Parere 14/2021 relativo al progetto di decisione di esecuzione della Commissione europea a norma del regolamento (UE) 2016/679 sull'adeguata protezione dei dati personali nel Regno Unito

Adottato il 13 aprile 2021

INDICE

Il comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettera s), del 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, di seguito "GDPR"),

visto l'accordo sullo Spazio economico europeo (di seguito "SEE") e in particolare l'allegato XI e il protocollo 37, come modificati dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti gli articoli 12 e 22 del suo regolamento,

HA ADOTTATO IL SEGUENTE PARERE:

1. SINTESI

1. La Commissione europea ha approvato il suo progetto di decisione di esecuzione (di seguito "progetto di decisione") sull'adeguata protezione dei dati personali da parte del Regno Unito (di seguito "Regno Unito") a norma del GDPR del 19 febbraio 2021[2]. A seguito di ciò, la Commissione europea ha avviato la procedura di adozione formale.

2. Nella stessa data, la Commissione europea ha chiesto il parere del comitato europeo per la protezione dei dati (di seguito "EDPB")[3]. L'EDPB ha valutato l'adeguatezza del livello di protezione garantito nel Regno Unito sulla base di un esame del progetto stesso di decisione, nonché sulla base di un'analisi della documentazione messa a disposizione dalla Commissione europea.

3. L'EDPB ha concentrato la propria attenzione sulla valutazione sia degli aspetti generali relativi al GDPR nel progetto di decisione sia sull'accesso da parte delle autorità pubbliche ai dati personali trasferiti dal SEE ai fini di contrasto e di sicurezza nazionale, tra cui i rimedi giuridici a disposizione degli interessati nel SEE. L'EDPB ha valutato anche la presenza ed efficacia delle garanzie previste dal quadro giuridico del Regno Unito.

4. L'EDPB ha utilizzato quale principale parametro per la propria attività i Criteri di riferimento per l'adeguatezza[4], adottati nel febbraio 2018, e le Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza[5].

[1] Nel presente parere con il termine "Stati membri" si intendono gli "Stati membri del SEE".
[2] Vedere il comunicato stampa della Commissione europea, Protezione dei dati: la Commissione europea avvia un processo sui flussi di dati personali verso il Regno Unito, 19 febbraio 2021, https://ec.europa.eu/commission/presscorner/detail/it/ip_21_661.
[3] Ibidem.
[4] Vedere Gruppo di lavoro "Articolo 29", Criteri di riferimento per l'adeguatezza, adottati il 28 novembre 2017, ultima revisione e adozione il 6 febbraio 2018, WP254 rev.01 (approvati dall'EDPB, cfr. https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines); (di seguito "*Criteri di riferimento per l'adeguatezza*").
[5] Cfr. Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza dell'EDPB, adottate il 10 novembre 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_it.

1.1. Settori di convergenza

5. Il principale obiettivo dell'EDPB è esprimere alla Commissione europea un parere sull'adeguatezza del livello di protezione offerto agli interessati nel Regno Unito. È importante riconoscere che l'EDPB non si aspetta che il quadro giuridico del Regno Unito replichi la normativa europea sulla protezione dei dati.

6. Tuttavia, l'EDPB ricorda che, affinché si possa ritenere adeguato il livello di protezione offerto, l'articolo 45 del GDPR e la giurisprudenza della Corte di giustizia dell'Unione europea (di seguito "Corte") impongono che la legislazione del paese terzo sia allineata con l'essenza dei principi fondamentali sanciti nel GDPR. Il quadro giuridico del Regno Unito in materia di protezione dei dati è in gran parte basato sul quadro giuridico di protezione dei dati personali dell'Unione europea (in particolare il GDPR e la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, di seguito "direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie" o "LED") in quanto il Regno Unito è stato uno Stato membro dell'Unione europea fino al 31 gennaio 2020. Inoltre, la legge Data Protection Act 2018 del Regno Unito, che è entrata in vigore il 23 maggio 2018 e che ha abrogato la legge Data Protection Act 1998 del Regno Unito, specifica ulteriormente che nel diritto del Regno Unito si applica il GDPR, oltre a recepire la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie dell'UE e a conferire poteri e imporre obblighi all'autorità nazionale di controllo della protezione dei dati, l'Information Commissioner's Office del Regno Unito (di seguito "ICO"). Per questo motivo l'EDPB riconosce che il Regno Unito ha in gran parte incorporato il GDPR nel proprio quadro giuridico in materia di protezione dei dati.

