COMMISSIONE
EUROPEA

Bruxelles, 25.7.2022
COM(2022) 364 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Prima relazione sull'applicazione e sul funzionamento della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie ("LED")

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Prima relazione sull'applicazione e sul funzionamento della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie ("LED")

Indice

1 LA LED COME STRUMENTO PRINCIPALE PER GARANTIRE LA PROTEZIONE DEI DATI NELLA POLITICA DI SICUREZZA DELL'UNIONE EUROPEA

La presente comunicazione costituisce la prima relazione della Commissione europea di valutazione e sul riesame della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giudiziarie[1] ("LED", dall'inglese Data Protection Law Enforcement Directive), ai sensi dell'articolo 62, paragrafo 1, della medesima direttiva.

In particolare, la presente relazione esamina, l'applicazione e il funzionamento delle norme di cui alla LED in materia di trasferimento di dati personali verso paesi terzi e organizzazioni internazionali come richiesto da tale direttiva, ma adotta anche un approccio di più ampio respiro. Colloca la LED nel quadro del diritto dell'Unione in materia di protezione dei dati personali e del diritto dell'Unione che disciplina il trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati ed esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica ("attività di contrasto in materia penale")[2]. La presente relazione fornisce una panoramica del recepimento della LED nelle rispettive legislazioni nazionali da parte degli Stati membri, presenta i primi insegnamenti tratti dall'applicazione e dal funzionamento di tale direttiva e delinea le azioni da intraprendere in futuro.

1.1 Un elemento fondamentale di un quadro coerente per la protezione dei dati dell'Unione europea

La LED costituisce uno dei tre pilastri del quadro dell'UE che garantisce il diritto fondamentale alla protezione dei dati personali. Gli altri due sono il regolamento generale sulla protezione dei dati ("GDPR")[3] e il regolamento sulla protezione dei dati da parte delle istituzioni, degli organi e degli organismi dell'Unione ("EUDPR")[4]. Il diritto fondamentale alla protezione dei dati è sancito dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea ("la Carta")[5] e dall'articolo 16 del trattato sul funzionamento dell'Unione europea ("TFUE")[6].

---

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

[2] Articolo 1, paragrafo 1, LED.

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

[4] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

[5] Carta dei diritti fondamentali dell'Unione europea (GU C 202 del 7.6.2016, pag. 389).

[6] Trattato sul funzionamento dell'Unione europea (versione consolidata) (GU C 202 del 7.6.2016, pag. 47).

La LED è entrata in vigore il 6 maggio 2016 e gli Stati membri erano tenuti a recepirla entro il 6 maggio 2018[7].

La LED è il primo atto legislativo dell'Unione che adotta un approccio globale alla protezione dei dati personali da parte delle autorità competenti (ossia autorità giudiziarie, forze di polizia e altre autorità di contrasto in materia penale come previsto dall'articolo 3, punto 7, LED) per finalità di contrasto in materia penale. Rispetto alla decisione quadro 2008/977/GAI del Consiglio[8], che ha abrogato e sostituito, la LED rappresenta un importante passo avanti nel garantire l'applicazione coerente delle norme in materia di protezione dei dati in tutta l'UE. Innanzitutto, la LED fornisce una serie completa di norme per il trattamento di dati personali a livello tanto transfrontaliero quanto nazionale per finalità di contrasto in materia penale, mentre la decisione quadro del Consiglio riguardava soltanto il trattamento a livello transfrontaliero. In secondo luogo, la LED fornisce un insieme completo e orizzontale di norme, mentre nell'approccio precedente ogni atto settoriale dell'UE che prevedeva il trattamento dei dati personali nel contesto delle attività di contrasto in materia penale era disciplinato dalle proprie norme concernenti la protezione dei dati[9].

Il GDPR, l'EUDPR e la LED si basano su concetti e principi analoghi[10], una circostanza questa che determina un'interpretazione e un'applicazione coerenti delle norme dell'UE in materia di protezione dei dati. Condividono definizioni comuni e contengono obblighi analoghi per i titolari e i responsabili del trattamento. Tuttavia la LED affronta in modo specifico anche i rischi legati al trattamento di dati personali nel contesto delle attività di contrasto in materia penale. Tra le disposizioni corrispondenti figurano l'obbligo di: i) distinguere tra diverse categorie di interessati; ii) distinguere tra dati personali fondati su fatti e dati fondati su una valutazione personale; iii) tenere registrazioni sull'uso dei dati personali e rispettare prescrizioni specifiche in materia di sicurezza[11].

Data la specificità della cooperazione giudiziaria in materia penale e della cooperazione di polizia, si è ritenuto necessario adottare norme specifiche in tali ambiti per la protezione dei dati personali e la libera circolazione dei dati personali[12]. Il carattere sensibile del settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, associato alla complessità dei quadri giuridici nazionali che disciplinano le attività di contrasto in materia penale, ha fatto sì che una direttiva fosse considerata lo strumento migliore per conseguire un livello elevato di protezione

[7] Articolo 63, paragrafo 1, LED.
[8] Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (GU L 350 del 30.12.2008, pag. 60).
[9] Ad esempio gli atti giuridici che disciplinano il sistema d'informazione Schengen e altri atti dell'*acquis* di Schengen contenevano disposizioni specifiche che disciplinavano questioni quali i diritti degli interessati.
[10] Tra questi figurano: liceità e correttezza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza; e responsabilizzazione (articolo 4 LED).
[11] Rispettivamente articolo 6, 7, 25 e 29 LED.
[12] Cfr. dichiarazione n. 21, relativa alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, allegata all'atto finale della conferenza intergovernativa che ha adottato il trattato di Lisbona (GU C 115 del 9.5.2008, pag. 335).

dei dati in questo settore. Una direttiva lascia inoltre agli Stati membri la necessaria flessibilità nell'attuazione dei principi, delle norme e delle deroghe a livello nazionale[13].

La Commissione ha pubblicato la sua prima relazione sull'attuazione del GDPR il 24 giugno 2020[14]. In tale documento ha concluso che l'opinione generale era che il GDPR aveva conseguito i suoi obiettivi, in particolare fornendo ai cittadini una solida serie di diritti azionabili e creando un nuovo sistema di governance e di applicazione nell'UE. Tale relazione ha definito un elenco di azioni da intraprendere per facilitare ulteriormente l'applicazione del GDPR da parte di tutti i portatori di interessi e per promuovere e sviluppare ulteriormente una cultura in materia di protezione dei dati nell'UE, unitamente a un'applicazione vigorosa della legislazione.

La presente relazione fa seguito al riesame degli atti giuridici adottati dall'UE che disciplinano il trattamento dei dati da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. Tale riesame mirava a valutare la necessità di allineare gli atti giuridici in questione rispetto alla LED[15]. Il 24 giugno 2020 la Commissione ha adempiuto tale obbligo adottando una comunicazione dal titolo "Via da seguire per allineare l'acquis dell'ex terzo pilastro alle norme sulla protezione dei dati"[16]. Ha individuato 10 atti giuridici che dovrebbero essere allineati rispetto alla LED e ha stabilito un calendario per tale attività.

La presente relazione è stata infine preparata parallelamente alla relazione della Commissione sull'applicazione dell'EUDPR. Un elemento importante di quest'ultima è il riesame delle sue norme, di cui al capo IX, sul trattamento dei dati personali operativi da parte di organi o organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della cooperazione di polizia e della cooperazione giudiziaria in materia penale[17] ("agenzie GAI"). Le norme in questione si basano in gran parte sulla LED. L'articolo 98 dell'EUDPR impone alla Commissione di riesaminare gli atti giuridici che disciplinano il trattamento dei dati personali operativi da parte delle agenzie GAI e le consente di presentare proposte legislative adeguate a Europol, in

[13] Relazione di cui alla proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati (COM(2012) 10 final), 25 gennaio 2012.
[14] 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), 24 giugno 2020.
[15] L'articolo 62, paragrafo 6, LED prevedeva che, entro il 6 maggio 2019, la Commissione riesaminasse gli altri atti giuridici dell'UE che disciplinano il trattamento dei dati personali per finalità di contrasto, al fine di valutare la necessità di allinearli alla LED e formulasse, ove opportuno, le proposte necessarie per modificarli in modo da garantire un approccio coerente alla protezione dei dati personali nell'ambito della medesima direttiva.
[16] Comunicazione della Commissione al Parlamento europeo e al Consiglio, Via da seguire per allineare l'acquis dell'ex terzo pilastro alle norme sulla protezione dei dati (COM(2020) 262 final), 24 giugno 2020.
[17] Parte terza, titolo V, capo 4 o capo 5, TFUE.

particolare ai fini dell'applicazione delle norme di cui al capo IX[18], e alla Procura europea, nonché di proporre eventuali modifiche a tale capo IX.

1.2 Un contributo essenziale alla garanzia di una solida politica di sicurezza all'interno dell'Unione europea

La Commissione ha sottolineato costantemente che un'UE efficace e veramente sicura può essere costruita soltanto sulla base del pieno rispetto dei diritti fondamentali sanciti dalla Carta e dal diritto derivato dell'UE. La LED fornisce un contributo fondamentale alla politica di sicurezza dell'UE, garantendo che i dati personali di vittime, testimoni e indiziati di reati siano debitamente protetti. Inoltre, armonizzando le norme in materia di protezione dei dati personali trattati dalle autorità competenti nell'UE e nei paesi dell'area Schengen, la LED contribuisce a rafforzare la fiducia e la sicurezza dei dati scambiati tra le autorità per finalità di contrasto in materia penale, facilitando così la cooperazione transfrontaliera nella lotta alla criminalità e al terrorismo[19]. La LED svolge altresì un ruolo chiave nella promozione di una cultura del rispetto della protezione dei dati tra le autorità competenti.

La strategia per l'Unione della sicurezza[20] sottolinea inoltre che le nuove tecnologie quali l'intelligenza artificiale potrebbero essere utilizzate come un potente strumento per combattere la criminalità. Realizzare tale potenziale significa altresì garantire i livelli più elevati di rispetto dei diritti fondamentali. La legislazione in materia di protezione dei dati, compresa la LED, fornisce la base su cui costruire la legislazione settoriale. Ad esempio, la proposta di legge sull'intelligenza artificiale[21] inquadrerebbe ulteriormente l'uso dei dati personali per l'identificazione biometrica remota in luoghi pubblici per finalità di contrasto.

Infine, in un mondo interconnesso, la criminalità (e in particolare la cibercriminalità informatica e altri reati favoriti dalla cibernetica) presenta sempre più un carattere transfrontaliero. Anche durante le indagini su casi nazionali, le autorità competenti si trovano sempre più spesso in situazioni transfrontaliere dato che le informazioni sono archiviate elettronicamente in un paese terzo. Ciò accresce la necessità di una cooperazione internazionale nelle indagini penali, tanto da parte delle autorità degli Stati membri quanto da parte di organismi dell'UE quali Europol ed Eurojust. Tale cooperazione, e in particolare la raccolta e lo scambio di prove elettroniche[22],

---

[18] Tale questione è già stata affrontata dalla proposta della Commissione del 2020 sulla modifica del regolamento Europol.

[19] Comunicazione della Commissione al Parlamento europeo e al Consiglio, Prima relazione sui progressi compiuti nella strategia dell'UE per l'Unione della sicurezza (COM(2020) 797 final), 9 dicembre 2020.

[20] Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla strategia dell'UE per l'Unione della sicurezza (COM(2020) 605 final), 24 luglio 2020.

[21] Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione (COM(2021) 206 final), 21 aprile 2021.

[22] Le informazioni e le prove elettroniche sono necessarie per circa l'85 % delle indagini relative a reati gravi, e il 65 % del numero totale di richieste è rivolto a prestatori con sede in un'altra giurisdizione. Cfr. documento di lavoro dei

comporta spesso il trasferimento di dati personali. Sono quindi essenziali garanzie forti in materia di protezione dei dati. Tali garanzie contribuiscono altresì a rafforzare la fiducia tra le autorità di contrasto, garantendo uno scambio di informazioni più rapido ed efficace e rafforzando la certezza del diritto quando le informazioni vengono poi utilizzate nei procedimenti penali. A tale proposito, la LED fornisce una serie aggiornata di strumenti per facilitare tali trasferimenti di dati personali dall'UE a un paese terzo o a un'organizzazione internazionale (ad esempio Interpol[23]), garantendo nel contempo che i dati personali continuino a beneficiare di un livello elevato di protezione. La Commissione e gli Stati membri hanno utilizzato l'intera gamma degli strumenti della LED sin dalla sua entrata in vigore, confermando così che tale atto dispone di un ambito di applicazione sufficientemente ampio ed è sufficientemente flessibile da rendere possibile una cooperazione giudiziaria e di polizia efficace a livello internazionale.

1.3 Considerazioni importanti in merito alla preparazione della relazione

Durante la redazione della presente relazione, la Commissione ha raccolto informazioni e riscontri da svariate fonti e mediante diverse attività di consultazione mirate. Oltre all'articolo 62 LED, la Commissione ha tenuto conto dei contributi e delle posizioni del Parlamento europeo[24], del Consiglio[25], del Comitato europeo per la protezione dei dati ("EDPB")[26] e delle autorità nazionali di controllo della protezione dei dati. Ulteriori riscontri sono stati ottenuti attraverso un questionario destinato a organizzazioni della società civile (attraverso l'Agenzia dell'Unione europea per i diritti fondamentali)[27] e dalle risposte a un invito pubblico a presentare contributi[28]. La Commissione ha preso altresì in considerazione le osservazioni del gruppo di esperti degli Stati

servizi della Commissione SWD(2018) 118 final (valutazione d'impatto che accompagna il documento proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale e 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).

[23] Cfr. anche il considerando 25 LED.

[24] Contributo della commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo all'imminente relazione della Commissione europea sulla valutazione e sul riesame della LED, del 7 febbraio 2022.

[25] Posizione e conclusioni del Consiglio in merito all'applicazione della LED (documento del Consiglio 13943/21 del 18 novembre 2021 https://data.consilium.europa.eu/doc/document/ST-13943-2021-INIT/it/pdf).

[26] Contributo dell'EDPB alla valutazione della LED da parte della Commissione europea ai sensi dell'articolo 62 LED, adottato il 14 dicembre 2021 ("contributo dell'EDPB alla valutazione della LED") (non disponibile in IT) - https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf.

