a tutti gli strumenti di applicazione della legge di cui all'articolo 58 del regolamento generale sulla protezione dei dati (ad esempio, avvisi pubblici, divieti temporanei o definitivi di trattamento nell'UE, applicazione della legge nei confronti di contitolari del trattamento stabiliti nell'UE).

Infine è molto importante che il comitato finalizzi il proprio lavoro chiarendo ulteriormente la relazione tra l'articolo 3 sull'applicazione diretta del regolamento

---

[109] Comitato europeo per la protezione dei dati, Linee guida 3/2018 sull'ambito di applicazione territoriale del RGPD, 12.11.2019. Le linee guida affrontano diverse delle questioni sollevate durante la consultazione pubblica, ad esempio l'interpretazione dei criteri in materia di trattamenti mirati e di controllo.

[110] Cfr. posizione e conclusioni del Consiglio, punti 34, 35 e 38.

[111] Cfr. articolo 27, paragrafo 4 e considerando 80 del regolamento generale sulla protezione dei dati ("Il rappresentante designato dovrebbe essere oggetto di misure attuative in caso di inadempienza da parte del titolare del trattamento o del responsabile del trattamento").

[112] Proposta di direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali [COM(2018) 226 final], articolo 3; proposta di regolamento del Parlamento europeo e del Consiglio relativo alla prevenzione della diffusione di contenuti terroristici online, [COM(2018) 640 final], articolo 16, paragrafi 2 e 3.

[113] Secondo le osservazioni presentate da un soggetto in risposta alla consultazione pubblica, uno dei punti principali da affrontare "è un'applicazione efficace e conseguenze effettive per coloro che hanno scelto di ignorare [...] tale prescrizione [...]. Occorre tenere presente in particolare che ciò pone le imprese stabilite nell'Unione in una situazione di svantaggio concorrenziale nei confronti delle imprese non conformi stabilite al di fuori dell'Unione che operano nell'Unione". Cfr. EU Business Partners, osservazioni presentate il 29 aprile 2020.

generale sulla protezione dei dati e le norme in materia di trasferimenti internazionali di cui al capo V[114].

Decisioni di adeguatezza

I contributi ricevuti dalle parti interessate confermano che le decisioni di adeguatezza continuano a costituire uno strumento essenziale per consentire agli operatori dell'UE di trasferire in maniera sicura i dati personali verso paesi terzi[115]. Tali decisioni mettono a disposizione la soluzione più completa, semplice ed efficace sotto il profilo dei costi per i trasferimenti di dati in quanto tali attività sono assimilate alle trasmissioni all'interno dell'UE, garantendo così la libera circolazione dei dati personali senza ulteriori condizioni o la necessità di un'autorizzazione. Di conseguenza le decisioni di adeguatezza aprono canali commerciali per gli operatori dell'UE e facilitano la cooperazione tra le autorità pubbliche, offrendo nel contempo un accesso privilegiato al mercato unico dell'UE. Basandosi sulla prassi a norma della direttiva del 1995, il regolamento generale sulla protezione dei dati prevede esplicitamente la possibilità di una decisione sull'adeguatezza con riferimento a un particolare territorio di un paese terzo o a un settore specifico all'interno di un paese terzo (la cosiddetta adeguatezza "parziale").

Il regolamento generale sulla protezione dei dati si basa sull'esperienza degli ultimi anni e sui chiarimenti forniti dalla Corte di giustizia che ha definito un catalogo dettagliato di elementi che la Commissione deve considerare nella sua valutazione. Il criterio dell'adeguatezza richiede un livello di protezione comparabile (o "sostanzialmente equivalente") a quello garantito all'interno dell'UE[116]. Ciò comporta una valutazione globale del sistema del paese terzo nel suo complesso, tra cui la sostanza delle tutele della vita privata, la loro effettiva attuazione e applicazione, nonché le norme in materia di accesso ai dati personali da parte delle autorità pubbliche, in particolare per finalità di contrasto e sicurezza nazionale[117].

Ciò si riflette anche negli orientamenti adottati dall'ex gruppo di lavoro Articolo 29 (e omologati dal comitato), in particolare i cosiddetti "criteri di riferimento per l'adeguatezza", il che chiarisce ulteriormente gli elementi di cui la Commissione deve tenere conto nell'effettuare una valutazione dell'adeguatezza, anche fornendo una panoramica delle "garanzie sostanziali" per l'accesso ai dati personali da parte delle

---

[114] Diverse osservazioni presentate in occasione della consultazione pubblica hanno sollevato questo aspetto ad esempio per quanto riguarda la trasmissione di dati personali a destinatari al di fuori dell'UE, ma soggetti al regolamento generale sulla protezione dei dati.

[115] Posizione e conclusioni del Consiglio, punto 17; contributo del comitato, pagg. 5-6. Diverse osservazioni presentate in risposta alla consultazione pubblica, tra le quali quelle di una serie di associazioni di categoria [quali l'associazione francese delle grandi imprese, Digital Europe, Global Data Alliance/BSA, Computer & Communication Industry Association (CCIA) o la Camera di commercio degli USA] hanno chiesto di intensificare i lavori in merito agli accertamenti di adeguatezza, in particolare con importanti partner commerciali.

[116] Sentenza della Corte di giustizia dell'Unione europea del 6 ottobre 2015, *Maximillian Schrems/Data Protection Commissioner* ("*Schrems*"), C-362/14, ECLI:EU:C:2015:650, punti 73, 74 e 96. Cfr. anche il considerando 104 del regolamento generale sulla protezione dei dati, che fa riferimento al livello di protezione sostanzialmente equivalente.

[117] Cfr. articolo 45, paragrafo 2 e considerando 104 del regolamento generale sulla protezione dei dati. Cfr. anche *Schrems*, punti 75 e 91.

autorità pubbliche[118]. Quest'ultimo aspetto si basa in particolare sulla giurisprudenza della Corte europea dei diritti dell'uomo. Sebbene non implichi una replica da punto a punto ("fotocopia") della normativa dell'UE, dal momento che i mezzi per garantire un livello di protezione comparabile possono variare tra i diversi sistemi di tutela della vita privata, spesso rispecchiando le diverse tradizioni giuridiche, il criterio della "protezione sostanzialmente equivalente" richiede tuttavia un livello di protezione elevato.

Tale criterio è giustificato dal fatto che una decisione di adeguatezza estende sostanzialmente a un paese terzo i vantaggi del mercato unico in termini di libera circolazione dei dati. Ciò significa tuttavia anche che talvolta vi saranno differenze significative tra il livello di protezione garantito nel paese terzo in questione rispetto al regolamento generale sulla protezione dei dati, che occorre vengano appianate ad esempio attraverso la negoziazione di garanzie aggiuntive. Tali garanzie dovrebbero essere considerate positivamente, in quanto rafforzano ulteriormente le tutele a disposizione delle persone fisiche nell'UE. Al tempo stesso la Commissione concorda con il comitato in merito all'importanza di monitorare costantemente la loro applicazione nella pratica, compresa la loro applicazione efficace da parte dell'autorità di protezione dei dati del paese terzo[119].

Il regolamento generale sulla protezione dei dati chiarisce che le decisioni di adeguatezza sono "strumenti viventi" che dovrebbero essere oggetto di un monitoraggio continuo e di un riesame periodico[120]. In linea con queste prescrizioni, la Commissione ha scambi regolari con le autorità competenti al fine di dare un seguito proattivo a nuovi sviluppi. Ad esempio, dall'adozione della decisione sullo scudo UE-USA per la privacy nel 2016[121], la Commissione, insieme a rappresentanti del comitato, ha effettuato tre riesami annuali per valutare tutti gli aspetti del funzionamento del quadro[122]. Tali riesami si sono basati su informazioni ottenute

---

[118] Criteri di riferimento per l'adeguatezza, WP 254 rev. 01, 6 febbraio 2018 (disponibile all'indirizzo: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

[119] Contributo del comitato, pagg. 5-6.

[120] L'articolo 45, paragrafi 4 e 5, del regolamento generale sulla protezione dei dati impone alla Commissione di monitorare costantemente gli sviluppi in paesi terzi e di riesaminare periodicamente, almeno ogni quattro anni, l'accertamento di adeguatezza. Tali disposizioni conferiscono inoltre alla Commissione il potere di abrogare, modificare o sospendere una decisione di adeguatezza qualora essa constati che il paese o l'organizzazione internazionale in questione non garantisce più un livello di protezione adeguato. L'articolo 97, paragrafo 2, lettera a), del regolamento generale sulla protezione dei dati impone inoltre alla Commissione di trasmettere una relazione di valutazione al Parlamento europeo e al Consiglio entro il 2020. Cfr. anche la sentenza della Corte di giustizia dell'Unione europea del 6 ottobre 2015, *Maximillian Schrems/Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650, punto 76.

[121] Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy. Questa decisione di adeguatezza è un caso specifico che, in assenza di una legislazione generale in materia di protezione dei dati negli Stati Uniti, si basa su impegni assunti dalle imprese partecipanti (che sono esecutivi ai sensi del diritto statunitense) di applicare le norme in materia di protezione dei dati stabilite in tale accordo. Inoltre, lo scudo per la privacy si fonda sulle specifiche osservazioni e garanzie espresse dal governo degli Stati Uniti per quanto riguarda l'accesso a fini di sicurezza nazionale, che sono alla base dell'accertamento di adeguatezza.

[122] I riesami hanno avuto luogo nel 2017 [relazione della Commissione al Parlamento europeo e al Consiglio sul primo riesame annuale del funzionamento dello scudo UE-USA per la privacy, COM(2017) 611 final], nel 2018 [relazione della Commissione al Parlamento europeo e al

tramite scambi con le autorità statunitensi nonché sul contributo di altre parti interessate, quali le autorità di protezione dei dati, la società civile e associazioni di categoria dell'UE. Tali riesami hanno consentito di migliorare il funzionamento pratico di vari elementi del quadro. In una prospettiva di più ampio respiro, i riesami annuali hanno contribuito a stabilire un dialogo più ampio con l'amministrazione statunitense in materia di tutela della vita privata in generale, nonché di limitazioni e garanzie relative in particolare alla sicurezza nazionale.

Nel quadro della sua prima valutazione del regolamento generale sulla protezione dei dati, la Commissione è altresì tenuta a riesaminare le decisioni di adeguatezza adottate in conformità con la direttiva del 1995[123]. I servizi della Commissione hanno avviato un dialogo intenso con ciascuno degli 11 territori e paesi interessati al fine di valutare in che modo i loro sistemi di protezione dei dati personali 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. Si tratta certamente di sviluppi positivi. 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 11 decisioni di adeguatezza menzionate in seguito alla pronuncia della sentenza della Corte di giustizia in tale causa[124].