7. **Analizzando la normativa e le pratiche di un paese terzo che è stato membro dell'Unione europea fino a poco tempo fa, evidentemente l'EDPB ha individuato molti elementi di equivalenza sostanziale.**

8. Nel campo della protezione dei dati, l'EDPB osserva un forte allineamento tra il quadro giuridico del GDPR e il quadro giuridico del Regno Unito per quanto concerne alcune disposizioni fondamentali come, ad esempio, i concetti di base ("dati personali"; "trattamento dei dati personali"; "titolare del trattamento"); criteri di liceità e correttezza del trattamento per finalità legittime; limitazione delle finalità; qualità e proporzionalità dei dati; conservazione, sicurezza e riservatezza dei dati; trasparenza; categorie particolari di dati; marketing diretto; processi decisionali automatizzati e profilazione.

1.2. Aspetti problematici

9. Fino a poco tempo fa il Regno Unito è stato uno Stato membro dell'UE; per questo motivo, nell'analizzare le sue norme e le sue pratiche, l'EDPB ha individuato molti elementi di equivalenza sostanziale. Al contempo, alla luce del suo ruolo nel processo di determinazione dell'adeguatezza, ma anche alla luce delle limitazioni di tempo, l'EDPB ha deciso di concentrare la propria attenzione sugli aspetti in cui ritiene vi sia un'esigenza di più attento esame e analisi più approfondita.

10. Permangono tuttavia aspetti problematici e l'EDPB ritiene che gli elementi che seguono debbano essere ulteriormente valutati al fine di accertare la sostanziale equivalenza del livello di protezione offerto, e che essi debbano essere oggetto di attenta osservazione nel Regno Unito da parte della Commissione europea.

1.2.1. Aspetti generali

11. La prima problematica, di natura generale, riguarda l'osservazione dell'evoluzione del sistema giuridico del Regno Unito in materia di protezione dei dati nel suo insieme. Infatti, il governo del Regno Unito ha manifestato l'intenzione di definire politiche distinte e indipendenti in materia di protezione dei dati, eventualmente tese a discostarsi dalla normativa dell'UE in materia di protezione dei dati. A queste dichiarazioni politiche non sono seguiti ancora atti concreti nel quadro giuridico del Regno Unito. Tuttavia, in futuro questa possibile **divergenza potrebbe mettere a rischio il mantenimento del livello di protezione previsto per i dati personali trasferiti dall'UE. Per questo motivo, la Commissione europea è invitata a osservare attentamente tali evoluzioni sin dall'entrata in vigore della sua decisione di adeguatezza e ad adottare le azioni necessarie, eventualmente anche modificando e/o sospendendo la decisione se necessario.**

1.2.2. Aspetti generali relativi alla protezione dei dati

12. In primo luogo, la cosiddetta "**esenzione per motivi di immigrazione**", prevista **dall'allegato 2 della legge Data Protection Act 2018, parte 1**, paragrafo 4, **presenta una formulazione "ampia"**. In particolare, essa si applica nel caso in cui i dati personali non siano raccolti per finalità di controllo dell'immigrazione da parte di un titolare del trattamento, ma siano messi da questo a disposizione di un altro titolare del trattamento che elabora i dati personali ai fini del controllo dell'immigrazione.