[27] Delle 804 organizzazioni della società civile contattate dall'Agenzia dell'Unione europea per i diritti fondamentali (FRA), 88 hanno fornito una risposta. Tuttavia, solo 17 dei *contributi hanno potuto essere presi in considerazione in quanto 61 contributi non erano correlati alla LED* o indicavano che l'organizzazione interessata non si occupava di protezione dei diritti fondamentali nel settore delle attività di contrasto in materia penale o *non aveva* affatto familiarità con la LED.

[28] Invito a presentare contributi, Protezione dei dati nelle attività di polizia e giudiziarie - relazione sulla direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, 24 gennaio 2022 - https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13288-Protezione-dei-dati-nelle-attivita-di-contrasto-relazione-sulla-direttiva-sulle-attivita-di-contrasto_it

membri sul GDPR e sulla LED[29] così come le osservazioni della presidenza tedesca del Consiglio[30]. Ha inoltre tenuto conto dell'analisi delle misure nazionali di recepimento e di un numero esiguo di denunce ricevute al riguardo.

Sebbene la LED si applichi a tutti gli Stati membri e a tutti i paesi dell'area Schengen (dato che costituisce uno sviluppo dell'*acquis* di Schengen[31]), la presente relazione riguarda soltanto gli Stati membri dell'UE.

Tre fattori hanno influito sulla preparazione della presente relazione. Innanzitutto due terzi degli Stati membri non hanno rispettato il termine del maggio del 2018 per recepire la LED nel diritto nazionale. Ciò nonostante la maggior parte degli Stati membri ha recepito tale direttiva entro il 2019 dopo che la Commissione aveva avviato procedure di infrazione. Di conseguenza l'esperienza sulla sua applicazione è piuttosto limitata, un aspetto sottolineato anche dall'EDPB[32] e dal Consiglio[33]. In secondo luogo, si è rivelato più difficile compilare statistiche sull'applicazione della LED, rispetto al GDPR. Alcune autorità di controllo della protezione dei dati non raccolgono statistiche sulle loro attività di controllo in modo distinto per la LED e il GDPR. Ciò si verifica ad esempio in relazione alle notifiche di violazione dei dati[34] e ai reclami presentati ai sensi della LED[35] e, a volte, tale circostanza rende difficile ottenere una panoramica accurata di tali disposizioni ai sensi della LED[36].

In terzo luogo, è importante considerare che la giurisprudenza sta iniziando soltanto ora a svilupparsi in merito all'applicazione della LED. Numerosi procedimenti sono attualmente pendenti dinanzi alla Corte di giustizia dell'Unione europea ("la Corte") in merito all'interpretazione di disposizioni chiave della LED quali il diritto di accesso degli interessati e il diritto a un ricorso giurisdizionale effettivo. Tali sentenze forniranno maggiore chiarezza e contribuiranno a un approccio più armonizzato tra gli Stati membri.

---

[29] Gruppo di esperti della Commissione sul regolamento (UE) 2016/679 e sulla direttiva (UE) 2016/680 (E03461) - https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=3461&lang=it.

[30] Relazione della presidenza del Consiglio dell'Unione europea sullo scambio di dati di polizia con paesi terzi - esperienze nell'applicazione dell'articolo 37 della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, dicembre 2020.

[31] Cfr. considerando da 101 a 103 LED.

[32] Contributo dell'EDPB alla valutazione della LED, punto 4.

[33] Posizione e conclusioni del Consiglio in merito all'applicazione della LED, punto 7.

[34] Ad esempio le autorità in Danimarca, Lituania, Norvegia, Austria e numerose autorità in Germania non tengono statistiche separate sulle violazioni dei dati ai sensi della LED. Sei autorità hanno riferito altresì di non aver ricevuto notifiche di violazioni ai sensi della LED.

[35] Ad esempio le autorità in Danimarca e Austria e numerose autorità in Germania non tengono statistiche separate per i reclami ai sensi della LED.

[36] Contributo dell'EDPB alla valutazione della LED, punto 43.

2 UN RECEPIMENTO SODDISFACENTE, SEBBENE PERSISTANO ALCUNE QUESTIONI IN SOSPESO

La Commissione ha istituito un gruppo di esperti degli Stati membri[37] per aiutare gli Stati membri a integrare la LED nel loro rispettivo diritto nazionale. Tale gruppo facilita le discussioni e la condivisione di esperienze tra gli Stati membri e la Commissione per quanto concerne le norme in materia di protezione dei dati. Si è riunito regolarmente tra l'adozione della LED nel 2016 e il termine di recepimento del maggio del 2018 e i suoi lavori sono ripresi nel 2021.

La panoramica concernente il recepimento presentata di seguito si concentra sulle questioni principali individuate finora. Si basa principalmente sull'analisi della Commissione delle informazioni fornite dagli Stati membri al momento della notifica alla Commissione delle misure nazionali adottate per recepire la LED nel loro diritto nazionale. Tale analisi è stata sostenuta da uno studio esterno condotto da un contraente esterno. La Commissione ha inoltre intrapreso scambi bilaterali con diversi Stati membri.

2.1 Un recepimento completo nel complesso, ma con alcune criticità in relazione a disposizioni specifiche

Nel luglio del 2018 la Commissione ha avviato procedure di infrazione contro 19 Stati membri che non avevano adottato leggi di recepimento della LED entro il termine fissato per maggio del 2018 e non avevano debitamente notificato alla Commissione il recepimento da parte loro. Un'ulteriore procedura di mancato recepimento parziale è stata avviata nel luglio del 2019 nei confronti di un altro Stato membro. Di conseguenza la maggior parte degli Stati membri ha successivamente notificato alla Commissione la propria legislazione nazionale di recepimento e nel 2019 quest'ultima ha progressivamente chiuso le procedure di infrazione nei loro confronti (nel 2020 per uno Stato membro). Nel 2021 la Commissione ha deferito alla Corte la sua azione di infrazione contro la Spagna perché quest'ultima non aveva ancora recepito la LED e non aveva notificato alla Commissione le sue misure di recepimento. Data la gravità e la durata dell'infrazione, la Corte, per la prima volta, ha imposto alla Spagna il versamento tanto di una somma forfettaria quanto di una sanzione pecuniaria[38].

Nell'aprile del 2022 la Commissione ha avviato altresì una procedura di infrazione nei confronti della Germania dopo aver rilevato una lacuna nel recepimento della LED in relazione alle attività della polizia federale tedesca.

La Commissione continuerà a valutare il recepimento della LED negli Stati membri e adotterà le misure necessarie per porre rimedio a eventuali lacune.

2.2 Priorità per la valutazione della conformità

La Commissione sta inoltre verificando che le disposizioni nazionali degli Stati membri abbiano recepito correttamente le prescrizioni della LED (verifica di conformità).

---

[37] Cfr. nota 29.

[38] Sentenza della Corte di giustizia del 25 febbraio 2021, *Commissione europea/Regno di Spagna*, C-658/19, ECLI:EU:C:2017:548.

Al momento del recepimento della LED, gli Stati membri hanno modificato la loro legislazione precedente in materia di protezione dei dati o l'hanno abrogata e sostituita con uno o più atti nuovi orizzontali in materia di protezione dei dati. In numerosi casi, le legislazioni nazionali recepiscono la LED facendo riferimento alla medesima disposizione o a una disposizione equivalente del GDPR (ad esempio per quanto riguarda definizioni, notifiche di violazioni dei dati, nomina del responsabile della protezione dei dati e disposizioni concernenti l'organizzazione, lo status, le competenze, i compiti e i poteri delle autorità nazionali di controllo della protezione dei dati). Diverse disposizioni della LED sono state recepite altresì attraverso disposizioni nuove ad esempio nel contesto del diritto amministrativo generale, del diritto procedurale amministrativo o della procedura penale. Taluni Stati membri hanno altresì recepito alcune disposizioni della LED nella legislazione settoriale che disciplina il funzionamento e i poteri di autorità competenti specifiche. Potrebbe essere pertanto necessario prendere in considerazione una serie di atti giuridici nazionali per stabilire se la LED sia stata recepita correttamente o meno in un determinato Stato membro. Nel complesso le leggi nazionali rispecchiano ampiamente i principi e le disposizioni fondamentali della LED. Tuttavia sono state individuate una serie di questioni, le più importanti delle quali sono illustrate nelle sezioni che seguono. La Commissione ha già avviato una serie di procedure di infrazione nei confronti di Stati membri[39]. Il processo di riesame è sempre in corso e la Commissione continuerà a utilizzare tutti gli strumenti disponibili, comprese le infrazioni, quando una misura nazionale di recepimento non risulta essere conforme alla LED.

La giurisprudenza in materia di LED è ancora agli albori. La Corte ha iniziato a emettere sentenze sull'interpretazione della direttiva, ad esempio nelle cause *WS/Bundesrepublik Deutschland*[40] e *B/Latvijas Republikas Saeima*[41]. Al momento della stesura della presente relazione, sono pendenti dinanzi alla Corte alcune pronunce pregiudiziali (come indicato nelle sezioni che seguono).

---

[39] Nell'aprile del 2022 la Commissione ha avviato procedure di infrazione nei confronti di Grecia, Finlandia e Svezia in quanto le loro leggi nazionali di recepimento non sono conformi alla LED. La causa contro la Grecia riguarda *una serie di punti, tra cui*, tra l'altro, la non applicazione del diritto nazionale di recepimento della LED al trattamento di dati personali da parte delle autorità giudiziarie e di quelle preposte all'esercizio dell'azione penale nonché da parte delle autorità che agiscono sotto la loro supervisione per la maggior parte dei reati; il recepimento delle disposizioni in materia di conservazione dei dati ed esame (articolo 5); la base giuridica per il trattamento dei dati (articolo 8); nonché garanzie nel contesto del processo decisionale automatizzato (articolo 11). Le procedure di infrazione nei confronti di Finlandia e Svezia sono state avviate perché le loro leggi non forniscono agli interessati accesso a un ricorso effettivo dinanzi a un organo giurisdizionale. La Commissione ha avviato una procedura di infrazione nei confronti della Germania nel maggio del 2022 perché diverse leggi nazionali di recepimento della LED non forniscono poteri correttivi effettivi a livello federale e di Land.

[40] Sentenza della Corte di giustizia del 12 maggio 2021, *WS/Bundesrepublik Deutschland*, C-505/19, ECLI:EU:C:2021:376. Questa causa riguardava, tra l'altro, la liceità del trattamento di dati personali (articolo 4, paragrafo 1, lettera a), e articolo 8 LED) nel contesto specifico di un avviso rosso emesso dall'Interpol. La Corte di giustizia dell'Unione europea non ha precluso la liceità del trattamento di dati personali che figurano in un avviso rosso emesso dall'Interpol fino a quando non sia stato stabilito mediante una decisione giudiziaria definitiva che il principio del *ne bis in idem* si applica agli atti su cui si basa tale avviso.

[41] Sentenza della Corte di giustizia del 22 giugno 2021, *B/Latvijas Republikas Saeima*, C-439/19, ECLI:EU:C:2021:504. La Corte di giustizia dell'Unione europea ha interpretato la definizione di autorità competente di cui all'articolo 3, paragrafo 7, e la nozione di reato. Cfr. anche la sezione che segue.

2.2.1 Ambito di applicazione della LED

La difficoltà di delimitare l'ambito di applicazione della LED rispetto a quello del GDPR è stata sollevata come motivo di preoccupazione tanto dal gruppo di esperti degli Stati membri sul GDPR e sulla LED[42], quanto dall'EDPB[43]. Alcune autorità di controllo della protezione dei dati hanno rilevato altresì che le autorità competenti possono incontrare difficoltà a tale riguardo[44].

L'ambito di applicazione della LED è definito[45] da due elementi fondamentali: la nozione di autorità competente (ambito di applicazione soggettivo) e la nozione di reato (ambito di applicazione materiale).

Per quanto concerne l'ambito di applicazione soggettivo, il trattamento dei dati è soggetto alla LED quando innanzitutto è svolto da un'autorità competente e, in secondo luogo, quando i dati personali sono trattati per finalità di cui alla LED[46] (ossia prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica). Secondo la Commissione, le "autorità competenti" quali definite dalla LED[47] sono organi dello Stato od organismi privati, ai quali la legge conferisce poteri speciali oltre a quelli risultanti dalle normali norme applicabili nei rapporti tra persone fisiche e/o dalla possibilità di esercitare il potere di coercizione. Tali autorità sono autorità competenti ai sensi della LED quando (anche se soltanto sporadicamente e/o in casi isolati) trattano dati per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica). Ciò significa ad esempio che il trattamento da parte di tali organismi di dati personali per finalità non legate alla LED (ad esempio risorse umane o altre finalità amministrative quali il trattamento di dati personali da parte delle unità di informazione finanziaria (FIU) ai sensi dell'*acquis*[48] in materia di antiriciclaggio) rientra nell'ambito di applicazione del GDPR e non della LED.

La nozione di "reato" è di fondamentale importanza ai fini della determinazione dell'eventualità che il trattamento dei dati rientri o meno nell'ambito di applicazione della LED. Secondo la Corte, tre criteri sono rilevanti per valutare la natura penale di un illecito: l'eventualità o meno che l'illecito sia qualificato come penale ai sensi del diritto nazionale; la natura intrinseca dell'illecito

---

[42] Cfr. verbale della riunione del gruppo di esperti della Commissione sul regolamento (UE) 2016/679 e sulla direttiva (UE) 2016/680 del 5 maggio 2021 - https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=it&meetingId=25283&fromExpertGroups=true.
[43] Contributo dell'EDPB alla valutazione della LED, punto 7.
[44] Le autorità di controllo della protezione dei dati di Irlanda, Francia e Ungheria hanno sollevato tale preoccupazione.
[45] Articolo 2, paragrafo 1, e considerando da 12 a 14 LED.
[46] Articolo 1 LED.
[47] Articolo 3, punto 7, LED.
[48] L'articolo 41 della direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione, che disciplina il funzionamento delle unità di informazione finanziaria, stabilisce esplicitamente che il trattamento di dati personali ai sensi di tale direttiva è soggetto all'applicazione del regolamento (UE) 2016/679.

e il grado di severità della sanzione in cui l'interessato rischia di incorrere[49]. Il carattere autonomo della nozione di reato di cui al considerando 13 LED implica, tra l'altro, che il diritto dello Stato membro non possa determinare la natura di un illecito come "penale" ai soli fini dell'applicazione della LED.