Consiglio sul secondo riesame annuale del funzionamento dello scudo UE-USA per la privacy, COM(2018) 860 final] e nel 2019 [relazione della Commissione al Parlamento europeo e al Consiglio sul terzo riesame annuale del funzionamento dello scudo UE-USA per la privacy, COM(2019) 495 final].

[123] Tali decisioni di adeguatezza esistenti riguardano paesi che sono strettamente integrati con l'Unione europea e i suoi Stati membri (Svizzera, Andorra, Isole Fær Øer, Guernsey, Jersey, Isola di Man), importanti partner commerciali (ad esempio Argentina, Canada, Israele, Stati Uniti) e paesi che hanno un ruolo di pioniere nell'elaborazione di leggi sulla protezione dei dati nella loro regione (Nuova Zelanda, Uruguay).

[124] 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. L'udienza relativa a tale causa ha avuto luogo il 9 luglio 2019 e la sentenza è stata annunciata per il 16 luglio 2020.

Attuando la strategia definita nella comunicazione del 2017 intitolata "Scambio e protezione dei dati personali in un mondo globalizzato", la Commissione ha altresì avviato nuovi dialoghi in materia di adeguatezza[125]. Tale lavoro ha già prodotto risultati significativi che hanno coinvolto partner importanti dell'UE. Nel gennaio del 2019 la Commissione ha adottato una decisione di adeguatezza per il Giappone, basata su un elevato grado di convergenza, anche attraverso garanzie specifiche, ad esempio nel settore dei trasferimenti successivi e attraverso la creazione di un meccanismo per indagare e risolvere i reclami di persone fisiche riguardanti l'accesso delle amministrazioni pubbliche ai dati personali per finalità di contrasto e di sicurezza nazionale.

Trattandosi del primo accertamento di adeguatezza adottato a norma del regolamento generale sulla protezione dei dati, il quadro concordato con il Giappone costituisce un precedente utile per decisioni future[126]. Ciò include il fatto che è stato ricambiato sul lato giapponese con un accertamento di "adeguatezza" nei confronti dell'UE. Congiuntamente, questi accertamenti di adeguatezza reciproci creano il più ampio spazio al mondo di libera e sicura circolazione di dati personali, integrando in tal modo l'accordo di partenariato economico UE-Giappone. Di fatto tale accordo sostiene annualmente circa 124 miliardi di EUR di scambi di merci e 42,5 miliardi di EUR di scambi di servizi.

Il processo relativo all'adeguatezza è in fase avanzata anche con la Corea del Sud. Un risultato importante è costituito dalla recente riforma legislativa della Corea del Sud, che ha portato all'istituzione di un'autorità indipendente di protezione dei dati dotata di forti poteri di applicazione. Ciò dimostra come un dialogo in materia di adeguatezza possa contribuire a una maggiore convergenza tra le norme dell'UE in materia di protezione dei dati e quelle di un paese straniero.

La Commissione concorda pienamente con l'invito delle parti interessate a intensificare il dialogo con i paesi terzi selezionati in vista di eventuali nuovi accertamenti di adeguatezza[127]. Sta valutando attivamente questa possibilità con altri importanti partner asiatici, dell'America latina e del vicinato, sfruttando l'attuale tendenza alla convergenza verso l'alto a livello globale delle norme in materia di protezione dei dati. Una normativa esaustiva in materia di tutela della vita privata è stata adottata o è nella fase avanzata del processo legislativo in America latina (Brasile, Cile) e si stanno delineando sviluppi promettenti in Asia (ad esempio India,

[125] Cfr. supra nota 109. La Commissione ha spiegato che, nel valutare con quali paesi terzi dovrebbe essere avviato un dialogo sull'adeguatezza, terrà conto dei seguenti criteri: i) la portata delle relazioni commerciali (esistenti o potenziali) dell'UE con il paese terzo, in particolare l'esistenza di un accordo di libero scambio o di negoziati in corso; ii) la portata dei flussi di dati personali provenienti dall'UE, indice di legami culturali e/o geografici; iii) il ruolo di pioniere del paese nel settore della protezione della vita privata e dei dati del paese terzo, che potrebbe fungere da modello per gli altri paesi della regione; e iv) le relazioni politiche generali con il paese, in particolare per quanto riguarda la promozione di valori comuni e obiettivi condivisi a livello internazionale.

[126] Risoluzione del Parlamento europeo, del 13 dicembre 2018, sull'adeguatezza della protezione dei dati personali offerta dal Giappone [2018/2979(RSP)], punto 27; contributo del comitato, pagg. 5-6.

[127] Cfr. ad esempio Risoluzione del Parlamento europeo del 12 dicembre 2017 su "Verso una strategia per il commercio digitale" (2017/2065(INI)), punti 8 e 9; posizione e conclusioni del Consiglio in merito all'applicazione del regolamento generale sulla protezione dei dati (14994/1/19), 19.12.2019, punto 17; contributo del comitato, pag. 5.

Indonesia, Malaysia, Sri Lanka, Taiwan e Thailandia), in Africa (ad esempio Etiopia, Kenya) nonché nel vicinato europeo orientale e meridionale (ad esempio Georgia, Tunisia). Ove possibile la Commissione si adopererà per adottare decisioni di adeguatezza esaustive riguardanti tanto il settore privato quanto quello pubblico[128].

Il regolamento generale sulla protezione dei dati ha inoltre introdotto la possibilità per la Commissione di adottare accertamenti di adeguatezza nei confronti di organizzazioni internazionali. Questa via potrebbe essere esaminata per la prima volta in un momento in cui talune organizzazioni internazionali stanno modernizzando i propri sistemi di protezione dei dati mettendo in atto norme generali, nonché meccanismi che garantiscono una vigilanza e un ricorso indipendenti.

Anche l'adeguatezza svolge un ruolo importante nel contesto delle relazioni con il Regno Unito in seguito alla Brexit, 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[129]. Data l'importanza dei flussi di dati con il Regno Unito e la sua prossimità al mercato dell'UE, un elevato grado di convergenza tra le norme in materia di protezione dei dati su entrambi i versanti del canale costituisce inoltre un aspetto importante per garantire parità di condizioni. 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[130]. In considerazione del carattere autonomo e unilaterale di una valutazione dell'adeguatezza, tali negoziati seguono una linea distinta da quelli concernenti un accordo sulle future relazioni tra l'UE e il Regno Unito.

Infine la Commissione accoglie con favore il fatto che altri paesi stanno mettendo in atto meccanismi di trasferimento dei dati analoghi a quelli di un accertamento di adeguatezza. Procedendo in tal senso tali paesi riconoscono spesso che l'UE e i paesi per i quali la Commissione ha adottato una decisione di adeguatezza costituiscono una destinazione sicura per i trasferimenti[131]. Il numero crescente di paesi che beneficiano di decisioni di adeguatezza dell'UE, da un lato, e di questa forma di riconoscimento da parte di altri paesi, dall'altro, può potenzialmente creare una rete di paesi nella quale i dati possono circolare liberamente e in maniera sicura. La Commissione ritiene che ciò costituisca uno sviluppo positivo che accrescerà ulteriormente i vantaggi di una

[128] Come richiesto anche dal Consiglio, cfr. posizione e conclusioni del Consiglio in merito all'applicazione del regolamento generale sulla protezione dei dati (14994/1/19), 19.12.2019, punti 17 e 40. Ciò richiede tuttavia che siano soddisfatte le condizioni per un accertamento di adeguatezza relativo ai trasferimenti di dati verso le autorità pubbliche, anche per quanto riguarda la vigilanza indipendente.

[129] Cfr. le direttive di negoziato allegate alla decisione del Consiglio che autorizza l'avvio di negoziati con il Regno Unito di Gran Bretagna e Irlanda del Nord per un nuovo accordo di partenariato (ST 5870/20 ADD 1 REV 3), punti 13 e 118.

[130] Cfr. testo riveduto della dichiarazione politica che definisce il quadro per le future relazioni tra l'Unione europea e il Regno Unito come concordato a livello di negoziatori il 17 ottobre 2019, punti da 8 a 10 (disponibile all'indirizzo https://ec.europa.eu/commission/sites/beta-political/files/revised_political_declaration.pdf).

[131] Ad esempio nel caso di Argentina, Colombia, Israele, Svizzera od Uruguay.

decisione di adeguatezza nei confronti di paesi terzi e contribuirà alla convergenza globale. Questo tipo di sinergie può altresì contribuire in maniera utile allo sviluppo di quadri per la circolazione libera e sicura di dati, come ad esempio nel contesto dell'iniziativa "Data Free Flow with Trust" (cfr. in appresso).

Garanzie adeguate

Il regolamento generale sulla protezione dei dati prevede una serie di altri strumenti di trasferimento al di là della soluzione globale di un accertamento di adeguatezza. La flessibilità di tale serie di strumenti è dimostrata dall'articolo 46 del regolamento generale sulla protezione dei dati, che disciplina i trasferimenti di dati basati su "garanzie adeguate", compresi diritti azionabili e mezzi di ricorso effettivi degli interessati. Al fine di assicurare garanzie adeguate, sono disponibili diversi strumenti destinati a rispondere alle esigenze di trasferimento tanto degli operatori commerciali quanto degli enti pubblici.

- Clausole contrattuali tipo

Il primo gruppo di tali strumenti riguarda strumenti contrattuali che possono essere clausole di protezione dei dati ad hoc, personalizzate, concordate tra un esportatore di dati dell'UE e un importatore di dati al di fuori dell'UE, autorizzate dall'autorità competente in materia di protezione dei dati [articolo 46, paragrafo 3, lettera a), del regolamento generale sulla protezione dei dati] oppure clausole tipo precedentemente approvate dalla Commissione [articolo 46, paragrafo 2, lettere c) e d), del regolamento generale sulla protezione dei dati[132]]. I più importanti di questi strumenti sono le cosiddette clausole contrattuali tipo, ossia clausole tipo in materia di protezione dei dati che l'esportatore di dati e l'importatore di dati possono integrare nei loro accordi contrattuali (ad esempio un contratto di servizi che richiede il trasferimento di dati personali) su base volontaria e che stabiliscono le prescrizioni in materia di garanzie adeguate.