13. L'EDPB invita la Commissione europea a verificare l'avanzamento del procedimento *Open Rights Group & Anor, R (On the Application Of) contro Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* e, poiché questa sentenza non è definitiva (*res judicata*), a verificare se essa sarà confermata o rivista da una sentenza d'appello, tenendo conto di eventuali aggiornamenti al riguardo, e specificandolo nella decisione. **L'EDPB invita inoltre la Commissione europea a presentare nella decisione di adeguatezza ulteriori informazioni sull'esenzione per motivi di immigrazione[6], in particolare in relazione alla necessità e alla proporzionalità di questa ampia esenzione prevista nell'ordinamento del Regno Unito, segnatamente per quanto concerne l'esteso ambito di applicazione *ratione personae*.** Al contempo, l'EDPB esorta la Commissione europea a verificare ulteriormente se nel quadro giuridico del Regno Unito esistono o potrebbero essere previste ulteriori garanzie, ad esempio, attraverso strumenti giuridicamente vincolanti a integrazione dell'esenzione per motivi di immigrazione, che ne perfezionino la prevedibilità e le garanzie per gli interessati, consentendo anche un migliore e più rapido esame e monitoraggio dei requisiti di necessità e proporzionalità.

14. In secondo luogo, benché l'EDPB riconosca che il Regno Unito ha incorporato per la maggior parte il capo V del GDPR nel proprio quadro giuridico sulla protezione dei dati, ha individuato alcuni aspetti del quadro giuridico del Regno Unito **relativi ai trasferimenti successivi** che possono pregiudicare il livello di protezione dei dati personali trasferiti dal SEE.

[6] Anche come risultato dell'esame in corso sull'uso dell'esenzione per motivi di immigrazione di cui a pagina 5 dell'Explanatory Framework for Adequacy Discussions del governo del Regno Unito, Section E3: Schedule 2 Restrictions, 13 marzo 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

15. Infatti, l'articolo 44 del GDPR[7] prevede che i trasferimenti e i trasferimenti successivi di dati personali possano avvenire unicamente a condizione che non sia compromesso il livello di protezione delle persone fisiche garantito dal GDPR. **Questo significa che non solo la legislazione del Regno Unito debba essere "sostanzialmente equivalente" alla legislazione UE per quanto concerne il trattamento dei dati personali trasferiti verso il Regno Unito nell'ambito della futura decisione di adeguatezza, ma anche che le regole che si applicano nel Regno Unito ai trasferimenti successivi di questi dati verso paesi terzi debbano assicurare la continuità delle garanzie concernenti un livello di protezione sostanzialmente equivalente.**

16. Pur prendendo atto della possibilità per il Regno Unito di riconoscere territori che offrono un livello adeguato di protezione dei dati secondo il quadro giuridico del Regno Unito in materia di protezione dei dati, l'EDPB desidera sottolineare che questi territori potrebbero non beneficiare al momento di una decisione di adeguatezza della Commissione europea e potrebbero non garantire un livello di protezione "sostanzialmente equivalente" a quello garantito nel SEE. Questo potrebbe determinare rischi per la protezione dei dati personali trasferiti dal SEE, in particolare se, in futuro, il quadro giuridico del Regno Unito in materia di protezione dei dati dovesse discostarsi dall'acquis dell'Unione. Inoltre, il Regno Unito ha già riconosciuto come adeguati i paesi terzi che beneficiano di una decisione di adeguatezza da parte della Commissione europea ai sensi della direttiva 95/46/CE[8], ma la Commissione europea procederà a breve a rivedere queste decisioni, e non sono ancora note le conclusioni di tale revisione.

17. **Per le situazioni di cui sopra, la Commissione dovrebbe adempiere alle funzioni di monitoraggio delle quali è investita, e qualora non sia mantenuto il livello sostanzialmente equivalente di protezione dei dati personali trasferiti dal SEE, dovrebbe valutare una modifica della decisione di adeguatezza al fine di introdurre specifiche garanzie per i dati trasferiti dal SEE e/o la sospensione della decisione di adeguatezza.**

18. **Per quanto concerne gli accordi internazionali conclusi tra il Regno Unito e i paesi terzi,** la Commissione europea è invitata a esaminare l'interazione esistente tra il quadro giuridico del Regno Unito in materia di protezione dei dati e i rispettivi impegni internazionali, oltre all'Accordo sull'accesso ai dati elettronici ai fini della lotta contro le forme gravi di criminalità tra il Regno Unito e gli Stati Uniti d'America (di seguito "Stati Uniti")[9] (di seguito ”Accordo UK-US CLOUD Act”), in particolare al fine di garantire la continuità del livello di protezione nel caso in cui i dati personali siano trasferiti dall'UE al Regno Unito sulla base della decisione di adeguatezza relativa al Regno Unito, e siano successivamente trasferiti verso altri paesi terzi; e a condurre un monitoraggio costante intervenendo, ove necessario, nel caso in cui la conclusione di accordi internazionali tra il

[7] "*Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato*".