La questione concernente la delimitazione tra gli ambiti di applicazione del GDPR e della LED si pone in alcuni Stati membri per quanto concerne la delimitazione tra l'ambito dei reati e quello degli illeciti amministrativi. In particolare alcune leggi nazionali di recepimento fanno riferimento a finalità di trattamento dei dati personali non elencate nell'articolo 1 LED (ad esempio minacce all'ordine pubblico o alla sicurezza pubblica). La questione si pone altresì in considerazione del fatto che alcuni Stati membri ritengono che un certo numero di organi amministrativi (ad esempio le FIU, di cui sopra) svolgano compiti che rientrano nell'ambito di applicazione della LED.

La maggior parte delle leggi degli Stati membri contempla in modo completo qualsiasi autorità competente per il trattamento di dati ai fini della LED. Al contrario, alcuni Stati membri hanno scelto di enumerare in modo esauriente le autorità competenti ai sensi della LED nella loro legislazione nazionale. Alcuni Stati membri hanno inoltre previsto una deroga per il trattamento da parte di determinati tipi di autorità competenti o di determinati tipi di dati.

La questione dell'ambito di applicazione della LED è oggetto di un rinvio pregiudiziale dinanzi alla Corte. L'organo giurisdizionale *Landesverwaltungsgericht Tirol* (Austria) ha sollevato la questione dell'ambito di applicazione della LED quando un'autorità competente ha tentato senza successo di accedere ai dati presenti su un telefono sequestrato (interpretazione dell'articolo 2 LED). Questa causa riguarda altresì le condizioni di tale accesso[50].

2.2.2 Governance e poteri delle autorità di controllo della protezione dei dati

Tutti gli Stati membri tranne due (Belgio e Svezia) hanno affidato l'applicazione della LED all'autorità di controllo competente anche dell'applicazione del GDPR. Il Belgio ha affidato il controllo sulle forze di polizia ai fini della LED a un'autorità di controllo distinta. In Svezia il controllo di alcune autorità competenti, comprese le forze di polizia, è condiviso dall'autorità di controllo competente per il GDPR e da un'altra autorità di controllo. Inoltre, ai sensi della LED, tutte le autorità di controllo della protezione dei dati non sono competenti per esercitare un controllo sugli organi giurisdizionali quando questi ultimi esercitano le loro funzioni giurisdizionali.

Per quanto concerne le disposizioni della LED in materia di indipendenza delle autorità di controllo della protezione dei dati[51], tutti gli Stati membri hanno previsto nella loro legislazione di recepimento che le autorità di controllo della protezione dei dati agiscano in modo indipendente nello svolgimento dei loro compiti. Richiedono inoltre che i membri delle loro autorità di controllo

[49] Sentenza della Corte di giustizia del 22 giugno 2021, *B/Latvijas Republikas Saeima*, C-439/19, ECLI:EU:C:2021: 504, punto 87.
[50] Domanda di pronuncia pregiudiziale nella causa *C.G./Bezirkshauptmannschaft Landeck*, C-548/21.
[51] Capo VI, sezione 1, LED.

della protezione dei dati non subiscano pressioni esterne e non sollecitino né accettino istruzioni da alcuno.

Il controllo della conformità da parte delle autorità di controllo della protezione dei dati è fondamentale e sancito dall'articolo 8, paragrafo 3, della Carta. La LED impone agli Stati membri di conferire alle autorità di controllo della protezione dei dati poteri d'indagine, correttivi e consultivi, che devono essere effettivi. Si tratta di un presupposto per la corretta applicazione delle norme in materia di protezione dei dati e, di conseguenza, per il conseguimento dell'obiettivo della LED di un livello elevato di protezione dei diritti fondamentali, in particolare per quanto concerne il diritto alla protezione dei dati personali, nonché per la garanzia della libera circolazione dei dati all'interno dell'UE. Le autorità di controllo della protezione dei dati devono disporre di poteri equivalenti in tutta l'UE, affinché possano svolgere i propri compiti come richiesto dalla LED[52].

Tutti gli Stati membri hanno conferito alle proprie autorità i poteri d'indagine specificati nella LED e la maggioranza di loro ha conferito loro altresì altri poteri (ad esempio per condurre attività di controllo, accedere a locali, effettuare copie di dati e sequestrare oggetti[53]). Di conseguenza quasi tutte le autorità di controllo della protezione dei dati hanno ritenuto di disporre di poteri d'indagine effettivi.

Quasi tutti gli Stati membri hanno previsto i poteri correttivi specificati nella LED[54]. Molti di loro hanno conseguito tale obiettivo attenendosi strettamente alla formulazione della LED, mentre molti altri hanno utilizzato una formulazione molto ampia che potrebbe essere ragionevolmente interpretata comprendere tutti i poteri di cui alla LED.

Inoltre la maggior parte delle leggi degli Stati membri conferisce alle autorità di controllo della protezione dei dati il potere di irrogare sanzioni amministrative pecuniarie[55].

Non tutti gli Stati membri hanno conferito alle proprie autorità di controllo della protezione dei dati il potere di portare all'attenzione delle autorità giudiziarie eventuali violazioni delle leggi nazionali adottate per recepire la LED e quello di avviare o di promuovere in altro modo procedimenti giudiziari. Tale potere è importante e integra gli altri mezzi a disposizione delle autorità di controllo della protezione dei dati destinati a garantire efficacemente un livello elevato

---

[52] Cfr. considerando 7 e 82 LED.

[53] Cfr. anche punto 23 del contributo dell'EDPB alla valutazione della LED: 24 Stati membri hanno previsto il potere di ottenere l'accesso a qualsiasi locale del titolare e del responsabile del trattamento, nonché a qualsiasi attrezzatura e mezzo di trattamento dei dati; 21 Stati membri hanno previsto un processo di controllo e 9 Stati membri hanno previsto altri poteri (ad esempio sequestro di oggetti, richiesta di audizione dinanzi all'autorità di controllo della protezione dei dati e richiesta di assistenza esecutiva alle forze di polizia).

[54] Articolo 47, paragrafo 2, lettere da a) a c), LED.

[55] 18 Stati membri hanno previsto tale possibilità: Bulgaria, Cechia, Estonia, Grecia, Croazia, Italia, Cipro, Lettonia, Lituania, Lussemburgo, Ungheria, Malta, Paesi Bassi, Austria, Portogallo, Romania, Slovacchia e Svezia. Le autorità di controllo della protezione dei dati in tre Stati membri (Estonia, Lettonia e Austria) possono irrogare sanzioni pecuniarie a persone fisiche (ad esempio dipendenti) o a soggetti privati (ad esempio soggetti privati che agiscono in veste di responsabili del trattamento dei dati).

di protezione dei diritti fondamentali delle persone fisiche e in particolare del loro diritto alla protezione dei loro dati personali.

2.2.3 Ricorsi

Tutti gli Stati membri hanno previsto il diritto di proporre reclamo presso la propria autorità di controllo pertinente[56]. La maggior parte delle legislazioni nazionali fissa un termine per la presentazione di tale reclamo. È importante che tale termine non ostacoli il diritto degli interessati a tale riguardo.

In linea con la LED[57], tutti gli Stati membri dispongono la possibilità di promuovere un ricorso giurisdizionale nei confronti delle decisioni dell'autorità di controllo, fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile nei loro ordinamenti giuridici. In tutti gli Stati membri è disponibile un ricorso giurisdizionale, fatta eccezione per due Stati membri[58] nei quali un'autorità di controllo non tratta un reclamo o non informa l'interessato entro 3 mesi dello stato o dell'esito del reclamo proposto[59].

La maggior parte degli Stati membri dispone altresì la possibilità di un ricorso giurisdizionale nei confronti del titolare del trattamento e del responsabile del trattamento[60] in caso di presunta violazione della LED. Tuttavia diverse leggi nazionali di recepimento non prevedono il diritto dell'interessato di dare mandato ad organismi, organizzazioni o associazioni senza scopo di lucro di proporre reclamo a un'autorità di controllo o di avviare un ricorso giurisdizionale per suo conto[61].

2.2.4 Termini per conservazione ed esame

Gli approcci degli Stati membri al recepimento dei termini di cui alla LED per la conservazione dei dati personali e il suo esame[62] variano notevolmente. La maggior parte degli atti nazionali in materia di protezione dei dati che recepiscono la LED soddisfa soltanto la prescrizione generale di cui all'articolo 5 LED. Ciò significa che spetta alla legislazione settoriale fissare effettivamente i termini per la cancellazione dei dati personali o per un esame periodico della necessità di conservare i dati personali. Alcuni Stati membri recepiscono la disposizione fissando i termini nella legislazione di settore.

In alcuni Stati membri tuttavia la legge lascia all'autorità competente la definizione dei termini. In alcuni casi la legge non stabilisce criteri per l'esame periodico né richiede che tali criteri siano

[56] Articolo 52 LED.
[57] Articolo 53 LED.
[58] Finlandia e Svezia.
[59] Articolo 53, paragrafo 2, LED.
[60] Articolo 54 LED.
[61] Articolo 55 LED.
[62] Articolo 5 LED.

previsti da altre leggi e/o non prevede l'esistenza di procedure destinate a garantire il rispetto dei termini nel diritto nazionale.

Occorre sottolineare che la Corte suprema amministrativa bulgara ha recentemente chiesto alla Corte di rispondere alla sua domanda di pronuncia pregiudiziale sull'interpretazione dell'articolo 5 LED in merito ai termini per la conservazione dei dati[63].

2.2.5 Base giuridica per il trattamento, comprese categorie particolari di dati personali

La maggior parte degli Stati membri prevede, utilizzando una formulazione che spesso corrisponde molto da vicino a quella dell'articolo 8 LED, che la base giuridica per il trattamento debba essere stabilita nel diritto dell'UE o degli Stati membri. Tuttavia alcuni atti nazionali in materia di protezione dei dati che recepiscono la LED non rispecchiano la prescrizione secondo la quale i dati personali da trattare e le finalità del trattamento debbano essere stabiliti per legge[64]. Altri atti nazionali in materia di protezione dei dati che recepiscono la LED non contengono tutte le disposizioni corrispondenti all'articolo 8. Spetta alla legislazione nazionale fissare le basi del trattamento e rispettare le prescrizioni di cui all'articolo 8. Inoltre la semplice ripetizione nel diritto nazionale delle prescrizioni generali di cui all'articolo 8 LED non può essere considerata una base giuridica sufficiente per un trattamento specifico: il diritto nazionale deve specificare quale autorità è competente per il trattamento dei dati personali, i compiti pubblici che svolge che giustificano tale trattamento e la finalità del trattamento stesso.

Per quanto concerne il trattamento di categorie particolari di dati personali[65], la maggior parte degli Stati membri richiede l'esistenza di una necessità effettiva come presupposto per il trattamento. La maggior parte degli Stati membri prevede altresì le stesse basi giuridiche per il trattamento di dati sensibili di cui all'articolo 10 LED (trattamento autorizzato dalla legge; necessario per tutelare un interesse vitale dell'interessato o di un'altra persona; o riguardi dati resi manifestamente pubblici dall'interessato). In alcuni Stati membri, le leggi di recepimento prevedono alcuni ulteriori motivi per il trattamento dei dati (ad esempio quando il trattamento di tali dati è necessario per scongiurare o prevenire un pericolo che minaccia direttamente la vita, l'integrità fisica o il patrimonio di persone oppure per proteggere la salute o gli interessi dell'interessato o di un'altra persona). Laddove la legge nazionale sulla protezione dei dati che recepisce la LED non fornisce le garanzie necessarie per i diritti e le libertà degli interessati (come nel caso di alcuni Stati membri), tali garanzie devono essere previste da leggi settoriali.

Alcune leggi nazionali di recepimento fanno riferimento al consenso in relazione al trattamento dei dati personali, compreso il trattamento di categorie particolari di dati personali. È importante ricordare che, sebbene agli Stati membri non sia impedito prevedere nel loro diritto nazionale che l'interessato possa acconsentire al trattamento dei propri dati personali per finalità di cui alla LED, tale consenso può fungere soltanto da garanzia e non può costituire la base giuridica per tale

---

[63] Domanda di pronuncia pregiudiziale nella causa *NG/Direktor na Glavna direktsia "Natsionalna politsia" pri MVR - Sofia*, C-118/22.
[64] Articolo 8, paragrafo 2, LED.
[65] Articolo 10 LED.

trattamento. Le discussioni in merito a questo tema indicano che sarebbe utile disporre di maggiori orientamenti sul ruolo del consenso nel contesto del trattamento di dati personali per finalità di contrasto in materia penale.

2.2.6 Processo decisionale automatizzato

Tutte le leggi di recepimento degli Stati membri contengono disposizioni che vietano una decisione basata unicamente sul trattamento automatizzato, fatto salvo il caso in cui detta decisione sia prevista dalla legge[66]. La maggior parte delle leggi di recepimento degli Stati membri richiede che tali decisioni non si basino su categorie particolari di dati personali, a meno che non siano previste garanzie adeguate[67]. Tali leggi proibiscono inoltre la profilazione che porta alla discriminazione[68]. Tuttavia alcune legislazioni nazionali non fanno riferimento a garanzie adeguate per i diritti e le libertà dell'interessato nei casi in cui il processo decisionale automatizzato sia autorizzato per legge. Più in particolare, non tutti gli Stati membri prevedono il diritto di ottenere l'intervento umano da parte del titolare del trattamento o non tutti richiedono misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

2.2.7 Diritti degli interessati

Tutti gli Stati membri hanno scelto di avvalersi della possibilità offerta dalla LED di limitare il diritto di accesso degli interessati ai propri dati personali[69]. La maggior parte degli Stati membri prevede altresì limitazioni di altri diritti degli interessati[70]. Gli atti nazionali in materia di protezione dei dati che recepiscono la LED spesso si limitano a seguire la formulazione generale della LED senza specificare ulteriormente le circostanze o le condizioni nelle quali si applicano le limitazioni. In tali casi, tali circostanze e condizioni devono essere specificate nella legislazione settoriale, altrimenti tale circostanza fornirebbe discrezionalità ai titolari del trattamento dei dati nell'applicazione di tali limitazioni.

La maggior parte degli Stati membri rispetta la prescrizione della LED che prevede sia consentito agli interessati di esercitare i propri diritti tramite l'autorità di controllo della protezione dei dati[71]. La maggior parte degli Stati membri si è avvalsa della facoltà di stabilire che i diritti degli interessati debbano essere esercitati conformemente al diritto nazionale nel contesto delle indagini e dei procedimenti penali nazionali[72].

---

[66] Articolo 11, paragrafo 1, LED.
[67] Articolo 11, paragrafo 2, LED.
[68] Articolo 11, paragrafo 3, LED.
[69] Articolo 15, paragrafo 1, LED.
[70] Articolo 13, paragrafo 3, e articolo 16, paragrafo 4.
[71] Articolo 17 LED.
[72] Articolo 18 LED.