Le clausole contrattuali tipo rappresentano il meccanismo di trasferimento dei dati di gran lunga più diffuso[133]. Migliaia di imprese dell'UE si affidano a clausole contrattuali tipo per fornire un'ampia gamma di servizi ai loro clienti, fornitori, partner e dipendenti, compresi i servizi essenziali per il funzionamento dell'economia. Il loro ampio uso indica che sono molto utili per le imprese nei loro sforzi di conformità e, in particolare, vanno a vantaggio delle imprese che non dispongono delle risorse per negoziare contratti individuali con ciascuno dei rispettivi partner commerciali. Attraverso la standardizzazione e l'approvazione preventiva, le clausole contrattuali tipo forniscono alle imprese uno strumento di facile attuazione per

[132] Le clausole contrattuali tipo per i trasferimenti internazionali richiedono sempre l'approvazione della Commissione, ma possono essere elaborate dalla Commissione stessa o da un'autorità nazionale di protezione dei dati. Tutte le clausole contrattuali tipo rientrano nella prima categoria.

[133] Secondo la relazione annuale del 2019 sulla governance in materia di vita privata dell'IAPP-EY, "lo strumento più popolare tra questi strumenti [di trasferimento], anno su anno, è in larga misura quello delle clausole contrattuali tipo: l'88 % degli intervistati nell'indagine di quest'anno ha dichiarato che le clausole contrattuali tipo rappresentano il metodo più adatto per i trasferimenti di dati extraterritoriali, seguito dal rispetto del regime dello scudo UE-USA per la privacy (60 %). Per quanto concerne gli intervistati che trasferiscono dati dall'UE al Regno Unito (52 %), il 91 % di loro segnala di intendere utilizzare le clausole contrattuali tipo per la conformità nel trasferimento di dati dopo la Brexit".

soddisfare le prescrizioni in materia di protezione dei dati in un contesto di trasferimento.

Le serie esistenti di clausole contrattuali tipo[134] sono state adottate ed approvate sulla base della direttiva del 1995. Tali clausole contrattuali tipo restano in vigore fino a quando non vengono modificate, sostituite o abrogate, se necessario, da una decisione della Commissione (articolo 46, paragrafo 5, del regolamento generale sulla protezione dei dati). Il regolamento generale sulla protezione dei dati amplia le possibilità di ricorrere a clausole contrattuali tipo tanto all'interno dell'UE quanto per i trasferimenti internazionali. La Commissione sta collaborando con le parti interessate per avvalersi di tali possibilità e aggiornare le clausole esistenti[135]. Al fine di garantire che la progettazione futura delle clausole contrattuali tipo sia adeguata alla finalità, la Commissione ha raccolto riscontri sulle esperienze delle parti interessate rispetto a tale strumento, attraverso il "gruppo multilaterale sul regolamento generale sulla protezione dei dati" e un seminario specifico tenutosi nel settembre 2019, ma anche attraverso contatti multipli con imprese che utilizzano le clausole contrattuali tipo e organizzazioni della società civile. Il comitato sta inoltre aggiornando una serie di orientamenti che potrebbero essere pertinenti per il riesame delle clausole contrattuali tipo, ad esempio in merito ai concetti di titolare e di responsabile del trattamento.

[134] Attualmente esistono tre serie di clausole contrattuali tipo adottate dalla Commissione per il trasferimento di dati personali verso paesi terzi: due per i trasferimenti da un titolare del trattamento del SEE a un titolare del trattamento non appartenente al SEE e uno per i trasferimenti da un titolare del trattamento del SEE a un responsabile del trattamento non appartenente al SEE. Tali serie di clausole sono state modificate nel 2016, in seguito alla sentenza della Corte di giustizia nella causa *Schrems I* (C-362/14), per eliminare eventuali limitazioni concernenti le autorità di controllo aventi competenza per esercitare i loro poteri di controllo sui trasferimenti di dati. Cfr. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_it.

[135] Cfr. anche il contributo del comitato, pagg. 6-7. Analogamente il Consiglio ha invitato la Commissione "a riesaminare e rivedere nel prossimo futuro [le clausole contrattuali tipo] al fine di tenere conto delle esigenze dei titolari e dei responsabili del trattamento". Cfr. posizione e conclusioni del Consiglio.

Sulla base del riscontro ricevuto, i servizi della Commissione stanno attualmente lavorando alla revisione delle clausole contrattuali tipo. In tale contesto sono stati individuati alcuni settori da migliorare, in particolare per quanto riguarda i seguenti aspetti:

1. aggiornamento delle clausole contrattuali tipo alla luce delle nuove prescrizioni introdotte dal regolamento generale sulla protezione dei dati, come quelle relative al rapporto tra titolare e responsabile del trattamento ai sensi dell'articolo 28 del regolamento generale sulla protezione dei dati (in particolare in merito agli obblighi del responsabile del trattamento), agli obblighi di trasparenza dell'importatore di dati (in termini di informazioni necessarie da fornire all'interessato), ecc.;
2. trattazione di una serie di scenari di trasferimento non trattati dalle clausole contrattuali tipo correnti, quali il trasferimento di dati da un responsabile del trattamento dell'UE a un (sub)responsabile del trattamento di un paese terzo, ma anche ad esempio situazioni nelle quali il titolare del trattamento è situato al di fuori dell'UE[136];
3. rispecchiare meglio le realtà dei trattamenti nell'economia digitale moderna nella quale tali operazioni coinvolgono spesso più importatori ed esportatori di dati, catene di trattamento lunghe e spesso complesse, relazioni commerciali in evoluzione, ecc. Al fine di tener conto di tali situazioni, tra le soluzioni esaminate si annoverano ad esempio la possibilità di consentire la firma di clausole contrattuali tipo da parte di più parti o l'adesione di nuove parti durante l'intero termine del contratto.

Nell'affrontare questi punti, la Commissione sta altresì vagliando le modalità per rendere l'attuale "architettura" delle clausole contrattuali tipo più facile da utilizzare, sostituendo ad esempio serie multiple di clausole contrattuali tipo con un unico documento esaustivo. La sfida consiste nel trovare un buon equilibrio tra la necessità di chiarezza e un certo grado di standardizzazione, da un lato, e la necessaria flessibilità che consentirà l'utilizzo delle clausole da parte di numerosi operatori con esigenze diverse, in contesti diversi e per tipi di trasferimenti diversi, dall'altro.

Un altro aspetto importante da considerare è l'eventuale necessità, alla luce dell'attuale contenzioso dinanzi la Corte di giustizia[137], di chiarire ulteriormente le garanzie per quanto concerne l'accesso da parte di autorità pubbliche straniere ai dati trasferiti in base a clausole contrattuali tipo, in particolare per finalità di sicurezza nazionale. Ciò può includere l'obbligo per l'importatore o l'esportatore di dati, oppure per entrambi, di intervenire e di chiarire il ruolo delle autorità di protezione dei dati in tale contesto. Sebbene la revisione delle clausole contrattuali tipo si trovi in fase avanzata, sarà

[136] Diverse osservazioni presentate in risposta alla consultazione pubblica hanno commentato quest'ultimo scenario, sollevando spesso preoccupazioni in merito al fatto che obbligare i responsabili del trattamento dell'UE ad assicurare garanzie adeguate nelle loro relazioni con titolari del trattamento di paesi terzi porrebbe tali responsabili in una condizione di svantaggio competitivo rispetto ai responsabili del trattamento stranieri che offrono servizi analoghi.

[137] Cfr. causa *Schrems II*.

necessario attendere la sentenza della Corte in maniera da riflettere qualsiasi eventuale prescrizione aggiuntiva nelle clausole rivedute, prima che un progetto di decisione su una nuova serie di clausole contrattuali tipo possa essere sottoposto al parere del comitato e successivamente proposto per l'adozione mediante "l'iter di comitologia"[138].

Parallelamente la Commissione è altresì in contatto con partner internazionali che stanno sviluppando strumenti analoghi[139]. Tale dialogo, che consente uno scambio di esperienze e migliori pratiche, potrebbe contribuire in maniera significativo a sviluppare ulteriormente la convergenza "sul campo", facilitando in tal modo il rispetto delle norme sui trasferimenti transfrontalieri per le imprese che operano in regioni diverse del mondo.

- Norme vincolanti d'impresa

Un altro strumento importante è costituito dalle cosiddette norme vincolanti d'impresa. Si tratta di politiche e disposizioni giuridicamente vincolanti che si applicano ai membri di un gruppo societario, compresi i loro dipendenti (articolo 46, paragrafo 2, lettera b) e articolo 47 del regolamento generale sulla protezione dei dati). Il ricorso alle norme vincolanti d'impresa consente ai dati personali di circolare liberamente tra i vari membri del gruppo in tutto il mondo, dispensandoli dalla necessità di concludere accordi contrattuali tra tutte le singole entità del gruppo, garantendo allo stesso tempo che in tutto il gruppo sia rispettato il medesimo livello elevato di protezione dei dati personali. Tali norme offrono una soluzione particolarmente valida per i gruppi societari di grandi dimensioni e per una stretta cooperazione tra le imprese che si scambiano dati in più giurisdizioni. A differenza di quanto accadeva per la direttiva del 1995, le norme vincolanti d'impresa del regolamento generale sulla protezione dei dati possono essere utilizzate da un gruppo di imprese che svolgono un'attività economica congiunta ma non fanno parte del medesimo gruppo societario.

Dal punto di vista procedurale, le norme vincolanti d'impresa devono essere approvate dalle autorità di protezione dei dati competenti, sulla base di un parere non vincolante del comitato[140]. Per orientare questo processo, il comitato ha riesaminato i "criteri di riferimento" delle norme vincolanti d'impresa (definendo norme sostanziali) per i titolari del trattamento[141] e i responsabili del trattamento[142] alla luce del regolamento

---

[138] Conformemente all'articolo 46, paragrafo 2, lettera c), del regolamento generale sulla protezione dei dati, le clausole contrattuali tipo devono essere adottate secondo la procedura d'esame di cui all'articolo 5, del regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13). Ciò richiede in particolare una decisione positiva da parte di un comitato composto da rappresentanti degli Stati membri.

[139] Ciò comprende ad esempio il lavoro attualmente svolto dagli Stati membri dell'ASEAN per sviluppare "clausole contrattuali tipo dell'ASEAN". Cfr. ASEAN, *Key Approaches for ASEAN Cross Border Data Flows Mechanism* [Approcci chiave per il meccanismo dei flussi di dati transfrontalieri ASEAN] (disponibile in inglese al seguente indirizzo: https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf).

[140] Per una panoramica dei pareri del comitato europeo per la protezione dei dati pubblicati finora, cfr. https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_it.

[141] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109.

generale sulla protezione dei dati e continua ad aggiornare tali documenti sulla base dell'esperienza pratica acquisita dalle autorità di controllo. Ha adottato inoltre vari documenti di orientamento per aiutare i richiedenti e razionalizzare il processo di domanda e approvazione di norme vincolanti d'impresa[143]. Secondo il comitato, sono attualmente più di 40 le norme vincolanti d'impresa che stanno seguendo l'iter di approvazione, metà delle quali dovrebbe essere approvata entro la fine del 2020[144]. È importante che le autorità garanti della protezione dei dati continuino a lavorare con l'obiettivo di razionalizzare ulteriormente l'iter di approvazione, in quanto la durata di tali procedure è spesso menzionata dalle parti interessate come un ostacolo pratico a un ricorso maggiore alle norme vincolanti d'impresa.

Infine, per quanto riguarda specificamente le norme vincolanti d'impresa approvate dall'autorità di protezione dei dati del Regno Unito (*Information Commissioner Office*), le imprese potranno continuare a utilizzarle come un valido meccanismo di trasferimento ai sensi del regolamento generale sulla protezione dei dati dopo la fine del periodo transitorio a norma dell'accordo di recesso UE-Regno Unito, ma soltanto se vengono modificate in maniera tale da sostituire eventuali legami con il sistema giuridico del Regno Unito con riferimenti adeguati a imprese ed autorità competenti all'interno dell'UE. È opportuno chiedere l'approvazione di eventuali norme vincolanti d'impresa nuove da parte di una delle autorità di controllo dell'UE.

- Meccanismi di certificazione e codici di condotta

Oltre a modernizzare e ampliare l'applicazione degli strumenti di trasferimento già esistenti, il regolamento generale sulla protezione dei dati ha introdotto strumenti nuovi, ampliando in tal modo le possibilità di effettuare trasferimenti internazionali. Ciò include il ricorso, a determinate condizioni, a codici di condotta e meccanismi di certificazione approvati (quali sigilli nonché marchi di tutela della vita privata) al fine di assicurare garanzie adeguate. Si tratta di strumenti dal basso verso l'alto che consentono soluzioni personalizzate, quali un meccanismo generale di responsabilizzazione (cfr. articoli da 40 a 42 del regolamento generale sulla protezione dei dati) e, in particolare, per i trasferimenti internazionali di dati, che riflettono ad esempio le caratteristiche e le esigenze specifiche di un determinato settore o di una specifica industria oppure di flussi di dati particolari. Calibrando gli obblighi con i rischi, i codici di condotta possono costituire altresì un modo molto utile ed efficace sotto il profilo dei costi per consentire alle piccole e medie imprese di adempiere ai loro obblighi in materia di regolamento generale sulla protezione dei dati.

Per quanto concerne i meccanismi di certificazione, sebbene il comitato abbia adottato orientamenti per promuoverne l'uso all'interno dell'UE, il suo lavoro sullo sviluppo di criteri per l'approvazione di meccanismi di certificazione in quanto strumenti per i

---

142 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110.

143 Tali documenti sono stati adottati (dall'ex gruppo di lavoro Articolo 29) a seguito dell'entrata in vigore del regolamento generale sulla protezione dei dati, ma prima della fine del periodo di transizione. Cfr. WP263 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056);
WP264 (https://edpb.europa.eu/sites/edpb/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf);
WP265 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623848).

144 Contributo del comitato, pag. 7.

trasferimenti internazionali è ancora in corso. Lo stesso vale per i codici di condotta, in relazione ai quali il comitato sta attualmente lavorando a linee guida per il loro utilizzo come strumento per effettuare trasferimenti.

Data l'importanza di fornire agli operatori un'ampia gamma di strumenti di trasferimento adattati alle loro esigenze nonché il potenziale presentato in particolare dai meccanismi di certificazione nel facilitare i trasferimenti di dati garantendo nel contempo un livello elevato di protezione dei dati, la Commissione esorta il comitato a mettere a punto i suoi orientamenti al più presto. Ciò riguarda aspetti tanto sostanziali (criteri) quanto procedurali (approvazione, monitoraggio, ecc.). Le parti interessate hanno espresso molto interesse nei confronti di questi meccanismi di trasferimento e dovrebbero essere in grado di utilizzare appieno gli strumenti del regolamento generale sulla protezione dei dati. Gli orientamenti del comitato contribuirebbero inoltre a promuovere il modello dell'UE per la protezione dei dati a livello globale e a promuovere la convergenza dato che altri sistemi di tutela della vita privata utilizzano strumenti analoghi.

È possibile trarre insegnamenti preziosi dagli sforzi esistenti di standardizzazione nel settore della tutela della vita privata a livello tanto europeo quanto internazionale. Un esempio interessante è rappresentato dalla norma internazionale ISO 27701[145], di recente pubblicazione, che mira ad aiutare le imprese a soddisfare le prescrizioni in materia di tutela della vita privata e a gestire i rischi connessi al trattamento dei dati personali mediante "sistemi di gestione delle informazioni per la tutela della vita privata". Sebbene la certificazione ai sensi della norma in quanto tale non soddisfi le prescrizioni di cui agli articoli 42 e 43 del regolamento generale sulla protezione dei dati, l'applicazione di sistemi di gestione delle informazioni per la tutela della vita privata può contribuire alla responsabilizzazione, anche nel contesto di trasferimenti internazionali di dati.

- Accordi internazionali e accordi amministrativi

Il regolamento generale sulla protezione dei dati consente inoltre di assicurare garanzie adeguate per i trasferimenti di dati tra autorità o enti pubblici sulla base di accordi internazionali [articolo 46, paragrafo 2, lettera a)] o di disposizioni amministrative [articolo 46, paragrafo 3, lettera b)]. Sebbene entrambi gli strumenti debbano assicurare il medesimo esito in termini di garanzie, nonché diritti azionabili e mezzi di ricorso effettivi degli interessati, essi differiscono in termini di loro natura giuridica e loro procedura di adozione.

A differenza degli accordi internazionali, che creano obblighi vincolanti ai sensi del diritto internazionale, gli accordi amministrativi (ad esempio sotto forma di un protocollo d'intesa) sono di norma non vincolanti e richiedono pertanto un'autorizzazione preventiva da parte dell'autorità di protezione dei dati competente (cfr. anche il considerando 108 del regolamento generale sulla protezione dei dati). Un esempio precoce riguarda l'accordo amministrativo per il trasferimento di dati personali tra autorità di controllo finanziario del SEE e non appartenenti al SEE che cooperano sotto l'egida dell'Organizzazione internazionale delle commissioni sui

[145]L'elenco delle prescrizioni specifiche che compongono la norma ISO è disponibile al seguente indirizzo: https://www.iso.org/standard/71670.html.

valori mobiliari (IOSCO), rispetto al quale il comitato ha espresso il suo parere[146] all'inizio del 2019. Da allora il comitato ha ulteriormente sviluppato la propria interpretazione di "garanzie minime" che gli accordi internazionali (di cooperazione) e gli accordi amministrativi tra autorità pubbliche od organismi (comprese le organizzazioni internazionali) devono assicurare per rispettare le prescrizioni di cui all'articolo 46 del regolamento generale sulla protezione dei dati. Il 18 gennaio 2020 ha adottato un progetto di linee guida[147], rispondendo così alla richiesta degli Stati membri di fornire ulteriori chiarimenti e orientamenti in merito a ciò che può essere considerato rientrare nel concetto di "garanzie adeguate" per i trasferimenti tra autorità pubbliche[148]. Il comitato raccomanda vivamente alle autorità pubbliche di utilizzare i tali orientamenti come punto di riferimento per i negoziati con terze parti[149].

Gli orientamenti dimostrano la flessibilità nella progettazione di tali strumenti, anche per quanto riguarda aspetti importanti quali la vigilanza[150] e i mezzi di ricorso[151]. Ciò dovrebbe consentire alle autorità pubbliche di superare le difficoltà ad esempio nel

---

[146] Comitato europeo per la protezione dei dati, parere 4/2019 sul progetto di accordo amministrativo per il trasferimento di dati personali tra le autorità di vigilanza finanziaria dello Spazio economico europeo (SEE) e le autorità di vigilanza finanziaria al di fuori del SEE, 12.2.2019.

[147] Comitato europeo per la protezione dei dati, *Guidelines 2/2020 on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies* [Linee guida 2/2020 sull'articolo 46, paragrafo 2, lettera a) e sull'articolo 46, paragrafo 3, lettera b) del regolamento 2016/679 per i trasferimenti di dati personali tra autorità ed organismi pubblici del SEE e non appartenenti al SEE] (progetto disponibile in inglese al seguente indirizzo: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_it). Secondo il comitato europeo per la protezione dei dati, "[l'autorità di controllo] competente baserà il proprio esame sulle raccomandazioni generali contenute nei presenti orientamenti, ma potrebbe anche chiedere garanzie maggiori in funzione del caso specifico". Il comitato ha presentato tali progetti di linee guida a una consultazione pubblica conclusasi il 18 maggio 2020.

[148] Posizione e conclusioni del Consiglio, punto 20.

[149] Allo stesso tempo il comitato chiarisce che le autorità pubbliche rimangono "libere di fare affidamento su altri strumenti pertinenti che prevedono garanzie adeguate ai sensi dell'articolo 46 del regolamento generale sulla protezione dei dati". Per quanto concerne la scelta dello strumento, il comitato sottolinea che "[è] opportuno valutare attentamente se ricorrere o meno ad accordi amministrativi giuridicamente non vincolanti per fornire garanzie nel settore pubblico, in considerazione della finalità del trattamento e della natura dei dati in questione. Se i diritti alla protezione dei dati e i mezzi di ricorso a disposizione delle persone fisiche del SEE non sono previsti dal diritto interno del paese terzo, occorre dare la preferenza alla conclusione di un accordo giuridicamente vincolante. Indipendentemente dal tipo di strumento adottato, le misure in vigore devono essere efficaci per garantire un'attuazione, un'applicazione e una vigilanza adeguate" (punto 67).

[150] Ciò può comprendere ad esempio la combinazione di verifiche interne (con l'impegno a informare l'altra parte in merito a qualsiasi caso di mancato rispetto della vigilanza indipendente attraverso meccanismi esterni o quanto meno attraverso meccanismi autonomi dal punto di vista funzionale), nonché la possibilità per l'ente pubblico trasferente di sospendere o cessare il trasferimento.