Le leggi di recepimento di diversi Stati membri non rispecchiano tutte le prescrizioni specifiche della LED in merito al modo in cui devono essere esercitati i diritti degli interessati (ad esempio formato e mezzi di comunicazione delle risposte, assenza di addebiti).

È pendente una pronuncia pregiudiziale[73] sollevata da un organo giurisdizionale tedesco in merito all'interpretazione delle limitazioni al diritto di accesso degli interessati ai propri dati (articolo 15 LED alla luce dell'articolo 54 LED) e al diritto a un ricorso giurisdizionale effettivo ai sensi dell'articolo 47 della Carta nonché alla libertà professionale di cui all'articolo 15 della Carta.

2.2.8 Alcune importanti disposizioni specifiche della LED

Alcune disposizioni della LED sono specifiche del contesto delle attività di contrasto in materia penale e non hanno equivalenti nel GDPR.

Categorie di interessati

La LED obbliga gli Stati membri a richiedere al titolare del trattamento di operare una distinzione, ove applicabile e per quanto possibile, tra i dati di categorie diverse di interessati e di fornire esempi di tali categorie (ad esempio una persona per la quale sussistono fondati motivi di ritenere che abbia commesso o stia per commettere un reato (un "indiziato"))[74]. Le leggi di alcuni Stati membri non specificano (in una certa misura o affatto) le categorie elencate dalla LED. Quando specificano la categoria degli "indiziati", alcune legislazioni nazionali non richiedono che vi siano "fondati motivi di ritenere che le persone in questione abbiano commesso o stiano per commettere un reato". L'imminente sentenza della Corte nella causa pendente *Ministerstvo na vatreshnite raboti/B.C.* chiarirà ulteriormente l'interpretazione della LED per quanto concerne le categorie di interessati, compresa la prescrizione secondo la quale la categorizzazione di un interessato come un indiziato dovrebbe essere subordinata all'esistenza di "fondati motivi di ritenere che la persona in questione abbia commesso o stia per commettere un reato"[75].

Distinzione tra classi di dati personali e verifica della loro qualità

Gli Stati membri devono disporre che i dati personali fondati su fatti siano differenziati, nella misura del possibile, da quelli fondati su valutazioni personali[76]. Devono altresì adottare misure affinché i dati personali inesatti, incompleti o non più aggiornati non siano trasmessi o resi disponibili. Qualora siano stati trasmessi dati errati, i destinatari dovrebbero essere informati senza indugio e in tali casi i dati personali devono essere rettificati, cancellati o il loro trattamento deve essere limitato. Sebbene la maggior parte degli Stati membri abbia recepito tale obbligo, alcune delle misure specifiche richieste non sono esplicitamente previste da diverse leggi nazionali di recepimento.

---

[73] Domanda di pronuncia pregiudiziale nella causa *TX/Repubblica federale di Germania*, C-481/21.
[74] Articolo 6 LED.
[75] Domanda di pronuncia pregiudiziale nella causa *Ministerstvo na vatreshnite raboti/B.C.*, C-205/21.
[76] Articolo 7 LED.

Registrazione

Complessivamente 12 Stati membri[77] si sono avvalsi della possibilità di posticipare fino a maggio del 2023 l'adeguamento del proprio sistema di trattamento automatizzato in linea con le prescrizioni in materia di registrazione[78].

La maggior parte degli Stati membri dispone che siano conservate registrazioni per i trattamenti nel contesto di sistemi di trattamento automatizzato[79]. Alcune leggi nazionali non richiedono la registrazione di tutti i tipi di operazioni. La LED stabilisce i tipi minimi di informazioni che tali registrazioni devono contenere. Alcune legislazioni nazionali non hanno incluso tutte le tipologie di informazioni richieste (ad esempio motivo della consultazione o divulgazione di dati personali).

3 PRIMI INSEGNAMENTI TRATTI DALL'APPLICAZIONE E DAL FUNZIONAMENTO DELLA LED

3.1 Reclami e impatto positivo sui diritti degli interessati

La LED garantisce la protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati. Fornisce un quadro completo per i diritti degli interessati e le modalità per l'esercizio di tali diritti, compreso il loro diritto di informazione, accesso, rettifica o cancellazione dei propri dati personali, oltre a prevedere la limitazione del trattamento. La LED ha migliorato la comprensione da parte degli interessati dei loro diritti e di come possono esercitarli, e ciò si traduce in un aumento del numero di richieste presentate alle autorità competenti. La pratica ha dimostrato che, tra i diritti conferiti agli interessati ai sensi della LED, il diritto di accesso e cancellazione sono quelli invocati più di frequente presso le autorità competenti[80].

La LED consente di porre limiti a determinati diritti (diritto di accesso[81] e diritto di rettifica o cancellazione[82]) e alle informazioni che un titolare del trattamento dei dati deve fornire all'interessato in relazione ai dati personali oggetto di trattamento[83]. Gli interessati possono chiedere alle autorità di controllo della protezione dei dati di riesaminare una limitazione del diritto in questione attuata da un'autorità competente oppure chiedere loro di verificare se la limitazione in questione sia stata effettuata in conformità con la LED (esercizio indiretto del diritto)[84].Circa la metà delle autorità di controllo della protezione dei dati dichiara di aver ricevuto una tale richiesta[85]. Dalla pratica emerge che il numero di richieste ricevute può variare in modo

[77] La Germania ha fatto uso dell'opzione per talune leggi che recepiscono la LED a livello federale e di Land.
[78] Articolo 63, paragrafo 2, LED.
[79] Articolo 25 LED.
[80] Posizione e conclusioni del Consiglio in merito all'applicazione della LED, punto 15.
[81] Articolo 15 LED.
[82] Articolo 16 LED.
[83] Articolo 13 LED.
[84] Articolo 17 LED.
[85] Quattro autorità di controllo della protezione dei dati non raccolgono statistiche sulle richieste ricevute ai sensi dell'articolo 17 LED.

significativo (ad esempio la Croazia ha ricevuto una richiesta di questo tipo, ma la Francia ne ha ricevute più di 1 500)[86]. Sebbene le autorità di controllo della protezione dei dati abbiano stabilito, a seguito di una verifica o di un riesame di tali reclami, che la maggior parte delle richieste era inammissibile, in diversi casi al titolare del trattamento è stato ordinato di rettificare o cancellare i dati personali o di limitare il trattamento dei dati personali dati, garantendo così la corretta applicazione delle limitazioni[87].

La LED dispone che un organismo, un'organizzazione o un'associazione senza scopo di lucro possa presentare un reclamo per conto di un interessato. Tuttavia il ricorso a tale possibilità sembra essere sottoutilizzato (soltanto quattro autorità di controllo della protezione dei dati hanno riferito di aver ricevuto tali reclami da un organismo di rappresentanza[88]). Analogamente le organizzazioni della società civile hanno segnalato soltanto un numero limitato di richieste di presentazione di un tale reclamo[89].

Le persone fisiche utilizzano sempre più anche il loro diritto di presentare reclami presso le autorità di controllo della protezione dei dati, anche nei casi in cui le autorità competenti limitano l'esercizio dei diritti degli interessati. Più di un terzo delle autorità di controllo della protezione dei dati ha segnalato un aumento del numero di reclami ricevuti in seguito al recepimento della LED nei propri Stati membri[90]. Alcuni dei reclami più frequenti ricevuti dalle autorità di controllo della protezione dei dati hanno riguardato la limitazione del diritto di accesso[91], il diritto di rettifica o cancellazione[92] e il diritto di informazione e le corrispondenti limitazioni[93]. A questi sono seguiti i reclami relativi al principio di limitazione della conservazione, che impone alle autorità competenti di conservare i dati personali per un periodo non superiore a quello necessario, e quindi i reclami relativi al diritto di informazione.

3.2 Maggiore consapevolezza della protezione dei dati in seno alle autorità competenti

Gli Stati membri riferiscono che l'introduzione della LED ha prodotto e continua a produrre un impatto notevole sensibilizzazione delle autorità competenti in merito all'importanza della protezione dei dati[94]. Diverse autorità di controllo della protezione dei dati hanno espresso il loro parere secondo il quale la maggiore ripercussione della LED è stata quella di aumentare la consapevolezza e l'attenzione verso questioni relative alla protezione dei dati e i diritti degli

[86] Si tratta di richieste formulate dal recepimento della LED fino a dicembre del 2021. Contributo dell'EDPB alla valutazione della LED (risposte individuali delle autorità di protezione dei dati).
[87] Contributo dell'EDPB alla valutazione della LED, punto 50.
[88] Contributo dell'EDPB alla valutazione della LED, punto 33.
[89] Tre organizzazioni (nel contesto delle risposte ai questionari inviati loro dall'Agenzia dell'Unione europea per i diritti fondamentali) hanno riferito di aver ricevuto una richiesta e un'organizzazione ha riferito di aver ricevuto più di una richiesta.
[90] Contributo dell'EDPB alla valutazione della LED, punto 31.
[91] Articolo 15 LED.
[92] Articolo 16 LED.
[93] Articolo 13 LED.
[94] Posizione e conclusioni del Consiglio in merito all'applicazione della LED, punto 21.

interessati[95]. Ciò è stato dimostrato anche dagli scambi tra le autorità di controllo della protezione dei dati e le autorità competenti sui diritti degli interessati e sulle modalità di esercizio di tali diritti[96]. Alcune autorità competenti hanno riferito di aver stanziato di conseguenza maggiori risorse a favore della protezione dei dati[97]. Sono rientrati in tale contesto investimenti a sostegno dell'incorporazione del principio di tutela della vita privata fin dalla progettazione e per impostazione predefinita nei loro sistemi informatici, la definizione di periodi di conservazione dei dati, l'applicazione del principio della minimizzazione dei dati e la segnalazione di violazioni. Di conseguenza la sicurezza complessiva dei dati trattati risulta migliorata[98].

Anche le attività di formazione e sensibilizzazione da parte delle autorità di controllo della protezione dei dati contribuiscono alla corretta attuazione della LED; inoltre le autorità di controllo hanno il compito di aumentare la consapevolezza dei titolari del trattamento e dei responsabili del trattamento dei dati degli obblighi imposti loro dalla presente direttiva[99].

Numerose autorità di controllo della protezione dei dati svolgono tale attività di sensibilizzazione pubblicando orientamenti. Alcuni degli argomenti trattati dalle diverse autorità di controllo della protezione dei dati comprendono: fornire assistenza alla magistratura, alle procure e le autorità di polizia nel rispettare il principio di responsabilizzazione; scambiare dati personali con le forze di polizia; nominare un responsabile della protezione dei dati; effettuare una valutazione d'impatto sulla protezione dei dati; trattare dati in settori in materia penale quali la criminalità organizzata e il terrorismo; tenere registrazioni delle attività di trattamento ed effettuare registrazioni; svolgere attività di videosorveglianza; fornire informazioni agli interessati; notificare violazioni dei dati; obblighi dei titolari del trattamento; ed esercizio dei diritti da parte delle persone fisiche.

Tuttavia otto autorità di controllo della protezione dei dati non hanno ancora emesso orientamenti e/o strumenti pratici destinati a sostenere le autorità competenti e i responsabili del trattamento nel rispettare i propri obblighi.

Inoltre 12 autorità di controllo della protezione dei dati non hanno erogato alcuna formazione né svolto attività di sensibilizzazione a favore delle autorità competenti o dei responsabili del trattamento nel quadro della LED[100]. Tra le autorità di controllo della protezione dei dati che hanno svolto tali attività, i temi trattati più di frequente sono stati: trattamento dei dati da parte di forze di polizia, procure, autorità giudiziarie e penitenziarie; definizione dei rispettivi settori di applicazione del GDPR e della LED; utilizzo di dati personali desunti da reti di social media;

[95] Contributo dell'EDPB alla valutazione della LED (risposte individuali delle autorità di protezione dei dati).
[96] Contributo dell'EDPB alla valutazione della LED, punto 40 e posizione e conclusioni del Consiglio in merito all'applicazione della LED, pag. 9.
[97] Contributo dell'EDPB alla valutazione della LED, punto 70.
[98] Contributo dell'EDPB alla valutazione della LED, punto 70.
[99] Articolo 46, paragrafo 1, lettera d), LED.
[100] Contributo dell'EDPB alla valutazione della LED (risposte individuali delle autorità di protezione dei dati).

trattamento di dati nel contesto di archivi di polizia; tecniche di videosorveglianza e megadati (*big data*); gestione dei diritti degli interessati; e trattamento dei dati personali di detenuti[101].

Un'ulteriore innovazione della LED è costituita dall'obbligo per i titolari del trattamento dei dati di designare un responsabile della protezione dei dati (RPD) i cui compiti comprendono, tra gli altri: informare e consigliare in merito ai requisiti in materia di protezione dei dati; sorvegliare l'osservanza della LED; fornire un parere sulle valutazioni d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento[102]. Il Consiglio ha riconosciuto altresì che ciò ha reso le autorità competenti maggiormente consapevoli in merito ai loro obblighi in materia di protezione dei dati oltre ad aver avuto un impatto positivo su dette autorità competenti per quanto riguarda la loro conformità alle norme in materia di protezione dei dati[103].

È importante investire nello sviluppo e nella massimizzazione delle competenze e delle conoscenze dei responsabili della protezione dei dati al fine di aiutare le autorità competenti ad applicare la LED in modo coerente[104]. La Commissione ha pertanto istituito e facilita la rete dei responsabili della protezione dei dati delle autorità competenti, delle agenzie che operano nel settore della giustizia e degli affari interni nonché della Procura europea. Tale rete è un'iniziativa permanente che si concentra sull'applicazione della LED da parte delle autorità competenti degli Stati membri. Mira a mettere a disposizione una piattaforma per la cooperazione e lo scambio di competenze tra i responsabili della protezione dei dati degli Stati membri. La rete di esperti in materia di protezione dei dati di Europol (EDEN) e le reti nazionali dei responsabili della protezione dei dati per le autorità competenti sono iniziative importanti che assistono i responsabili della protezione dei dati delle autorità competenti a promuovere lo scambio di migliori prassi e informazioni sull'applicazione della LED.