[151] Ciò può comprendere ad esempio meccanismi vincolanti quasi giudiziari (ad esempio l'arbitrato) oppure meccanismi di risoluzione alternativa delle controversie, associati alla possibilità per l'autorità pubblica trasferente di sospendere o cessare il trasferimento di dati personali qualora le parti non riescano a risolvere amichevolmente una controversia, oltre ad un impegno da parte dell'autorità pubblica ricevente di restituire o cancellare i dati personali. Quando opta per meccanismi di ricorso alternativi sotto forma di strumenti vincolanti ed esecutivi poiché non vi è la possibilità di garantire un ricorso giurisdizionale effettivo, il comitato raccomanda di chiedere il parere dell'autorità di controllo competente prima di concludere tali strumenti.

garantire che i diritti dell'interessato siano azionabili mediante accordi non vincolanti. Un aspetto importante di tali accordi è il loro continuo monitoraggio da parte dell'autorità di protezione dei dati competente, sostenuta dalle prescrizioni in materia di informazione e tenuta di registri, nonché la sospensione dei flussi di dati, se non è più possibile assicurare nella pratica garanzie adeguate.

Deroghe

Infine il regolamento generale sulla protezione dei dati chiarisce il ricorso alle cosiddette "deroghe". Si tratta di motivi specifici per i trasferimenti di dati (ad esempio consenso esplicito[152], esecuzione di un contratto o importanti motivi di interesse pubblico) riconosciuti dalla legge e sui quali i soggetti possono fare affidamento in assenza di altri strumenti di trasferimento e a determinate condizioni.

Per chiarire l'uso di tali motivi previsti dalla legge, il comitato ha pubblicato orientamenti specifici[153] e interpretato l'articolo 49 in una serie di casi riguardanti scenari specifici di trasferimento[154]. In ragione del loro carattere eccezionale, il comitato ritiene che le deroghe debbano essere interpretate in modo restrittivo caso per caso. Nonostante la loro interpretazione restrittiva, tali motivi riguardano un'ampia gamma di scenari di trasferimento. Ciò comprende, in particolare, i trasferimenti di dati da parte di autorità pubbliche e soggetti privati necessari per "importanti motivi di interesse pubblico", ad esempio tra le autorità garanti della concorrenza, le autorità finanziarie, fiscali o doganali, i servizi competenti in materia di sicurezza sociale o per la sanità pubblica (come nel caso del tracciamento dei contatti in relazione a malattie contagiose o per eliminare il doping nello sport)[155]. Un altro settore è quello della cooperazione transfrontaliera per finalità di contrasto penale, in particolare per quanto riguarda i reati gravi[156].

Il comitato ha chiarito che, sebbene il pertinente interesse pubblico debba essere riconosciuto nel diritto dell'UE o dello Stato membro, ciò può essere stabilito anche sulla base di "un accordo o di una convenzione internazionale che stabilisca un

---

[152] Si tratta di un cambiamento rispetto alla direttiva 95/46, che si limitava a richiedere il consenso "inequivocabile". Inoltre si applicano le prescrizioni generali in materia di consenso di cui all'articolo 4, paragrafo 11, del regolamento generale sulla protezione dei dati.

[153] Comitato europeo per la protezione dei dati, linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679, 25.5.2018 (disponibile al seguente indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_it.pdf).

[154] Ciò comprende ad esempio i trasferimenti internazionali di dati sanitari per finalità di ricerca nel contesto della pandemia di Covid-19. Cfr. comitato europeo per la protezione dei dati, Linee guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al Covid-19, 21.4.2020 (disponibile all'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_it.pdf).

[155] Cfr. considerando 112.

[156] Cfr. lettera della Commissione europea per conto dell'Unione europea in veste di *amicus curiae* a sostegno di nessuna delle parti nella causa *Stati Uniti contro Microsoft*, pag. 15: "[i]n generale il diritto dell'Unione così come quello interno degli Stati membri riconosce l'importanza della lotta contro le forme gravi di criminalità e, di conseguenza, l'applicazione del diritto penale e la cooperazione internazionale a tale riguardo, come un obiettivo di interesse generale. [...] L'articolo 83 del TFUE individua diversi settori della criminalità particolarmente gravi e aventi dimensioni transfrontaliere, come il traffico illecito di stupefacenti" (disponibile in inglese all'indirizzo https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf).

determinato obiettivo, da favorire con la cooperazione internazionale, [che] può essere un indicatore ai fini della valutazione dell'esistenza di un interesse pubblico ai sensi dell'articolo 49, paragrafo 1, lettera d), purché l'Unione europea o gli Stati membri abbiano sottoscritto tale accordo o convenzione"[157].

Decisioni da parte di organi giurisdizionali o autorità stranieri: non costituiscono motivo di trasferimento

Oltre a stabilire in maniera positiva i motivi per i trasferimenti di dati, il capo V del regolamento generale sulla protezione dei dati chiarisce anche (all'articolo 48) che le ordinanze di organi giurisdizionali e le decisioni di autorità amministrative al di fuori dell'UE non costituiscono tali motivi, fatto salvo il caso in cui siano riconosciuti o resi esecutivi sulla base di un accordo internazionale (ad esempio un trattato di mutua assistenza giudiziaria). Qualsiasi divulgazione da parte del soggetto richiesto nell'UE all'organismo straniero o all'autorità straniera in risposta a tale ordinanza o decisione costituisce un trasferimento internazionale di dati che deve basarsi su uno degli strumenti di trasferimento menzionati[158].

Il regolamento generale sulla protezione dei dati non costituisce una "disposizione di legge di divieto" e, a determinate condizioni, consente un trasferimento in risposta a una richiesta appropriata di applicazione della legge da parte di un paese terzo. L'aspetto importante è che sia il diritto dell'UE a stabilire se questo sia il caso e sulla base di quali garanzie sia possibile effettuare tali trasferimenti.

La Commissione ha illustrato il funzionamento dell'articolo 48 del regolamento generale sulla protezione dei dati, compreso il possibile ricorso alla deroga per motivi di interesse pubblico, nel contesto di un'ordinanza (mandato) di produzione di prove di un'autorità straniera incaricata dell'applicazione del diritto penale nella causa *Microsoft* dinanzi la Corte suprema degli Stati Uniti[159]. A suo avviso la Commissione

---

[157] Comitato europeo per la protezione dei dati, Linee guida sulle deroghe (supra nota 153), pag. 10. Il comitato europeo per la protezione dei dati ha inoltre chiarito che, sebbene i trasferimenti di dati basati sulla deroga per motivi di interesse pubblico non debbano essere "su larga scala" o "sistematici", ma "[debbano] essere limitati a situazioni specifiche e [...] garantire la conformità [...] al rigido test di necessità", non è necessario che essi siano "occasionali".

[158] Ciò è chiarito dalla formulazione dell'articolo 48 del regolamento generale sulla protezione dei dati ("fatti salvi gli altri presupposti di trasferimento a norma del presente capo") e del considerando 115 di accompagnamento ("[i] trasferimenti dovrebbero quindi essere consentiti solo se ricorrono le condizioni previste dal presente regolamento per i trasferimenti a paesi terzi. Ciò vale, tra l'altro, quando la comunicazione è necessaria per un rilevante motivo di interesse pubblico riconosciuto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento"). Tale aspetto è riconosciuto anche dal comitato europeo per la protezione dei dati, cfr. linee guida sulle deroghe (supra nota 153), pag. 5. Come per tutti i trattamenti, occorre che siano rispettate anche le altre garanzie previste dal regolamento (ad esempio i dati devono essere trasferiti per una finalità specifica, devono essere pertinenti, limitati a quanto necessario per le finalità della richiesta, ecc.).

[159] Presentazione Microsoft (supra nota 156). Come spiegato dalla Commissione, il regolamento generale sulla protezione dei dati rende pertanto i trattati di mutua assistenza giudiziaria "l'opzione preferita" per i trasferimenti in quanto tali trattati "prevedono la raccolta di prove mediante consenso e sono l'espressione di un equilibrio accuratamente negoziato tra gli interessi di Stati diversi, che è stato concepito per attenuare i conflitti giurisdizionali che possono sorgere in altro modo". Cfr. anche comitato europeo per la protezione dei dati, Linee guida sulle deroghe (supra nota 153), pag. 5 ("Laddove sussista un accordo internazionale, quale un trattato bilaterale di mutua assistenza giudiziaria, in linea generale le imprese dell'Unione dovrebbero rifiutare richieste dirette e rimandare l'autorità richiedente del paese terzo all'accordo o al trattato vigente").

ha sottolineato l'interesse dell'UE a garantire che la cooperazione in materia di applicazione della legge si svolga "in un quadro giuridico che eviti conflitti di legge e si basi sul [...] rispetto degli interessi fondamentali reciproci nel contesto tanto della tutela della vita privata quanto delle attività di contrasto"[160]. In particolare, "dal punto di vista del diritto internazionale pubblico, quando un'autorità pubblica impone a un'impresa stabilita nella propria giurisdizione di produrre dati elettronici conservati in un server in una giurisdizione straniera, si assumono i principi di territorialità e di cortesia ai sensi del diritto internazionale pubblico"[161].

Ciò trova riscontro anche nella proposta della commissione di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale[162], che contiene una specifica "clausola di cortesia" che consente di sollevare un'obiezione nei confronti di un ordine di produzione di prove qualora il rispetto delle leggi di un paese terzo contrasti con le leggi di un paese terzo che vietano la divulgazione, in particolare sulla base del motivo che ciò è necessario per tutelare i diritti fondamentali delle persone interessate[163].

Garantire la cortesia internazionale è importante, dato che le attività di applicazione della legge, così come i reati e in particolare i reati informatici, hanno sempre più natura transfrontaliera e pertanto sollevano spesso questioni giurisdizionali e creano potenziali conflitti di legge[164]. Non sorprende che il modo migliore per affrontare tali questioni sia attraverso accordi internazionali che prevedano le necessarie limitazioni e garanzie per l'accesso transfrontaliero a dati personali, anche assicurando un livello elevato di protezione dei dati da parte dell'autorità richiedente.

La Commissione, agendo a nome dell'UE, è attualmente impegnata in negoziati multilaterali per un secondo protocollo aggiuntivo alla convenzione del Consiglio d'Europa sulla criminalità informatica ("Budapest"), che mira a rafforzare le norme

---

160 Presentazione Microsoft (supra nota 156), pag. 4.

161 Presentazione Microsoft supra nota 156), pag. 6.

162 Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale [COM(2018) 225 final], 17.4.2018. Il 7.12.2018 il Consiglio ha adottato il proprio approccio generale alla proposta di regolamento (disponibile all'indirizzo: https://www.consilium.europa.eu/it/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-eevidence-council-agrees-its-position/#). Cfr. anche GEPD, Parere 7/19 sulle proposte relative a ordini europei di produzione e di conservazione di prove elettroniche in materia penale (disponibile all'indirizzo: https://edps.europa.eu/data-protection/ourwork/publications/opinions/electronic-evidence-criminal-matters_en).