3.3 La sicurezza dei dati è migliorata ma si registrano divergenze nelle notifiche di violazioni dei dati

La LED ha migliorato la sicurezza dei dati personali richiedendo alle autorità competenti di adottare misure destinate a conseguire obiettivi specifici in materia di sicurezza. Ad esempio richiede alle autorità competenti di effettuare valutazioni d'impatto sulla protezione dei dati quando un'attività di trattamento dei dati è suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati. Le valutazioni d'impatto implicano l'individuazione dei rischi e di misure destinate a mitigarli. Tale requisito, oltre all'assoluto rispetto del principio della protezione dei dati fin dalla progettazione e per impostazione predefinita nonché degli obblighi di notifica delle

[101] Contributo dell'EDPB alla valutazione della LED, punti 41 e 42.
[102] Articoli da 32 a 34 LED.
[103] Posizione e conclusioni del Consiglio in merito all'applicazione della LED, punto 22.
[104] Posizione e conclusioni del Consiglio in merito all'applicazione della LED, punto 25.

violazioni dei dati, ha portato a un miglioramento della sicurezza del trattamento di dati personali[105].

Anche il Consiglio ha riconosciuto tale circostanza, ritenendo che la LED abbia migliorato il livello di sicurezza dei dati anche attraverso piani di sicurezza; la modernizzazione dei sistemi informatici e delle misure organizzative; le valutazioni d'impatto sulla protezione dei dati; e l'imposizione dell'obbligo per le autorità competenti di tenere registri in merito a trattamenti specifici[106].

La LED stabilisce le circostanze nelle quali i titolari del trattamento devono notificare una violazione dei dati personali alla propria autorità di controllo della protezione dei dati e all'interessato in questione[107]. Nonostante tale obbligo, si registra un'ampia disparità nel numero di violazioni dei dati che sono state notificate alle autorità di controllo della protezione dei dati da quando è stata introdotta la LED[108]. Sei autorità di controllo della protezione dei dati hanno riferito di non aver ricevuto notifiche di violazione dei dati[109] e molte altre hanno riferito di aver ricevuto pochissime notifiche di tale tipo. Ad esempio l'autorità italiana ha segnalato soltanto tre notifiche di violazione dei dati e l'autorità francese ne ha segnalate otto, ma l'autorità dei Paesi Bassi ne ha segnalate oltre 500.

Tale differenza nel numero di notifiche di violazione dei dati segnalate suggerisce (dopo aver tenuto conto di fattori quali la dimensione della popolazione) che sembrano esserci pratiche divergenti tra le autorità competenti degli Stati membri per quanto concerne ciò che è considerato una violazione e quando è necessario segnalarla ad un'autorità di controllo della protezione dei dati. La Commissione lo ha notato anche nella sua relazione sul GDPR[110]. L'EDPB ha pubblicato di recente linee guida sulle violazioni ai sensi del GDPR[111]. Tali linee guida, sebbene non direttamente applicabili, sono pertinenti anche per le violazioni dei dati ai sensi della LED. Dovrebbero pertanto contribuire a un approccio più uniforme alla gestione delle violazioni dei dati ai sensi della LED negli Stati membri.

---

[105] Contributo dell'EDPB alla valutazione della LED, punti 70 e 71, e risposte individuali delle autorità di protezione dei dati (Germania, Finlandia, Francia, Ungheria, Malta).
[106] Posizione e conclusioni del Consiglio in merito all'applicazione della LED, punto 26.
[107] Articoli 30 e 31 LED.
[108] I dati comprendono tutte le violazioni dei dati segnalate tra il recepimento della LED e il mese di dicembre del 2021. I dati sono stati raccolti dalle autorità di controllo della protezione dei dati nel dicembre del 2021.
[109] Spagna, Croazia, Lituania, Portogallo, Slovacchia e Slovenia.
[110] Documento di lavoro dei servizi della Commissione che accompagna la 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).
[111] EDPB, Linee guida 1/2021 concernenti esempi relativi alla notifica delle violazioni dei dati personali, adottate il 14 dicembre 2021, disponibili (solo in EN) al seguente indirizzo: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_it?page=1&order=field_edpb_pc_country&sort=asc.

3.4 Controllo esercitato dalle autorità di controllo della protezione dei dati

3.4.1 Risorse delle autorità di controllo della protezione dei dati

Dotare ciascuna autorità di controllo delle risorse umane, tecniche e finanziarie, dei locali e delle infrastrutture necessari costituisce un presupposto per l'effettivo adempimento dei loro compiti e l'esercizio dei loro poteri e rappresenta di conseguenza una condizione essenziale per la loro indipendenza[112]. La Commissione ha costantemente ribadito il fatto che gli Stati membri sono tenuti a destinare risorse umane, finanziarie e tecniche sufficienti alle autorità di controllo della protezione dei dati[113]. Il Consiglio ha inoltre invitato specificamente gli Stati membri ad assegnare sufficienti risorse umane, tecniche e finanziarie alle autorità di controllo competenti per la protezione dei dati[114].

Tuttavia l'aumento complessivo del personale delle autorità di controllo della protezione dei dati negli ultimi anni[115] non sembra riguardare compiti relativi alla LED. Il numero di membri del personale che lavorano alla LED è rimasto invariato o è addirittura diminuito presso la metà delle autorità di controllo della protezione dei dati[116]. Gli eventuali aumenti sono stati decisamente modesti, pari in media a meno di due persone in equivalenti a tempo pieno ("ETP")[117]. Presso quasi la metà delle autorità di controllo della protezione dei dati (comprese quelle con un numero totale di dipendenti superiore a 100 ETP), tra meno dell'1 % e il 7 % dell'organico complessivo si occupa di LED[118]. In numeri assoluti, circa la metà delle autorità di controllo della protezione dei dati dedica da 1 a 4 ETP a compiti concernenti la LED, mentre otto autorità di controllo della protezione dei dati dedicano da 7 a 15 ETP a tali compiti. Tuttavia un'autorità di controllo della protezione dei dati dispone di 53 ETP che si occupano di LED[119]. Analogamente il segretariato dell'EDPB ha dedicato meno di 1,5 ETP a questioni interamente legate alla LED.

---

[112] Articolo 42, paragrafo 4, LED.
[113] 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).
[114] Posizione e conclusioni del Consiglio in merito all'applicazione della LED, punto 12.
[115] Contributo dell'EDPB alla valutazione del regolamento generale sulla protezione dei dati ai sensi dell'articolo 97, 18 febbraio 2020, pagg. da 26 a 29 (solo in EN) - https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_it; Panoramica dell'EDPB sulle risorse messe a disposizione dagli Stati membri alle autorità di protezione dei dati e sulle azioni di contrasto promosse da tali autorità ("Panoramica dell'EDPB sulle risorse"), 5 agosto 2021, pagg. 4 e 5 (solo in EN) - https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/overview-resources-made-available-member-states-data_it.
[116] Contributo dell'EDPB alla valutazione della LED, punto 65 e figura relativa al quesito 41, pag. 20.
[117] La Germania ha comunicato un aumento significativo da 33 a 53 ETP tra il 2017 e il 2021.
[118] Contributo dell'EDPB alla valutazione della LED, figura relativa al quesito 41, pag. 20. Panoramica dell'EDPB sulle risorse, pag. 5.
[119] Contributo dell'EDPB alla valutazione della LED, figura relativa al quesito 41, pag. 19.

Tale situazione non è soddisfacente, anche se 10 autorità di controllo della protezione dei dati hanno indicato di disporre di risorse finanziarie, umane e tecniche sufficienti[120]. Al contrario, 16 autorità di controllo della protezione dei dati hanno riscontrato di non disporre di risorse sufficienti. Tra queste ultime autorità, alcune hanno rilevato che ciò ha avuto un impatto negativo sulle indagini condotte di propria iniziativa[121], sulla gestione dei reclami[122], sull'ispezione di sistemi informatici su larga scala (sistema d'informazione Schengen (SIS) e sistema d'informazione visti (VIS)) nonché sull'emissione di pareri di propria iniziativa[123]. Le specificità del settore fanno in effetti sì che l'attuazione efficace della LED richieda ispezioni sistematiche delle attività di trattamento che sono spesso complesse, così come che non sia sufficiente fare affidamento sui singoli reclami (che sono di gran lunga inferiori rispetto a quelli per il GDPR)[124].

Inoltre le autorità di controllo della protezione dei dati hanno sottolineato la mancanza di competenze informatiche per far fronte alla complessità sempre crescente delle tecnologie informatiche utilizzate nel settore delle attività di contrasto[125].

3.4.2 Esercizio dei poteri

Esercizio dei poteri correttivi

Complessivamente 19 autorità di controllo della protezione dei dati hanno esercitato i propri poteri d'indagine, di propria iniziativa o sulla base di un reclamo[126]. Le autorità di controllo della protezione dei dati hanno segnalato difficoltà soltanto in pochissimi casi (ad esempio quando un titolare del trattamento dei dati non ha fornito tutte le informazioni pertinenti o ha rifiutato l'accesso alle informazioni)[127].

Le stesse 19 autorità di controllo della protezione dei dati hanno inoltre esercitato i propri poteri correttivi. Il potere di gran lunga più esercitato è stato quello di emettere ordini affinché il trattamento fosse reso conforme alla legge, compresi gli ordini di rettifica o cancellazione di dati personali o di limitazione del loro trattamento. Le autorità di controllo della protezione dei dati

---

[120] Belgio, Danimarca, Irlanda, Grecia, Lettonia, Lussemburgo, Ungheria, Malta, Austria e Finlandia.
[121] Germania e Francia.
[122] Francia e Svezia.
[123] Paesi Bassi.
[124] L'Irlanda ha ricevuto 135 reclami relativi alla LED dal 2018, l'Ungheria ne ha ricevuti 141 dal 2018 e la Danimarca ne ha ricevuti 223 dal 2017. Al contrario ci sono stati migliaia di reclami relativi al GDPR (cfr. Panoramica dell'EDPB sulle risorse, pag. 10.)
[125] Contributo dell'EDPB alla valutazione della LED, punto 69.
[126] Le autorità di controllo della protezione dei dati di Irlanda, di Malta e dei Paesi Bassi hanno riferito di aver condotto indagini di propria iniziativa. Le autorità di controllo della protezione dei dati di Grecia, Spagna, Lituania e Ungheria hanno condotto indagini sulla base di reclami. Le autorità di controllo della protezione dei dati di Belgio, Bulgaria, Danimarca, Germania, Francia, Italia, Lussemburgo, Austria, Polonia, Slovenia e Svezia hanno condotto indagini tanto di propria iniziativa quanto sulla base di reclami.
[127] Le autorità di controllo della protezione dei dati di Germania e Ungheria hanno dichiarato di non aver ricevuto tutte le informazioni necessarie e/o che il titolare del trattamento ha negato loro l'accesso alle informazioni necessarie. Le autorità tedesche hanno affermato che non è previsto un potere analogo a quello di cui all'articolo 58, paragrafo 1, lettera a), del GDPR.

hanno esercitato tale potere in 114 casi. Il fatto che tale potere di ordinare una limitazione temporanea o definitiva (compreso il divieto) di un trattamento sia stato esercitato soltanto in quattro casi[128] dimostra che le autorità di controllo della protezione dei dati hanno esercitato tali poteri con cautela.

Esercizio dei poteri consultivi

Il perseguimento sistematico di consultazioni preventive e la richiesta del parere delle autorità di controllo della protezione dei dati in merito a progetti di misure legislative e amministrative costituiscono un mezzo efficace per garantire un livello elevato di protezione del diritto alla protezione dei dati personali nonché per ridurre il numero di reclami conseguenti. La consultazione preventiva delle autorità di controllo della protezione dei dati è di particolare importanza quando si utilizzano tecnologie nuove suscettibili di incidere in maniera significativa sui diritti fondamentali.

La metà delle autorità di controllo della protezione dei dati ha riferito di essere stata consultata in merito a valutazioni d'impatto sulla protezione dei dati. Il numero di consultazioni preventive varia da uno Stato membro all'altro. Talune autorità sono state consultate soltanto una volta mentre un'altra autorità ha ricevuto 59 consultazioni preventive[129]. Nella maggior parte di questi casi le autorità di controllo della protezione dei dati hanno fornito consulenza scritta e in alcuni casi hanno utilizzato i propri poteri correttivi in relazione al trattamento, in particolare hanno emesso avvertimenti od ordinato misure destinate a rendere il trattamento dei dati conforme alla legge. In un caso, l'autorità di controllo della protezione dei dati ha emesso un parere negativo che sembra avere avuto lo stesso effetto di un divieto del trattamento.

Inoltre sembra che le autorità di controllo della protezione dei dati si occupino anche delle richieste di consulenza, al di fuori della procedura di consultazione preventiva. Il tipo più comune di questione in merito alla quale le autorità competenti si sono rivolte alle autorità di controllo della protezione dei dati per una consulenza riguardava tipi specifici di trattamento (in particolare l'uso di tecnologie, meccanismi o procedure nuovi, seguiti da vicino da adeguate misure di sicurezza, il trattamento di categorie particolari di dati personali, la determinazione della base giuridica per un trattamento, il principio di limitazione della conservazione e termini adeguati[130]).

[128] Contributo dell'EDPB alla valutazione della LED, punto 30, e anche risposte individuali delle autorità di Austria e Lussemburgo.
[129] Le autorità di controllo della protezione dei dati di Danimarca e Lituania hanno riferito di essere state consultate soltanto una volta. L'autorità di controllo della protezione dei dati belga ha ricevuto 59 consultazioni preventive.
[130] Contributo dell'EDPB alla valutazione della LED, punto 39.

Inoltre 22 autorità di controllo della protezione dei dati hanno emesso pareri destinati ai rispettivi parlamenti e governi nazionali in merito a misure legislative e amministrative relative al trattamento di dati personali. Numerose hanno riferito di essere consultate occasionalmente[131].

3.4.3 Controllo giurisdizionale delle azioni delle autorità di controllo della protezione dei dati

Quasi la metà delle autorità di controllo della protezione dei dati ha riferito che in un numero esiguo di casi ha dovuto affrontare procedimenti giudiziari in relazione alle sue decisioni oppure a una sua non azione. Tali procedimenti sono stati avviati principalmente da interessati e, in alcuni casi, da autorità competenti[132]. Diversi casi sono stati dichiarati inammissibili dagli organi giurisdizionali oppure sono stati ritirati dai ricorrenti. Nella maggior parte dei casi rimanenti l'organo giurisdizionale ha confermato la decisione dell'autorità di controllo della protezione dei dati, ma in alcuni casi l'ha ribaltata (inoltre altri erano ancora pendenti). L'esiguo numero di sentenze emesse fino ad oggi fa sì che non sia ancora possibile rilevare una tendenza evidente.

3.4.4 Linee guida dell'EDPB

La coerenza e un livello elevato di protezione tra gli Stati membri sono fondamentali per garantire un'efficace cooperazione giudiziaria in materia penale e di polizia[133]. La LED prevede che l'EDPB emetta linee guida, raccomandazioni e migliori prassi (di propria iniziativa o su richiesta della Commissione) al fine di garantire che gli Stati membri applichino la LED in modo coerente. L'EDPB ha prodotto linee guida specifiche per la LED pertinenti per il capo V (trasferimenti internazionali)[134]; orientamenti sull'uso delle tecnologie di riconoscimento facciale[135]; e (nella sua precedente qualità di Gruppo di lavoro Articolo 29, in appresso "Gruppo di lavoro") un parere in merito ad alcune questioni fondamentali della LED[136].

Numerose delle linee guida dell'EDPB sul GDPR sono pertinenti anche per la LED nella misura in cui si basano su concetti o tecnologie comuni. Tali linee guida comprendono quelle sui concetti

---

[131] Le autorità di controllo della protezione dei dati di Cechia, Grecia, Croazia, Lettonia e Svezia hanno riferito di non aver emesso pareri. Le autorità di controllo della protezione dei dati di Grecia, Croazia, Lettonia, Polonia, Romania, Slovenia e Slovacchia sono state consultate soltanto occasionalmente.

[132] Questa osservazione si basa sulle risposte ricevute dalle autorità di controllo della protezione dei dati di Belgio, Bulgaria, Germania, Estonia, Irlanda, Italia, Ungheria, Paesi Bassi, Austria, Polonia, Finlandia e Svezia.

[133] Considerando 7 LED.

[134] EDPB, Raccomandazioni 1/2021 sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, adottate il 2 febbraio 2021 - https://edpb.europa.eu/system/files/2021-05/recommendations012021onart.36led.pdf_it.pdf.

[135] EDPB, Linee guida 5/2022 sull'uso della tecnologia di riconoscimento facciale nel settore delle attività di contrasto, adottate il 12 maggio 2022, versione per la consultazione pubblica, disponibile (solo in EN) all'indirizzo: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.

[136] Gruppo di lavoro, Parere su alcune questioni fondamentali della direttiva (UE) 2016/680 sulla protezione dei dati nelle attività di polizia e giustizia, WP 258, adottato il 29 novembre 2017, disponibile (solo in EN) all'indirizzo: https://ec.europa.eu/newsroom/article29/items/610178/en.

di titolare del trattamento e responsabile del trattamento[137], sui diritti degli interessati[138], sulla notifica delle violazioni dei dati personali[139], sulla valutazione dell'impatto sulla protezione dei dati[140], sulla protezione dei dati fin dalla progettazione e per impostazione predefinita[141] e sul processo decisionale automatizzato relativo alle persone fisiche[142].

La produzione di linee guida complete e pratiche richiede lavoro e risorse significativi, ma tali documenti sono essenziali (come ha riscontrato anche il Consiglio[143]). È quindi molto positivo che l'EDPB abbia indicato che presto fornirà ulteriori linee guida, anche sul concetto di poteri d'indagine e correttivi effettivi delle autorità di controllo della protezione dei dati e sui trasferimenti internazionali soggetti a garanzie adeguate.

Le linee guida dell'EDPB possono ridurre altresì il carico di lavoro delle autorità di controllo della protezione dei dati (ad esempio compiti quali la consulenza a favore di titolari del trattamento dei dati o la gestione di reclami). Ad esempio numerose delle questioni affrontate nel parere del Gruppo di lavoro in merito ad alcune questioni fondamentali della LED (come i termini appropriati, la base giuridica del trattamento, le condizioni per il trattamento di categorie particolari di dati) sono anche alcune delle questioni più frequenti in merito alle quali le autorità competenti hanno chiesto consulenza alle autorità di controllo della protezione dei dati[144].

3.4.5 Assistenza reciproca

Per garantire l'applicazione coerente della LED, le autorità di controllo della protezione dei dati sono tenute a prestarsi assistenza reciproca. Rientra in tale contesto l'assistenza sotto forma di

---

[137] EDPB, Linee guida 7/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR, adottate il 7 luglio 2021, disponibili all'indirizzo https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_it.pdf.

[138] EDPB, Linee guida 1/2022 sui diritti degli interessati: diritto di accesso, adottate il 18 gennaio 2022, versione per la consultazione pubblica, disponibili (solo in EN) all'indirizzo: https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.

[139] Gruppo di lavoro, Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679, WP 250rev.01, ultima revisione del 6 febbraio 2018 approvata dall'EDPB il 25 maggio 2018, disponibile all'indirizzo https://ec.europa.eu/newsroom/article29/items/612052/en; EDPB, Linee guida 1/2021 concernenti esempi relativi alla notifica delle violazioni dei dati personali, adottate il 14 dicembre 2021, disponibili (solo in EN) al seguente indirizzo: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_it?page=1&order=field_edpb_pc_country&sort=asc.

[140] Gruppo di lavoro, Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, WP 248rev.01, ultima revisione del 4 ottobre 2017 approvata dall'EDPB il 25 maggio 2018, disponibile all'indirizzo: https://ec.europa.eu/newsroom/article29/items/611236.

[141] EDPB, Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita, adottate il 20 ottobre 2020, disponibili all'indirizzo: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_it.pdf.

[142] Gruppo di lavoro, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, WP 251rev01, ultima revisione del 6 febbraio 2018 approvata dall'EDPB il 25 maggio 2018, disponibili all'indirizzo: https://ec.europa.eu/newsroom/article29/items/612053/en.

[143] Posizione e conclusioni del Consiglio in merito all'applicazione della LED, punto 14.

[144] Contributo dell'EDPB alla valutazione della LED, punto 39.

richieste di informazioni e richieste di effettuare consultazioni, ispezioni e indagini[145]. Tuttavia l'assistenza reciproca è stata utilizzata molto raramente fino ad oggi. Soltanto sei autorità di controllo della protezione dei dati vi hanno fatto ricorso, principalmente in risposta a richieste di informazioni ricevute da altre autorità di controllo della protezione dei dati. La maggior parte delle autorità di controllo della protezione dei dati ha dichiarato di aver ricevuto una sola richiesta di informazioni. Tutte queste autorità di controllo della protezione dei dati hanno riferito di aver ottemperato alla richiesta ricevuta. Non è stato fatto ricorso nemmeno allo scambio di assistenza reciproca volontaria, che non è soggetto a una scadenza fissata per legge o a un obbligo rigoroso di risposta. L'EDPB ha dichiarato che pubblicherà le linee guida sul quadro dell'assistenza reciproca ai sensi del GDPR e della LED[146].

3.5 Strumento flessibile per trasferimenti internazionali di dati

Il capo V LED riguarda i trasferimenti di dati personali alle autorità competenti di paesi terzi e ad organizzazioni internazionali. Tale capo garantisce essenzialmente che vi sia una continuità di protezione quando i dati personali sono trasferiti da uno Stato membro verso un paese terzo o a un'organizzazione internazionale per finalità di contrasto. Come osservato in precedenza, tale continuità di protezione costituisce una condizione importante per una cooperazione in materia di attività di contrasto tra partner fidati che sia rapida, efficace e certa in termini di diritto.

In particolare, ai sensi delle norme pertinenti della LED[147], i trasferimenti internazionali tra autorità competenti ai sensi di tale direttiva devono basarsi su uno dei vari strumenti di trasferimento di cui agli articoli da 36 a 38 della medesima direttiva (se i dati provengono da un altro membro Stato, il trasferimento richiede altresì l'autorizzazione preventiva di tale Stato membro). Tra tali strumenti figurano decisioni di adeguatezza, trasferimenti basati su garanzie adeguate e il ricorso a deroghe in situazioni specifiche. L'articolo 39 LED consente anche trasferimenti diretti a destinatari che non sono autorità di contrasto in materia penale, sono stabiliti in paesi terzi, in casi singoli e specifici, e soddisfano diverse condizioni.

3.5.1 Decisioni di adeguatezza

La Commissione ha accelerato i propri lavori per conseguire il pieno potenziale degli strumenti disponibili nel quadro della LED. Rientra in tale contesto l'adozione, per la prima volta, nel giugno del 2021, di una "decisione di adeguatezza" riguardante le attività di trattamento di dati per finalità

[145] Articolo 50 LED.
[146] Programma di lavoro dell'EDPB 2021/2022 (disponibile solo in EN): edpb_workprogramme_2021-2022_en.pdf (europa.eu).
[147] Cfr. articolo 35, paragrafo 3 e considerando 64 LED. Per quanto concerne i trasferimenti successivi, cfr. articolo 35, paragrafo 1, lettera e), e considerando 65 LED.

di contrasto ai sensi dell'articolo 36 LED in relazione al Regno Unito[148]. Tale decisione di adeguatezza consente una circolazione sicura e libera di dati personali verso le autorità competenti del paese terzo interessato, senza la necessità di ulteriori garanzie o autorizzazioni specifiche (fatto salvo il caso in cui un altro Stato membro, dal quale sono stati ottenuti i dati, debba autorizzare il trasferimento in questione[149]). La decisione di adeguatezza relativa al Regno Unito del giugno 2021 costituisce una base fondamentale per la cooperazione giudiziaria e di polizia post-Brexit che, secondo l'accordo sugli scambi commerciali e la cooperazione UE-Regno Unito, si basa "sull'impegno che le parti onorano da lunga data di garantire un elevato livello di protezione dei dati personali"[150]. A norma dell'articolo 36, paragrafo 4, LED, la Commissione controlla eventuali sviluppi nel quadro giuridico del Regno Unito che potrebbero incidere su tale decisione di adeguatezza. Detta decisione di adeguatezza relativa al Regno Unito dovrebbe applicarsi per un periodo di 4 anni dalla sua entrata in vigore, prorogabile in linea di principio di ulteriori 4 anni qualora il controllo svolto dalla Commissione confermi che il Regno Unito continua a mantenere un livello adeguato di protezione[151].

Inoltre anche l'EDPB ha contribuito allo sviluppo di tale strumento chiarendo il criterio giuridico attraverso linee guida sugli elementi da considerare nella valutazione dell'adeguatezza nel contesto delle attività di contrasto, con l'emissione dei propri criteri di riferimento per l'adeguatezza ai sensi della LED[152]. In particolare il paese terzo deve garantire diritti individuali azionabili, un mezzo di ricorso effettivo in sede giudiziaria e un controllo indipendente.

La Commissione sta promuovendo attivamente la possibilità di svolgere accertamenti di adeguatezza con altri partner internazionali chiave, in particolare con i paesi con i quali è necessaria una stretta e tempestiva cooperazione nella lotta contro la criminalità e il terrorismo e con i quali sono già in atto scambi di dati personali[153]. Sebbene finora non siano state adottate altre decisioni di adeguatezza, ciò è principalmente dovuto al fatto che questo strumento è stato introdotto solo di recente. Inoltre, e a differenza del trattamento di dati da parte di operatori commerciali, soltanto ora inizia a svilupparsi una convergenza globale delle norme in materia di

---

[148] Decisione di esecuzione (UE) 2021/1773 della Commissione del 28 giugno 2021 a norma della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito, disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32021D1773&from=IT.

[149] Cfr. articolo 35, paragrafo 1, lettera c), articolo 35, paragrafo 2 e considerando 66 LED.

[150] Cfr. articolo 525, paragrafo 1, accordo sugli scambi commerciali e la cooperazione.

[151] Cfr. considerando da 172 a 174 della decisione di esecuzione (UE) 2021/1773 della Commissione del 28 giugno 2021 a norma della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito, disponibile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32021D1773&from=IT.

[152] EDPB, Raccomandazioni 1/2021 sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, adottate il 2 febbraio 2021. Cfr. anche articolo 36, paragrafo 2 e considerando 67 LED.

[153] Cfr. Comunicazione della Commissione al Parlamento europeo e al Consiglio, Scambio e protezione dei dati personali in un mondo globalizzato (COM(2017) 7 final), pag. 15.

protezione dei dati nel settore delle attività di contrasto in materia penale (trainata, ad esempio, da accordi multilaterali quali la convenzione 108 del Consiglio d'Europa modernizzata o il secondo protocollo addizionale alla convenzione di Budapest sulla criminalità informatica). Ciò nonostante l'esperienza maturata in relazione all'adozione della decisione di adeguatezza relativa al Regno Unito contribuirà a preparare il terreno per iniziative analoghe negli anni a venire. Nel contesto della sua strategia internazionale, la Commissione esaminerà altri possibili candidati per future decisioni di adeguatezza ai sensi della LED e procederà in tal senso operando in contatto diretto con le altre istituzioni e gli altri organi competenti dell'UE[154]. A tal fine, e conformemente al considerando 68 LED, la Commissione presterà particolare attenzione agli impegni internazionali dei paesi valutati in relazione alla protezione dei dati personali, compresa l'adesione ai summenzionati accordi multilaterali o ad altri strumenti di contrasto che prevedano garanzie adeguate di protezione dei dati.

3.5.2 Garanzie adeguate

La LED contiene altri strumenti di trasferimento oltre alla soluzione complessiva di una decisione di adeguatezza. La flessibilità di tale "pacchetto di strumenti" si rispecchia nell'articolo 37 LED, che disciplina i trasferimenti di dati sulla base di "garanzie adeguate" per quanto concerne la protezione dei dati personali. Tali garanzie adeguate possono essere fornite da uno strumento giuridicamente vincolante, oppure quando il titolare del trattamento, sulla base di una valutazione di tutte le circostanze relative al trasferimento, conclude che esistono garanzie adeguate (la cosiddetta "autovalutazione" per i trasferimenti).

Nei primi anni di applicazione della LED, la Commissione ha lavorato in particolare a strumenti giuridici vincolanti sotto forma di accordi internazionali capaci di fornire garanzie adeguate. Tali accordi svolgono un ruolo importante tanto nel contesto della cooperazione "tradizionale" (ossia la cooperazione tra autorità competenti) quanto in altre forme di cooperazione in materia di contrasto (ossia la cooperazione che coinvolge terzi quali imprese private). Possono fungere altresì da base per i trasferimenti di dati da parte di Europol ed Eurojust nel contesto dei rispettivi quadri giuridici le cui norme in materia di trasferimenti internazionali sono molto simili a quelle previste dalla LED.

Per quanto riguarda le forme tradizionali di cooperazione in materia di contrasto, la Commissione sta riesaminando gli accordi internazionali adottati prima dell'entrata in vigore della LED al fine di garantirne la coerenza con il regime modernizzato dell'UE in materia di protezione dei dati[155].

---

[154] Posizione e conclusioni del Consiglio in merito all'applicazione della LED, punto 18.