163 La relazione, pag. 35, chiarisce che, oltre a rispettare il principio di cortesia internazionale rispetto agli interessi sovrani dei paesi terzi, proteggere la persona interessata e far fronte a eventuali obblighi contrastanti in capo al prestatore di servizi, una motivazione importante per la clausola di cortesia è la reciprocità, ossia la garanzia del rispetto delle norme UE, compresa la protezione dei dati personali (articolo 48 del regolamento generale sulla protezione dei dati). Cfr. anche dichiarazione del gruppo di lavoro Articolo 29 del 29 novembre 2017, *Data protection and privacy aspects of cross-border access to electronic evidence* [Aspetti relativi alla protezione dei dati e alla tutela della vita privata nel contesto dell'accesso transfrontaliero a prove elettroniche] (Dichiarazione WP29) (disponibile al seguente indirizzo: file:///C:/Users/ralfs/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/20171207_e-Evidence_Statement_FINALpdf%20(1).pdf), pag. 9.

164 Cfr. dichiarazione WP29 (supra nota 163), pag. 6.

esistenti per ottenere l'accesso transfrontaliero alle prove elettroniche nelle indagini penali, garantendo nel contempo adeguate garanzie in materia di protezione dei dati nell'ambito del protocollo[165]. Analogamente, sono stati avviati negoziati bilaterali su un accordo tra l'UE e gli Stati Uniti in materia di accesso transfrontaliero a prove elettroniche per la cooperazione giudiziaria in materia penale[166]. La Commissione conta sul sostegno del Parlamento europeo e del Consiglio e sugli orientamenti del comitato europeo per la protezione dei dati in tutti questi negoziati.

Più in generale 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.

7.3 Cooperazione internazionale nel settore della protezione dei dati

Promuovere la convergenza tra sistemi diversi di tutela della vita privata significa anche trarre insegnamenti reciproci, attraverso lo scambio di conoscenze, esperienze e migliori pratiche. Tali scambi sono essenziali per far fronte alle nuove sfide sempre più globali in termini di natura e portata. Per questo motivo la Commissione ha intensificato il proprio dialogo sulla protezione dei dati e sui flussi di dati con un'ampia gamma di soggetti e in sedi diverse, a livello bilaterale, regionale e multilaterale.

La dimensione bilaterale

In seguito all'adozione del regolamento generale sulla protezione dei dati, si è registrato un maggiore interesse nei confronti dell'esperienza dell'UE nella progettazione, nella negoziazione e nell'attuazione delle norme moderne sulla tutela

---

[165] Cfr. raccomandazione di decisione del Consiglio che autorizza la partecipazione ai negoziati su un secondo protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica (STCE n. 185) [COM(2019) 71 final] 5.2.2019. Cfr. anche GEPD, Parere 3/2019 concernente la partecipazione ai negoziati in vista di un secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica, 2.4.2019 (disponibile in inglese al seguente indirizzo: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_budapest_convention_en.pdf); comitato europeo per la protezione dei dati, *Contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)* [Contributo alla consultazione su un secondo protocollo aggiuntivo alla convenzione del Consiglio d'Europa sulla criminalità informatica ("convenzione di Budapest")], 13.11.2019 (disponibile al seguente indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf).

[166] Cfr. raccomandazione di decisione del Consiglio che autorizza l'avvio di negoziati in vista di un accordo tra l'Unione europea e gli Stati Uniti d'America sull'accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale [COM(2019) 70 final], 5.2.2019. Cfr. anche GEPD, Parere 2/2019 sul mandato di negoziato concernente un accordo tra l'UE e gli USA sull'accesso transfrontaliero alle prove elettroniche (disponibile al seguente indirizzo: https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf).

della vita privata. Il dialogo con i paesi che hanno avviato processi analoghi ha assunto forme diverse.

I servizi della Commissione hanno presentato osservazioni su una serie di consultazioni pubbliche organizzate da governi stranieri concernenti la legislazione in materia di tutela della vita privata ad esempio da parte di Stati Uniti[167], India[168], Malaysia ed Etiopia. In alcuni paesi terzi, i servizi della Commissione hanno avuto il privilegio di testimoniare dinanzi gli organi parlamentari competenti, ad esempio in Brasile[169], Cile[170], Ecuador e Tunisia[171].

Inoltre, nel contesto delle attuali riforme delle leggi sulla protezione dei dati, si sono tenute riunioni dedicate con i rappresentanti del governo o le delegazioni parlamentari di numerose regioni del mondo (ad esempio Georgia, Kenya, Taiwan, Thailandia, Marocco). Ciò ha incluso l'organizzazione di seminari e visite di studio ad esempio con rappresentanti del governo indonesiano e una delegazione del personale del congresso degli Stati Uniti. Ciò ha fornito l'opportunità di chiarire concetti importanti del regolamento generale sulla protezione dei dati, di migliorare la comprensione reciproca in materia di tutela della vita privata e di illustrare i vantaggi della convergenza per garantire un livello elevato di protezione dei diritti individuali, degli scambi e della cooperazione. In taluni casi ha altresì consentito di ammonire in merito a taluni malintesi relativi alla protezione dei dati che possono comportare l'introduzione di misure protezionistiche quali gli obblighi di localizzazione forzata.

Dall'adozione del regolamento generale sulla protezione dei dati, la Commissione ha inoltre avviato un dialogo con diverse organizzazioni internazionali, anche alla luce dell'importanza degli scambi di dati con tali organizzazioni in una serie di settori interessati. In particolare è stato instaurato un dialogo specifico con le Nazioni Unite,

---

[167] Cfr. osservazioni della DG Giustizia e di consumatori del 9 novembre 2018 in risposta a una richiesta di osservazioni da parte del pubblico su un approccio proposto alla tutela della vita privata dei consumatori [prot. n. 180821780-8780-01] dall'amministrazione nazionale delle telecomunicazioni e dell'informazione degli Stati Uniti (disponibile all'indirizzo: https://ec.europa.eu/info/sites/info/files/european_commission_submission_on_a_proposed_approach_to_consumer_privacy.pdf).

[168] Cfr. osservazioni presentate dalla DG Giustizia e da consumatori del 19 novembre 2018 sul progetto di legge sulla protezione dei dati personali dell'India del 2018 al ministero dell'Elettronica e della tecnologia dell'informazione (disponibile all'indirizzo: https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en).

[169] Cfr. riunione plenaria del 17 aprile 2018 del Senato brasiliano (https://www25.senado.leg.br/web/atividade/sessao-plenaria/-/pauta/23384), riunione del 10 aprile 2019 del comitato misto in merito al MP 869/2018 del congresso brasiliano (https://www12.senado.leg.br/ecidadania/visualizacaoaudiencia?id=15392), e riunione del 26 novembre 2019 del comitato speciale della camera dei deputati brasiliana (https://www.camara.leg.br/noticias/616579-comissao-discutira-protecao-de-dados-no-ambito-das-constituicoes-de-outros-paises/).

[170] Cfr. riunioni del 29 maggio 2018 (https://senado.cl/appsenado/index.php?mo=comisiones&ac=asistencia_sesion&idcomision=186&idsesion=12513&idpunto=15909&sesion=29/05/2018&listado=1) e del 24 aprile 2019 (https://www.senado.cl/appsenado/index.php?mo=comisiones&ac=sesiones_celebradas&idcomision=186&tipo=3&legi=485&ano=2019&desde=0&hasta=0&idsesion=13603&idpunto=17283&listado=2) nonché della commissione costituzionale, legislativa e giudiziaria del Senato cileno.

[171] Cfr. riunione del 2 novembre 2018 della commissione Diritti, libertà e relazioni esterne dell'Assemblea tunisina dei rappresentanti del popolo (https://www.facebook.com/1515094915436499/posts/2264094487203201/).

al fine di facilitare le discussioni con tutte le parti interessate al fine di assicurare trasferimenti agevoli dei dati e sviluppare ulteriormente la convergenza tra i rispettivi sistemi di protezione dei dati. Nel contesto di tale dialogo, la Commissione collaborerà strettamente con il comitato europeo per la protezione dei dati per chiarire ulteriormente in che modo gli operatori pubblici e privati dell'UE possano adempiere i loro obblighi in materia di regolamento generale sulla protezione dei dati quando scambiano dati con organizzazioni internazionali quali le Nazioni Unite.

La Commissione è pronta a continuare a condividere gli insegnamenti tratti dal suo processo di riforma con i paesi interessati e con le organizzazioni internazionali, così come ha tratto insegnamenti da altri sistemi in fase di elaborazione della propria proposta di nuove norme dell'UE in materia di protezione dei dati. Questo tipo di dialogo è reciprocamente vantaggioso per l'UE e i suoi partner in quanto consente di ottenere una migliore comprensione del contesto in rapida evoluzione in materia di tutela della vita privata e di scambiare opinioni su soluzioni giuridiche e tecnologiche emergenti.

È in questo spirito che la Commissione sta istituendo una "Accademia per la protezione dei dati" destinata a promuovere gli scambi tra le autorità di regolamentazione europee e di paesi terzi e, in tal modo, a migliorare la cooperazione "sul campo".

Inoltre è necessario sviluppare 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. La Commissione si avvarrà pertanto dei poteri concessi in questo settore dall'articolo 50 del regolamento generale sulla protezione dei dati e, in particolare, intende chiedere l'autorizzazione ad avviare negoziati per la conclusione di accordi di cooperazione in materia di esecuzione con i paesi terzi pertinenti. In tale contesto, terrà altresì conto dei pareri del comitato in merito a quali paesi dovrebbero essere considerati prioritari alla luce del volume dei trasferimenti di dati, del ruolo e dei poteri dell'autorità di contrasto in materia di tutela della vita privata nel paese terzo e della necessità di una cooperazione in materia di applicazione della legge per affrontare casi di interesse comune.

La dimensione multilaterale

Oltre agli scambi bilaterali, la Commissione partecipa attivamente a una serie di consessi multilaterali per promuovere valori condivisi e sviluppare una convergenza a livello regionale e globale.