[155] Nella sua comunicazione "Via da seguire per allineare l'acquis dell'ex terzo pilastro alle norme sulla protezione dei dati", la Commissione ha concluso che diversi accordi esistenti non richiedono un ulteriore allineamento con la LED (ad esempio l'accordo tra l'Unione europea e la Repubblica d'Islanda e il Regno di Norvegia sull'applicazione di talune

Innanzitutto la Commissione sta valutando le disposizioni in materia di protezione dei dati contenute negli accordi di cooperazione esistenti tra Europol[156] e paesi terzi conclusi prima del 1° maggio 2017, come previsto dal regolamento (UE) 2016/794 sull'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (di seguito il "regolamento Europol")[157]. Conformemente all'articolo 9 del protocollo n. 36 del trattato sull'Unione europea[158] e del TFUE (sulle disposizioni transitorie), gli effetti giuridici di tali accordi sono stati preservati finché questi non siano stati abrogati, annullati o modificati[159]. La Commissione informerà il Parlamento europeo e il Consiglio in merito all'esito di tale valutazione e, se del caso, presenterà al Consiglio una raccomandazione di decisione che autorizzi l'avvio di negoziati per modificare l'accordo o gli accordi corrispondenti a norma dell'articolo 218 TFUE. Si tratta di un compito complesso che prevede la valutazione di 18 accordi ed è stato ritardato dalle perturbazioni causate dalla pandemia di COVID-19. La Commissione prevede di completare la propria valutazione nella seconda metà del 2022.

La coerenza di tutti i meccanismi di cooperazione in materia di contrasto rispetto alle norme sancite dalla LED è un principio guida che la Commissione segue anche quando negozia nuovi accordi per il trasferimento di dati personali da parte di Europol verso paesi terzi od organizzazioni internazionali. Da quando l'attuale regolamento Europol è entrato in vigore nel 2017, l'articolo 218 TFUE ha costituito la base giuridica per tali accordi internazionali che assicurano garanzie adeguate. Nel 2018 e nel 2019 il Consiglio ha adottato nove mandati affinché la Commissione potesse avviare negoziati con paesi terzi a nome dell'Unione. La Commissione è stata inoltre autorizzata ad avviare negoziati in merito a un accordo di cooperazione con Interpol concernente lo scambio di dati con svariati organi e agenzie dell'UE. In tutti questi casi, il Consiglio ha indirizzato alla Commissione direttive di negoziato al fine di garantire che siano incluse le garanzie necessarie per la protezione dei dati personali e di altri diritti e libertà fondamentali delle persone fisiche. Su questa base la Commissione ha già concluso i negoziati con la Nuova Zelanda, che hanno portato alla firma di un accordo di cooperazione in data 30 giugno 2022]. Inoltre sono stati compiuti progressi nei negoziati con Israele. Per quanto concerne la Turchia, i negoziati sono in una fase avanzata, ma non possono essere conclusi finché la Turchia non adotterà le necessarie riforme della propria legislazione in materia di protezione dei dati. Autorizzazioni analoghe sono state concesse nel marzo del 2021 per la negoziazione di accordi di cooperazione volti a consentire lo scambio di dati da parte di Eurojust con 13 paesi terzi.

---

disposizioni della convenzione del 29 maggio 2000 relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea e del relativo protocollo del 2001).

[156] Per maggiori informazioni sugli accordi Europol esistenti, consultare il sito web dell'Agenzia all'indirizzo: https://www.europol.europa.eu/partners-collaboration/agreements.

[157] Cfr. articolo 25, paragrafo 4, del regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI (GU L 135 del 24.5.2016, pag. 53).

[158] Versione consolidata del trattato sull'Unione europea (GU C 202 del 7.6.2016, pag. 13), disponibile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A02016M%2FTXT-20200301.

[159] Considerando 35 del regolamento Europol.

In secondo luogo la Commissione sta conducendo il primo riesame congiunto dell'accordo tra gli Stati Uniti d'America e l'Unione europea sulla protezione delle informazioni personali a fini di prevenzione, indagine, accertamento e perseguimento di reati ("accordo quadro"). L'accordo quadro, entrato in vigore nel febbraio del 2017, contiene un insieme completo e armonizzato di norme in materia di protezione dei dati che si applicano a tutti gli scambi transatlantici tra autorità competenti. Integra gli accordi esistenti tra l'UE e gli Stati Uniti e tra gli Stati membri dell'UE e gli Stati Uniti tra autorità di contrasto, stabilisce un livello elevato di protezione per accordi futuri in questo settore e rafforza la cooperazione per finalità di contrasto facilitando lo scambio di informazioni. Il riesame congiunto mira a valutare l'attuazione efficace dell'accordo quadro, in particolare per quanto concerne le disposizioni sul trasferimento successivo, sui diritti individuali e sul ricorso in sede giudiziaria. La tempistica per il riesame congiunto è stata influenzata dalle perturbazioni legate alla pandemia di COVID-19, nonché dai negoziati paralleli sul secondo protocollo addizionale alla convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica[160]. La Commissione prevede che tale attività sarà completata nella seconda metà del 2022.

Trattandosi del primo accordo internazionale bilaterale che prevede un catalogo completo di diritti e obblighi in materia di protezione dei dati, l'accordo quadro costituisce un punto di riferimento per la negoziazione di accordi quadro analoghi con i principali partner incaricati dello svolgimento di attività di contrasto in materia penale[161]. A tal fine la Commissione terrà conto anche degli sviluppi pertinenti, comprese le linee guida dell'EDPB, la giurisprudenza della Corte e l'esito dei negoziati internazionali sulle garanzie in materia di protezione dei dati in questo settore (quali ad esempio il secondo protocollo addizionale alla convenzione di Budapest sulla criminalità informatica o l'accordo di Europol con la Nuova Zelanda[162]).

In terzo luogo la Commissione ha individuato nell'accordo tra l'Unione europea e il Giappone relativo all'assistenza giudiziaria in materia penale (il "trattato di mutua assistenza giudiziaria UE-Giappone")[163] un atto dell'UE che disciplina il trattamento dei dati (trasferimenti) per finalità di contrasto in materia penale che deve essere modificato per assicurare l'esistenza di garanzie adeguate in materia di protezione dei dati in linea con la LED. A seguito dell'adozione da parte del Consiglio di una decisione[164] che autorizza l'avvio di negoziati per modificare il trattato di mutua

---

[160] La Commissione, a nome dell'Unione europea, e gli Stati Uniti si sono impegnati notevolmente in questi negoziati, anche nel contesto del sottogruppo dedicato alla protezione dei dati (essendo tale argomento uno di quelli maggiormente discussi).

[161] Cfr. comunicazione della Commissione al Parlamento europeo e al Consiglio, Scambio e protezione dei dati personali in un mondo globalizzato (COM(2017) 7 final), pag. 16.

[162] Accordo tra l'Unione europea, da una parte, e la Nuova Zelanda, dall'altra, sullo scambio di dati personali tra l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e le autorità neozelandesi competenti per la lotta contro le forme gravi di criminalità e il terrorismo.

[163] Accordo tra l'Unione europea e il Giappone relativo all'assistenza giudiziaria in materia penale (GU L 39 del 12.2.2010, pag. 20) - https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A22010A0212(01).

[164] Decisione del Consiglio che autorizza l'avvio di negoziati per modificare l'accordo tra l'Unione europea e il Giappone sull'assistenza giudiziaria reciproca in materia penale (solo in EN) (documento LT 223/21).

assistenza giudiziaria UE-Giappone, la Commissione continua a dialogare con le autorità giapponesi al fine di iniziare i negoziati il prima possibile.

Inoltre ora si fa sempre più affidamento anche su altre forme di cooperazione adattate alle sfide e alle esigenze specifiche delle indagini penali nell'economia digitale odierna. Si tratta principalmente di una cooperazione rafforzata nel settore della cibercriminalità e per la raccolta di prove in formato elettronico relative a reati. Tale cooperazione comprende la cooperazione diretta con soggetti privati per l'accesso a prove elettroniche.

La Commissione si è inoltre impegnata con partner internazionali al fine di garantire che tali altre forme (importanti) di cooperazione possano aver luogo sulla base di garanzie adeguate in materia di protezione dei dati.

Innanzitutto la Commissione ha rappresentato l'UE durante i negoziati[165] nel contesto del secondo protocollo addizionale alla convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica[166].Il protocollo, approvato dal Comitato dei ministri del Consiglio d'Europa il 17 novembre 2021, contempla garanzie solide in relazione alla protezione dei diritti fondamentali, nonché un articolo[167] contenente disposizioni dettagliate sulla protezione dei dati personali trasferiti ai sensi del protocollo. Tali disposizioni riguardano tutti i principi, i diritti e gli obblighi essenziali in materia di protezione dei dati riconosciuti dal diritto dell'Unione. Tali garanzie sono integrate da una disposizione in materia di controllo e dalla possibilità di sospendere i trasferimenti in caso di violazione sistematica o sostanziale delle garanzie contenute nel protocollo, ad esempio in assenza di ricorsi giurisdizionali effettivi. Attraverso tali disposizioni, fornisce garanzie adeguate in linea con i requisiti dell'articolo 37, paragrafo 1, lettera a), LED[168]. Si tratta di un risultato significativo, data la varietà delle parti che hanno aderito alla convenzione di Budapest, che attualmente conta 66 Stati parti che rappresentano tradizioni e contesti giuridici diversi. Consentirà alle autorità competenti degli Stati membri di beneficiare di una cooperazione transfrontaliera efficace nella lotta alla cibercriminalità, garantendo nel contempo il rispetto dei valori dell'UE come rispecchiati nella Carta dei diritti fondamentali dell'Unione europea, nei trattati dell'UE e nel diritto derivato dell'UE. In considerazione del numero elevato di parti aderenti

[165] A seguito dell'approvazione del 6 giugno 2019 di un mandato da parte del Consiglio dell'Unione europea. Tale mandato è disponibile all'indirizzo: https://www.consilium.europa.eu/it/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/.

[166] Il 17 novembre 2021 il Comitato dei ministri del Consiglio d'Europa ha approvato il secondo protocollo addizionale alla convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche. Tale documento è stato preparato dal comitato per la convenzione sulla criminalità informatica (T-CY) tra il settembre del 2017 e il maggio del 2021. Il testo del protocollo (copia autenticata) è disponibile (solo in EN e FR) all'indirizzo: https://rm.coe.int/1680a4b2e1. La relazione esplicativa del protocollo è inoltre disponibile (solo in EN) all'indirizzo: https://rm.coe.int/1680a49c9d.

[167] Cfr. articolo 14 del protocollo addizionale, unitamente ai punti da 220 a 287 della relazione esplicativa.

[168] Nel suo parere 1/2022, del 20 gennaio 2022, sul progetto di decisioni del Consiglio che autorizzano la firma e la ratifica del protocollo addizionale, il garante europeo della protezione dei dati (GEPD) constata con favore le numerose garanzie che sono state incluse nel protocollo.

alla convenzione di Budapest, che attualmente comprende paesi di tutto il mondo, il protocollo contribuirà altresì alla promozione di livelli elevati di protezione dei dati per il trattamento di dati nel settore delle attività di contrasto in materia penale a livello globale. Il protocollo è stato aperto alla firma il 12 maggio 2022 e complessivamente sono 22 le parti della convenzione di Budapest (compresi 13 Stati membri dell'UE) che lo hanno già firmato.

In secondo luogo la Commissione ha avviato negoziati in merito a un accordo bilaterale con gli Stati Uniti sull'accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale[169]. Tale accordo mira a trattare le prove elettroniche sotto forma di dati tanto non personali quanto personali, compresi i dati sul traffico e sui contenuti. È importante sottolineare che i negoziati mirano altresì all'inclusione di ulteriori garanzie in materia di protezione dei dati che integrino quelle di cui all'accordo quadro, tenendo conto, in particolare, della natura sensibile delle categorie di dati interessate nonché dei requisiti del trasferimento di prove elettroniche direttamente dai prestatori di servizi. I progressi nel contesto di tali negoziati dipenderanno in gran parte da quelli concernenti il processo legislativo in corso sul pacchetto dell'UE in materia di prove elettroniche[170].

Queste svariate iniziative della Commissione destinate a sviluppare strumenti internazionali che facilitino la cooperazione con partner internazionali in materia di contrasto, garantendo nel contempo garanzie adeguate per la protezione dei dati, sono state sostenute dal lavoro dell'EDPB e del GEPD. Rientrano nel contesto di tale lavoro la dichiarazione dell'EDPB sul progetto di secondo protocollo addizionale alla convenzione di Budapest[171] e i pareri del GEPD sul progetto di mandati negoziali per accordi internazionali ai sensi dell'articolo 218 TFUE che consentirebbe a Europol ed Eurojust di scambiare dati personali con paesi terzi od organizzazioni internazionali[172]. L'EDPB ha inoltre rilasciato una dichiarazione nella quale invita gli Stati membri a valutare e, ove necessario, riesaminare gli accordi internazionali che comportano trasferimenti

[169] Decisione del Consiglio che autorizza l'avvio di negoziati in vista della conclusione 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. Il mandato è disponibile all'indirizzo seguente: https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/it/pdf.

[170] 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) e 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).

[171] EDPB, Dichiarazione 2/2021 sul nuovo progetto di disposizioni del secondo protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica (convenzione di Budapest), adottata il 2 febbraio 2021, disponibile all'indirizzo: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_it.

[172] GEPD, Parere 04/2021 sul riesame del mandato di Europol, adottato l'8 marzo 2021, disponibile all'indirizzo (non disponibile in IT): https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-amendment-europol-regulation_en.

internazionali di dati personali[173]. Tale dichiarazione riguarda gli accordi conclusi prima del 6 maggio 2016, anche nel settore delle attività di contrasto in materia penale, e invita gli Stati membri a stabilire se sia necessario un ulteriore allineamento con la legislazione e la giurisprudenza dell'UE in materia di protezione dei dati.

L'articolo 37 LED consente altresì trasferimenti internazionali di dati sulla base di un'autovalutazione da parte di un'autorità competente in merito al fatto che un paese terzo (o un'organizzazione internazionale) disponga o meno di garanzie adeguate in materia di protezione dei dati. In tali casi l'autorità deve documentare il trasferimento (compresi data e ora, informazioni sull'autorità ricevente, motivazione del trasferimento e dati personali trasferiti) e tale documentazione deve essere messa a disposizione dell'autorità di controllo su richiesta (articolo 37 (3) LED). Il riscontro fornito dagli Stati membri[174] indica che tale strumento è stato utilizzato raramente.