L'adesione sempre più universale alla "Convenzione 108" del Consiglio d'Europa, l'unico strumento multilaterale giuridicamente vincolante in materia di protezione dei dati personali, è una chiara indicazione di questa tendenza verso una convergenza (verso l'alto)[172]. La convenzione, aperta anche ai non aderenti al Consiglio d'Europa, è

[172] È importante sottolineare che la convenzione aggiornata non è soltanto un trattato che prevede forti garanzie in materia di protezione dei dati, ma crea anche una rete di autorità di controllo con strumenti per la cooperazione in materia di applicazione della legge e, con la commissione della

già stata ratificata da 55 paesi tra cui alcuni Stati africani e dell'America latina[173]. La Commissione ha contribuito in maniera significativa all'esito positivo dei negoziati sull'aggiornamento della convenzione[174] e ha garantito che riflettesse gli stessi principi sanciti dalle norme dell'UE in materia di protezione dei dati. La maggior parte degli Stati membri dell'UE ha firmato il protocollo di modifica, anche se le firme di Danimarca, Malta e Romania sono ancora pendenti. Finora solo quattro Stati membri (Bulgaria, Croazia, Lituania e Polonia) hanno ratificato il protocollo di modifica. La Commissione esorta i tre Stati membri rimanenti a firmare la convenzione aggiornata e tutti gli Stati membri a procedere rapidamente alla ratifica, in maniera da consentirne l'entrata in vigore nel prossimo futuro[175]. Oltre a ciò continuerà ad incoraggiare in maniera proattiva l'adesione da parte di paesi terzi.

I flussi di dati e la protezione dei dati sono stati affrontati di recente anche in seno al G20 e al G7. Nel 2019 i leader mondiali hanno approvato per la prima volta l'idea che la protezione dei dati contribuisca a creare fiducia nell'economia digitale e faciliti i flussi di dati. Con il sostegno attivo della Commissione[176], i leader hanno approvato il concetto di "Data Free Flow with Trust" (DFFT) originariamente proposto dal Giappone nella dichiarazione di Osaka del G20[177] e dal vertice del G7 a Biarritz[178]. Tale approccio trova riscontro anche nella comunicazione della Commissione del 2020 dal titolo "Una strategia europea per i dati"[179], che mette in evidenza la sua intenzione di continuare a promuovere la condivisione di dati con partner di fiducia,

---

Convenzione, un forum di discussione, scambio di migliori pratiche e sviluppo di norme internazionali.

173 Cfr. elenco completo dei membri: https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/108/signatures. Tra i paesi dell'Africa figurano Capo Verde, Maurizio, Marocco, Senegal e Tunisia; tra quelli dell'America latina si annoverano invece Argentina, Messico e Uruguay. Il Burkina Faso è stato invitato ad aderire alla convenzione.

174 Cfr. testo della convenzione aggiornata: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf.

175 Secondo la propria decisione sul protocollo di modifica del 18 maggio 2018, il comitato dei ministri "ha sollecitato gli Stati membri e le altre parti della convenzione ad adottare senza indugio le misure necessarie per consentire l'entrata in vigore del protocollo entro tre anni dalla sua apertura alla firma nonché ad avviare immediatamente, ma in ogni caso entro un anno dalla data di apertura del protocollo alla firma, il processo previsto dalla loro legislazione nazionale che porta alla ratifica...". Ha inoltre "incaricato i suoi deputati di esaminare ogni due anni e per la prima volta un anno dopo la data di apertura del protocollo alla firma, i progressi complessivi compiuti verso la ratifica sulla base delle informazioni che devono essere fornite al segretario generale da ciascuno degli Stati membri e dalle altre Parti della convenzione al più tardi un mese prima di tale esame". Cfr. https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016808a3c9f.

176 A margine del vertice UE-Giappone dell'aprile del 2019, il presidente Juncker ha espresso sostegno a favore dell'iniziativa del Giappone "Data Free Flow with Trust" e del lancio della "Osaka Track" e ha impegnato la Commissione a "svolgere un ruolo attivo nel contesto di entrambe le iniziative".

177 Cfr. testo della dichiarazione dei leader del G20 di Osaka: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

178 Cfr. testo della strategia del G7 di Biarritz per una trasformazione digitale aperta, libera e sicura: https://www.elysee.fr/admin/upload/default/0001/05/62a9221e66987d4e0d6ffcb058f3d2c649fc6d9d.pdf.

179 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], 19.2.2020 (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0066&from=IT), pagg. 26-27.

lottando al tempo stesso contro gli abusi, quali un accesso sproporzionato ai dati da parte di autorità pubbliche (straniere).

Così facendo l'UE potrà contare su una serie di strumenti in diversi settori interessati che tengono sempre più conto dell'impatto sulla tutela della vita privata: ad esempio il primo quadro in assoluto dell'UE per il controllo degli investimenti esteri, che diventerà pienamente applicabile nell'ottobre del 2020, conferisce all'UE e ai suoi Stati membri la possibilità di esaminare le operazioni di investimento che hanno effetti sull'"accesso a informazioni sensibili, compresi i dati personali, o la capacità di controllare tali informazioni", se incidono sulla sicurezza o sull'ordine pubblico[180].

In diversi altri consessi multilaterali la Commissione collabora con paesi con vedute analoghe al fine di promuovere attivamente i propri valori e le proprie norme. Un consesso importante è costituito dal gruppo di lavoro dell'OCSE sulla tutela della vita privata e la governance dei dati (DGP), che persegue una serie di importanti iniziative in materia di protezione dei dati, condivisione dei dati e trasferimenti di dati. Ciò comprende la valutazione delle linee guida dell'OCSE del 2013 in materia di tutela della vita privata. Inoltre la Commissione ha contribuito attivamente alla raccomandazione del Consiglio dell'OCSE sull'intelligenza artificiale[181] e ha garantito che l'approccio incentrato sulla persona sia rispecchiato nel testo finale, il che significa che le applicazioni di intelligenza artificiale devono rispettare i diritti fondamentali e in particolare la protezione dei dati. È importante sottolineare che la raccomandazione sull'intelligenza artificiale, che è stata successivamente integrata nei principi in materia di intelligenza artificiale del G20 allegati alla dichiarazione dei leader del G20 di Osaka[182], stabilisce i principi di trasparenza e spiegabilità al fine di "consentire a coloro che sono stati lesi da un sistema di intelligenza artificiale di contestarne l'esito sulla base di informazioni semplici e facilmente comprensibili sui fattori e sulla logica utilizzati come base per la previsione, la raccomandazione o la decisione", rispecchiando così da vicino i principi del regolamento generale sulla protezione dei dati per quanto riguarda il processo decisionale automatizzato[183].

La Commissione sta inoltre intensificando il dialogo con le organizzazioni e le reti regionali che svolgono sempre più un ruolo centrale nella definizione di norme comuni in materia di protezione dei dati[184], promuovendo lo scambio di migliori pratiche e facilitando la cooperazione tra le autorità di contrasto. Ciò riguarda, in particolare, l'Associazione delle nazioni del sud-est asiatico (ASEAN), anche nel contesto dei lavori in corso in materia di strumenti di trasferimento di dati, l'Unione africana, il forum delle autorità di protezione dei dati Asia-Pacifico (APPA, *Asia Pacific Privacy Authorities forum*) e la rete per la protezione dei dati ibero-americana (*Ibero-American Data Protection Network*), che hanno dato il via a importanti

---

[180] Articolo 4, paragrafo 1, lettera d), del regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio, del 19 marzo 2019, che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione (GU L 79I del 21.3.2019, pag. 1).

[181] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[182] Dichiarazione ministeriale del G20 sul commercio e sull'economia digitali: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

[183] Cfr. articolo 13, paragrafo 2, lettera f), articolo 14, paragrafo 2, lettera g) e articolo 22 del regolamento generale sulla protezione dei dati.

[184] Cfr. ad esempio la *convenzione sulla sicurezza informatica e la protezione dei dati personali* dell'Unione africana ("convenzione di Malabo") e le *norme per la protezione dei dati per gli Stati ibero-americani* sviluppate dalla rete per la protezione dei dati ibero-americana.

iniziative in questo settore e mettono a disposizione consessi per un dialogo proficuo tra le autorità di regolamentazione in materia di tutela della vita privata e altre parti interessate.

L'Africa è un esempio significativo della complementarità tra le dimensioni nazionale, regionale e mondiale della tutela della vita privata. Le tecnologie digitali stanno trasformando rapidamente e profondamente il continente africano. Ciò può potenzialmente accelerare il conseguimento degli obiettivi di sviluppo sostenibile promuovendo la crescita economica, alleviando la povertà e migliorando la vita delle persone. Disporre di un quadro moderno per la protezione dei dati che attragga investimenti e promuova lo sviluppo di imprese competitive, contribuendo nel contempo al rispetto dei diritti umani, della democrazia e allo Stato di diritto, è un aspetto fondamentale di tale trasformazione. L'armonizzazione delle norme in materia di protezione dei dati in tutta l'Africa consentirebbe l'integrazione del mercato digitale, mentre la convergenza con le norme globali agevolerebbe gli scambi di dati con l'UE. Tali dimensioni diverse della protezione dei dati sono interconnesse e si rafforzano reciprocamente.

In numerosi paesi africani si registra attualmente un interesse crescente per la protezione dei dati e il numero di paesi africani che hanno adottato o stanno adottando norme moderne in materia di protezione dei dati ha ratificato la convenzione 108[185] o la convenzione di Malabo[186] continua ad aumentare[187]. Nel contempo il quadro normativo rimane fortemente disomogeneo e frammentato in tutto il continente africano. Numerosi paesi offrono ancora garanzie scarse o inesistenti in materia di protezione dei dati. Le misure che limitano i flussi di dati sono ancora diffuse e ostacolano lo sviluppo di un'economia digitale regionale.

Per sfruttare i vantaggi reciproci della convergenza delle norme sulla protezione dei dati, la Commissione si impegnerà con i partner africani tanto a livello bilaterale quanto di consessi regionali[188]. Ciò si basa sui lavori della task force UE-UA sull'economia digitale nel contesto del nuovo partenariato Africa-Europa per l'economia digitale[189]. Nel perseguire tali obiettivi, inoltre, l'ambito di applicazione

[185] Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=DW5jevqD.

[186] Convenzione dell'Unione Africana sulla sicurezza informatica e sulla protezione dei dati personali https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection. Diverse comunità economiche regionali hanno inoltre sviluppato norme sulla protezione dei dati, ad esempio la Comunità economica degli Stati dell'Africa occidentale (ECOWAS) e la Comunità per lo sviluppo dell'Africa meridionale (SADC). Cfr. rispettivamente http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf e http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf.

[188] Tra l'altro, attraverso l'iniziativa di politica e regolamentazione per l'Africa digitale (PRIIDA), cfr. informazioni al seguente indirizzo: https://www.africa-eu-partnership.org/en/projects/policy-and-regulation-initiative-digital-africa-prida.

[189] Cfr. comunicazione congiunta della Commissione europea e dell'alto rappresentante per gli affari esteri e la politica di sicurezza "Verso una strategia globale per l'Africa" (disponibile al seguente indirizzo: https://ec.europa.eu/international-partnerships/system/files/communication-eu-africa-strategy-join-2020-4-final_en.pdf); Task force sull'economia digitale, nuovo partenariato Africa-Europa per l'economia digitale: *Accelerating the Achievement of the Sustainable Development Goals*

dello strumento di partenariato della Commissione "Protezione rafforzata dei dati e flussi di dati" è stato esteso per includere l'Africa. Il progetto sarà mobilitato per sostenere i paesi africani che intendono sviluppare quadri moderni di protezione dei dati o che desiderano rafforzare la capacità delle loro autorità di regolamentazione, attraverso la formazione, la condivisione di conoscenze e lo scambio di migliori pratiche.

Infine, 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 scambi, la Commissione è anche determinata ad affrontare il protezionismo digitale, come recentemente sottolineato nella strategia in materia di dati[190]. A tal fine, ha messo a punto disposizioni specifiche sui flussi di dati e sulla protezione dei dati negli accordi commerciali 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. 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.

Sebbene i dialoghi sulla protezione dei dati e i negoziati commerciali debbano seguire percorsi separati, possono integrarsi a vicenda. In effetti, la convergenza, basata su standard elevati e sostenuta da un'efficace applicazione delle norme, fornisce la base più solida per lo scambio di dati personali, una circostanza questa sempre più riconosciuta dai nostri partner internazionali. Dato che le imprese operano sempre più a livello transfrontaliero e preferiscono applicare insiemi analoghi di norme in tutte le loro attività commerciali a livello mondiale, tale convergenza contribuisce a creare un ambiente favorevole agli investimenti diretti, facilitando gli scambi e migliorando la fiducia tra partner commerciali. 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, nella nostra economia sempre più digitalizzata.

[Accelerare il conseguimento degli obiettivi di sviluppo sostenibile] (disponibile al seguente indirizzo: https://www.africa-eu-partnership.org/sites/default/files/documents/finaldetfreportpdf.pdf).

[190] https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf, pag. 23.

ALLEGATO I – Clausole di specificazione facoltative stabilite dalla legislazione nazionale

Oggetto	Ambito di applicazione	Articoli del regolamento generale sulla protezione dei dati
Specificazioni per gli obblighi giuridici e i compiti di servizio pubblico	Adeguamento dell'applicazione delle disposizioni per quanto riguarda il trattamento per adempiere un obbligo giuridico o un compito di servizio pubblico, anche per situazioni di trattamento specifiche a norma del capo IX	Articolo 6, paragrafi 2 e 3
Limiti di età per il consenso in relazione a servizi della società dell'informazione	Determinazione dell'età minima tra 13 e 16 anni	Articolo 8, paragrafo 1
Trattamenti riguardanti categorie particolari di dati	Mantenimento o introduzione di ulteriori condizioni, comprese limitazioni, per il trattamento di dati genetici, dati biometrici o dati relativi alla salute.	Articolo 9, paragrafo 4
Deroghe alle prescrizioni in materia di informazione	Ottenimento o divulgazione di informazioni espressamente previste dalla legge o per il segreto professionale regolamentato dalla legge	Articolo 14, paragrafo 5, lettere c) e d)
Processo decisionale automatizzato relativo alle persone fisiche	Autorizzazione a svolgere un processo decisionale automatizzato in deroga al divieto generale	Articolo 22, paragrafo 2, lettera b)
Limitazioni dei diritti degli interessati	Limitazioni derivanti dagli articoli da 12 a 22, dall'articolo 34 e corrispondenti disposizioni di cui all'articolo 5, ove necessario e proporzionato per salvaguardare gli obiettivi importanti elencati in modo esaustivo	Articolo 23, paragrafo 1
Requisito di consultazione e autorizzazione	Obbligo per i titolari del trattamento di consultare l'autorità di protezione dei dati o di ottenerne l'autorizzazione per trattamenti per lo svolgimento di un compito di interesse pubblico	Articolo 36, paragrafo 5

Designazione di un responsabile della protezione dei dati in casi aggiuntivi	Designazione di un responsabile della protezione dei dati in casi diversi da quelli di cui all'articolo 37, paragrafo 1	Articolo 37, paragrafo 4
Limitazioni dei trasferimenti	Limitazione dei trasferimenti di categorie particolari di dati personali	Articolo 49, paragrafo 5
Reclami e azioni giudiziarie di organizzazioni a loro titolo	Autorizzazione delle organizzazioni di tutela della vita privata a presentare reclami e azioni giudiziarie indipendentemente da un mandato da parte degli interessati	Articolo 80, paragrafo 2
Accesso ai documenti ufficiali	Conciliazione dell'accesso del pubblico ai documenti ufficiali con il diritto alla protezione dei dati personali	Articolo 86
Trattamento del numero di identificazione nazionale	Condizioni specifiche per il trattamento del numero di identificazione nazionale	Articolo 87
Trattamento dei dati nei rapporti di lavoro	Norme più specifiche per il trattamento dei dati personali dei dipendenti	Articolo 88
Deroghe per trattamenti a fini di archiviazione nel pubblico interesse, di ricerca o a fini statistici	Deroghe a specifici diritti degli interessati nella misura in cui tali diritti rischino di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche	Articolo 89, paragrafi 2 e 3
Conciliazione della protezione dei dati con obblighi di segretezza	Norme specifiche sui poteri investigativi delle autorità di protezione dei dati in relazione ai titolari o ai responsabili del trattamento soggetti ad obblighi di segreto professionale	Articolo 90

ALLEGATO II – Panoramica delle risorse delle autorità di protezione dei dati

La tabella che segue presenta una panoramica delle risorse (in termini di personale e bilancio) delle autorità di protezione dei dati per Stato membro dell'UE/del SEE[191].

Nel confrontare i dati tra gli Stati membri è importante tenere presente che le autorità possono svolgere compiti, assegnati loro, oltre a quelli previsti dal regolamento generale sulla protezione dei dati e che tali compiti possono variare da uno Stato membro all'altro. Il rapporto tra il personale impiegato dalle autorità e un milione di abitanti e il rapporto tra il bilancio delle autorità e un milione di EUR del PIL sono inclusi soltanto per fornire ulteriori elementi di confronto tra Stati membri di dimensioni analoghe e non dovrebbero essere considerati isolatamente. I dati assoluti, i rapporti e l'evoluzione nel corso degli ultimi anni dovrebbero essere considerati congiuntamente nel valutare le risorse di una determinata autorità.

	PERSONALE (equivalenti a tempo pieno)					BILANCIO (EUR)				
Stati membri UE/SEE	**2019**	**Previsioni 2020**	**Crescita % 2016-2019**	**Crescita % 2016-2020 (previsione)**	**Personale per milione di abitanti (2019)**	**2019**	**Previsioni 2020**	**Crescita % 2016-2019**	**Crescita % 2016-2020 (previsione)**	**Bilancio per milione di EUR del PIL (2019)**
Austria	34	34	48 %	48 %	3,8	2 282 000	2 282 000	29 %	29 %	5,7
Belgio	59	65	9 %	20 %	5,2	8 197 400	8 962 200	1 %	10 %	17,3
Bulgaria	60	60	-14 %	-14 %	8,6	1 446 956	1 446 956	24 %	24 %	23,8
Croazia	39	60	39 %	114 %	9,6	1 157 300	1 405 000	57 %	91 %	21,5
Cipro	24	22	NA	NA	27,4	503 855	NA	114 %	NA	23,0
Repubblica ceca	101	109	0 %	8 %	9,5 %	6 541 288	6 720 533	10 %	13 %	29,7
Danimarca	66	63	106 %	97 %	11,4	5 610 128	5 623 114	101 %	101 %	18,0
Estonia	16	18	-11 %	0 %	12,1	750 331	750 331	7 %	7 %	26,8
Finlandia	45	55	114 %	162 %	8,2	3 500 000	4 500 000	94 %	150 %	14,6
Francia	215	225	9 %	14 %	3,2	18 506 734	20 143 889	-2 %	7 %	7,7
Germania	888	1 002	52 %	72 %	10,7	76 599 800	85 837 500	48 %	66 %	22,3
Grecia	33	46	-15 %	18 %	3,1	2 849 000	3 101 000	38 %	50 %	15,2
Ungheria	104	117	42 %	60 %	10,6	3 505 152	4 437 576	102 %	155 %	24,4
Islanda	17	17	143 %	143 %	47,6	2 272 490	2 294 104	167 %	170 %	105,2
Irlanda	140	176	169 %	238 %	28,5	15 200 000	16 900 000	223 %	260 %	43,8
Italia	170	170	40 %	40 %	2,8	29 127 273	30 127 273	46 %	51 %	16,3
Lettonia	19	31	-10 %	48 %	9,9	640 998	1 218 978	4 %	98 %	21,0
Lituania	46	52	-8 %	4 %	16,5	1 482 000	1 581 000	40 %	49 %	30,6
Lussemburgo	43	48	126 %	153 %	70,0	5 442 416	6 691 563	165 %	226 %	85,7
Malta	13	15	30 %	50 %	26,3	480 000	550 000	41 %	62 %	36,3
Paesi Bassi	179	188	145 %	158 %	10,4	18 600 000	18 600 000	130 %	130 %	22,9
Norvegia	49	58	2 %	21 %	9,2	5 708 950	6 580 660	27 %	46 %	15,9
Polonia	238	260	54 %	68 %	6,3	7 506 345	9 413 381	66 %	108 %	14,2
Portogallo	25	27	-4 %	4 %	2,4	2 152 000	2 385 000	67 %	86 %	10,1
Romania	39	47	-3 %	18 %	2,0	1 103 388	1 304 813	3 %	22 %	4,9
Slovacchia	49	51	20 %	24 %	9,0	1 731 419	1 859 514	47 %	58 %	18,4
Slovenia	47	49	42 %	48 %	22,6	2 242 236	2 266 485	68 %	70 %	46,7

[191] Fatta eccezione per il Liechtenstein.

Spagna	170	220	13 %	47 %	3,6	15 187 680	16 500 000	8 %	17 %	12,2
Svezia	87	87	81 %	81 %	8,5	8 800 000	10 300 000	96 %	129 %	18,5
TOTALE	**2 966**	**3 372**	**42 %**	**62 %**	**6,6**	**249 127 139**	**273 782 870**	**49 %**	**64 %**	**17,4**

Origine dei dati grezzi: contributo del comitato. Calcoli della Commissione.