Per consentire agli Stati membri di utilizzare appieno gli strumenti in materia di trasferimento della LED, è importante che l'EDPB intensifichi il lavoro in corso sui vari meccanismi di trasferimento. Tra l'altro, l'EDPB dovrebbe fornire linee guida sui meccanismi inclusi nell'articolo 37, paragrafo 1, LED, in particolare sui trasferimenti basati su autovalutazioni da parte delle autorità competenti. Anche il Consiglio ha sottolineato tale necessità[175].

3.5.3 Ricorso a deroghe

Infine le cosiddette "deroghe" costituiscono un motivo importante per i trasferimenti a determinate condizioni, di cui all'articolo 38 LED. Tali condizioni stabiliscono un equilibrio tra le considerazioni in materia di tutela della vita privata e le esigenze operative delle autorità competenti. In particolare, l'articolo 38, paragrafo 1, consente i trasferimenti, o persino categorie di trasferimenti, di dati personali, laddove ciò sia necessario per prevenire una minaccia grave e immediata alla sicurezza pubblica[176] o, nei singoli casi, a fini di prevenzione, indagine, accertamento e perseguimento di reati[177]. Contrariamente alle deroghe ai sensi dell'articolo 49 GDPR, attualmente non esistono linee guida per le deroghe ai sensi dell'articolo 38 LED.

---

[173] EDPB, Dichiarazione 4/2021 sugli accordi internazionali, compresi i trasferimenti, adottata il 13 aprile 2021, disponibile all'indirizzo: https://edpb.europa.eu/system/files/2022-05/edpb_statement042021_international_agreements_including_transfers_it_0.pdf.

[174] Cfr. relazione della presidenza del Consiglio sullo scambio di dati di polizia con paesi terzi - Esperienze nell'applicazione dell'articolo 37 della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie. L'EDPB ha annunciato che includerà le conclusioni della relazione della presidenza, oltre ad altre informazioni e osservazioni degli Stati membri, nei suoi sforzi intesi a elaborare orientamenti in merito all'articolo 37 della direttiva. Cfr. lettera del presidente dell'EDPB alla rappresentanza permanente della Repubblica federale di Germania presso l'Unione europea del 26 febbraio 2021 (documento 13555/1/20).

[175] Cfr. posizione e conclusioni del Consiglio in merito all'applicazione della LED, punto 20.

[176] Articolo 38, paragrafo 1, lettera c), LED.

[177] Articolo 38, paragrafo 1, lettera d), LED.

3.5.4 Cooperazione giudiziaria e di polizia efficace a livello transfrontaliero

La LED è diventata un punto di riferimento internazionale per la protezione dei dati nel contesto delle attività di contrasto ed ha agito da catalizzatore per i paesi di tutto il mondo spingendoli a prendere in considerazione l'introduzione di norme moderne in materia di tutela della vita privata in questo settore. Si tratta di uno sviluppo molto positivo che offre nuove opportunità per proteggere meglio le persone fisiche nell'UE quando i loro dati vengono trasferiti all'estero per finalità di contrasto, facilitando allo stesso tempo i flussi di dati che possono contribuire a combattere la criminalità.

Più in generale è importante garantire che, se invitate a condividere dati per finalità di contrasto sulla base di richieste dirette di cooperazione, le imprese attive nel mercato europeo possano farlo senza dover affrontare conflitti di legge e nel pieno rispetto dei diritti fondamentali dell'UE[178]. Al fine di migliorare tali trasferimenti, 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.

In questo contesto, la Commissione si è impegnata in contesti bilaterali, regionali e multilaterali al fine di promuovere attivamente la convergenza internazionale delle norme in materia di protezione dei dati per la cooperazione nel contesto di attività di contrasto in materia penale. Durante i dialoghi con diversi paesi partner esteri sulle riforme in corso delle leggi sulla protezione dei dati, i servizi della Commissione hanno profuso sforzi in diversi modi (ad esempio comunicazioni in risposta a consultazioni pubbliche, partecipazione ad audizioni parlamentari e incontri dedicati con rappresentanti di governo e responsabili delle politiche) in merito all'elaborazione di norme sul trattamento di dati personali da parte di autorità competenti.

In un contesto regionale e multilaterale, la Commissione sostiene ad esempio progetti di sviluppo di capacità nel contesto dell'attuazione della convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica[179]. Tra tali progetti figura il programma GLACY+ destinato a rafforzare la capacità degli Stati di applicare la legislazione in materia di cibercriminalità e a rafforzare la loro capacità di cooperare in maniera efficace a livello internazionale in linea con la convenzione di Budapest e i suoi protocolli addizionali. Ciò comporta altresì lo sviluppo di una legislazione in materia di protezione dei dati per il trattamento di dati in questo settore. Il programma sostiene attualmente 17 paesi prioritari e hub in Africa, nella regione Asia-Pacifico, così come nella regione America latina e Caraibi.

La Commissione ha inoltre interagito con Ameripol, un'organizzazione di cooperazione di polizia che riunisce 18 paesi dell'America latina, nel contesto dello sviluppo di un quadro di protezione

[178] A titolo di esempio il secondo protocollo addizionale alla convenzione di Budapest potrebbe essere considerato un accordo internazionale ai fini dell'articolo 48 GDPR.
[179] Cfr.: https://www.coe.int/en/web/cybercrime/glacyplus.

dei dati per lo scambio di informazioni tra Ameripol e i suoi Stati membri. Tale attività avviene nel contesto del progetto "*EL PAcCTO: Support to Ameripol*" che mira a migliorare il livello di cooperazione internazionale tra le forze di polizia, la magistratura e le procure dei paesi partner nella lotta contro la criminalità organizzata.

La Commissione promuove inoltre la convenzione 108 modernizzata (nota come convenzione 108+)[180], applicabile anche alle attività di trattamento di dati per finalità di contrasto in materia penale. Tale convenzione, aperta anche ai non membri del Consiglio d'Europa, è importante non soltanto perché è l'unico accordo vincolante multilaterale in materia di protezione dei dati, ma anche perché attraverso il suo comitato della convenzione mette a disposizione un consesso per lo scambio delle migliori prassi e la definizione di norme globali[181]. Nel contesto della sua strategia internazionale sui flussi di dati, la Commissione incoraggia l'adesione di paesi terzi alla Convenzione 108+.

Infine, la Commissione incoraggia una maggiore convergenza a livello internazionale condividendo la nostra esperienza con i partner sugli aspetti relativi alla protezione dei dati della cooperazione nel settore delle attività di contrasto in materia penale. L'"Accademia sulla protezione dei dati" della Commissione, che costituisce parte del progetto "*International Digital Cooperation - Enhanced Data Protection and Data Flows*", finanziato dallo strumento di politica estera, è uno strumento chiave nel contesto di tale sforzo. L'Accademia è stata istituita per favorire gli scambi tra le autorità di regolamentazione europee e di paesi terzi e per migliorare la cooperazione sul campo. Le attività dell'Accademia trattano tutti gli aspetti del controllo in materia di protezione dei dati, anche nel settore delle attività di contrasto.

4 PROSSIME TAPPE

Al fine di garantire un'efficace politica di sicurezza dell'UE che rispetti pienamente il diritto fondamentale alla protezione dei dati personali, la Commissione continuerà a verificare che gli Stati membri abbiano recepito correttamente la LED nonché a monitorare l'applicazione delle sue disposizioni.

La LED ha contribuito in modo significativo a un livello più armonizzato e più elevato di protezione dei diritti delle persone fisiche e a un quadro giuridico più coerente per le autorità competenti.

---

[180] Protocollo che modifica la Convenzione sulla protezione delle persone rispetto al trattamento di dati a carattere personale, adottato dal Comitato dei ministri nella sua 128ª sessione tenutasi a Elsinora il 18 maggio 2018 (Convenzione 108+), disponibile all'indirizzo (solo in EN): https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[181] Cfr. ad esempio Guida pratica sull'uso dei dati personali nel settore delle forze di polizia, disponibile (solo in EN) all'indirizzo https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5.

In generale la LED è stata recepita in modo soddisfacente, ma sono state individuate diverse questioni. La Commissione ha già avviato procedure di infrazione per quanto concerne tanto il mancato recepimento quanto la non conformità delle legislazioni nazionali rispetto alla LED e continuerà a lavorare per garantire il pieno e corretto recepimento di tale atto.

La LED ha prodotto un livello più elevato di consapevolezza e attenzione rispetto alla protezione dei dati da parte delle autorità nazionali competenti, anche per quanto riguarda la sicurezza del trattamento.

Il controllo attivo svolto dalle autorità di controllo della protezione dei dati è fondamentale per garantire che gli obiettivi della LED siano conseguiti nella pratica. Occorre quindi conferire alle autorità tutti i tipi di poteri richiesti dalla LED, unitamente a risorse adeguate.

In questa fase, l'obiettivo dovrebbe essere quello di realizzare il pieno potenziale della LED. In questo contesto, e in considerazione della limitata esperienza acquisita in relazione a queste nuove regole, la Commissione ritiene che sia troppo presto per prendere in considerazione una revisione della LED.

La Commissione continuerà a collaborare attivamente con tutti i soggetti interessati nella prospettiva in vista della prossima valutazione prevista entro il 2026. Nel frattempo continuerà a lavorare per garantire la coerenza con altre normative dell'UE pertinenti al trattamento dei dati personali per finalità di contrasto in materia penale.

Quadro giuridico

La Commissione:

- continuerà a valutare il recepimento della LED da parte degli Stati membri e ad adottare misure adeguate ove necessario (compreso l'avvio di procedure di infrazione);
- continuerà a portare avanti gli scambi bilaterali con gli Stati membri;
- garantirà che le future proposte legislative siano coerenti con la LED.

Gli Stati membri dovrebbero:

- garantire il pieno e corretto recepimento della LED a livello nazionale, anche specificando i requisiti necessari di tale direttiva laddove le leggi nazionali in materia di protezione dei dati che recepiscono la LED non vi provvedano.

Controllo esercitato dalle autorità di controllo della protezione dei dati

Gli Stati membri dovrebbero:

- fornire alle autorità di controllo della protezione dei dati risorse sufficienti per svolgere i loro compiti di applicazione della LED;
- garantire che le autorità di controllo della protezione dei dati possano esercitare tutti i tipi di poteri previsti dalla LED;
- consultare sistematicamente le proprie autorità di controllo della protezione dei dati in merito a progetti di misure legislative ed amministrative di applicazione generale relativi alla

protezione di dati personali, nonché tenere debitamente conto dei loro pareri (in particolare nel caso di tecnologie nuove).

Le autorità di controllo della protezione dei dati sono invitate a:

- fare pieno uso dei propri poteri d'indagine, anche svolgendo ispezioni di propria iniziativa;
- raccogliere statistiche specifiche relative alle proprie attività di controllo nel contesto della LED;
- avvalersi degli strumenti di assistenza reciproca e sviluppare misure pratiche destinate a facilitare le richieste di assistenza, anche attraverso le linee guida previste dell'EDPB.

L'EDPB è invitato a:

- espandere il gruppo di esperti di sostegno[182] per i compiti relativi alla LED.

Sostegno a favore delle autorità competenti

La Commissione:

- faciliterà le discussioni e la condivisione di esperienze tra gli Stati membri e la Commissione in seno al gruppo di esperti degli Stati membri relativo alla LED;
- faciliterà lo scambio di opinioni tra i responsabili della protezione dei dati attraverso la rete a loro dedicata.

Gli Stati membri sono invitati a:

- proseguire gli sforzi destinati a fornire alle autorità competenti formazione sui requisiti in materia di protezione dei dati, anche in relazione alle nuove tecnologie.

L'EDPB e le autorità di controllo della protezione dei dati sono invitati a:

- rafforzare i propri sforzi volti all'adozione di linee guida pertinenti (ad esempio sul ruolo del consenso nel contesto del trattamento di dati personali per finalità di contrasto in materia penale e sui diritti degli interessati, comprese le loro eventuali limitazioni), adottando nuove linee guida autonome o integrando quelle già adottate per il GDPR.

Trasferimenti transfrontalieri di dati

La Commissione intende:

- promuovere attivamente possibili nuove decisioni di adeguatezza con i principali partner internazionali;
- negoziare nuovi accordi di cooperazione tra Europol ed Eurojust, da un lato, e paesi terzi, dall'altro. Ove necessario, cercherà di rinegoziare gli accordi di cooperazione di Europol esistenti per assicurare che contemplino garanzie adeguate in materia di protezione dei dati;

[182] EDPB, Documento sul quadro di riferimento del gruppo di esperti di sostegno dell'EDPB, adottato il 15 dicembre 2020 (solo in EN).

- avviare negoziati con il Giappone al fine di modificare l'accordo esistente di mutua assistenza giudiziaria UE-Giappone per assicurare che contempli garanzie adeguate in materia di protezione dei dati;
- perseguire e concludere la negoziazione di un accordo bilaterale con gli Stati Uniti sull'accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale, anche integrando le garanzie in materia di protezione dei dati assicurate dall'accordo quadro UE-USA al fine di rispecchiare il contesto specifico di cooperazione tra autorità di contrasto e prestatori di servizi;
- esaminare la possibilità di concludere accordi quadro in materia di protezione dei dati per il trattamento di dati nel settore delle attività di contrasto in materia penale con i principali partner incaricati dello svolgimento di attività di contrasto in materia penale, basandosi sull'esempio dell'accordo quadro UE-USA.

L'EDPB è invitato a:

- adottare linee guida al fine di chiarire ulteriormente la nozione e il contenuto di "garanzie adeguate" (articolo 37 LED) nonché il ricorso a deroghe (articolo 38 LED).

Promozione della convergenza e sviluppo della cooperazione internazionale

La Commissione:

- amplierà la portata del proprio impegno con i partner internazionali al fine di rafforzare la convergenza delle norme in materia di protezione dei dati nel settore delle attività di contrasto in materia penale, anche promuovendo l'adesione alla convenzione 108+ come unico accordo globale vincolante in materia di protezione dei dati;
- promuoverà la cooperazione bilaterale, regionale e multilaterale e sosterrà progetti di sviluppo di capacità nel settore della protezione dei dati e della cooperazione di polizia. Rientreranno in tale contesto la formazione e lo scambio di conoscenze e migliori prassi attraverso l'Accademia sulla protezione dei dati.

Gli Stati membri sono invitati a:

- ratificare rapidamente il secondo protocollo addizionale alla convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, non appena siano autorizzati a farlo da una decisione del Consiglio.