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

[9] Cfr. Accordo tra il governo del Regno Unito di Gran Bretagna e Irlanda del Nord e il governo degli Stati Uniti d'America sull'accesso ai dati elettronici ai fini della lotta contro le forme gravi di criminalità, 3 ottobre 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

Regno Unito e paesi terzi rischi di compromettere il livello di protezione dei dati personali previsto nell'UE.

19. Inoltre, la Commissione europea è invitata a monitorare se l'Accordo UK-US CLOUD Act garantisca adeguate ulteriori garanzie, tenuto conto del livello di sensibilità delle categorie di dati interessate e dei requisiti concernenti esclusivamente il trasferimento di prove digitali direttamente da parte di fornitori di servizi anziché tra autorità, valutando anche in quali circostanze si possano prevedere garanzie con un'opportuna applicazione dell'adattamento dell'accordo quadro UE-USA[10].

20. Inoltre, l'EDPB osserva che i trasferimenti successivi possono avvenire a partire dal Regno Unito verso altri paesi terzi sulla base di **strumenti di trasferimento previsti dalla normativa applicabile del Regno Unito sulla protezione dei dati**[11]. Conformemente a *Schrems II*[12], l'EDPB esorta la Commissione europea a fornire nella decisione di adeguatezza rassicurazioni sul fatto che saranno effettivamente presenti le necessarie garanzie, tenuto conto anche della legislazione del paese terzo di destinazione.

21. Per quanto concerne l'assenza **delle tutele previste dall'articolo 48 del GDPR** nella legislazione del Regno Unito, l'EDPB invita la Commissione europea a presentare ulteriori rassicurazioni e specifici riferimenti alla normativa del Regno Unito che garantiscano che il livello di protezione previsto dal quadro giuridico del Regno Unito sia sostanzialmente equivalente al livello di protezione garantito nel SEE.

22. Con riguardo ai **meccanismi procedurali e di attuazione,** l'EDPB osserva che l'esistenza e l'effettivo funzionamento di un'autorità di controllo indipendente; l'esistenza di un sistema che garantisce un buon livello di conformità; e un sistema di accesso a opportuni meccanismi di ricorso che conferiscono ai cittadini nel SEE gli strumenti per far valere i propri diritti e presentare ricorso senza incontrare onerose barriere rispetto alla tutela amministrativa e giudiziaria sono elementi fondamentali che un quadro giuridico di protezione dei dati coerente con quello europeo deve presentare.

23. L'EDPB riconosce che nel GDPR del Regno Unito e nella legge Data Protection Act 2018, il Regno Unito ha trasfuso in gran parte le equivalenti disposizioni del GDPR; ciononostante, la Commissione europea è invitata a monitorare costantemente eventuali sviluppi del quadro giuridico e delle pratiche nel Regno Unito che potrebbero determinare ripercussioni negative su questi ambiti.

1.2.3. In merito all'accesso da parte delle autorità pubbliche ai dati trasferiti verso il Regno Unito

24. L'EDPB osserva i significativi cambiamenti nel quadro giuridico del Regno Unito applicabili alle agenzie di sicurezza e di intelligence, in particolare per quanto concerne l'intercettazione e l'acquisizione dei dati delle comunicazioni. A quanto risulta all'EDPB, questi cambiamenti sono, tra l'altro, una risposta ai procedimenti avviati davanti alla Corte e alla Corte europea dei diritti dell'uomo (di seguito "Corte EDU") e le loro recenti sentenze in materia.

25. In particolare, l'EDPB accoglie con favore il fatto che il Regno Unito abbia istituito l'Investigatory Powers Tribunal (di seguito "IPT"). L'IPT è competente non solo per le cause relative all'uso dei poteri

[10] 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, dicembre 2016 (di seguito "accordo quadro UE-USA"), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=LEGISSUM%3A3104_8.
[11] Cfr. articoli 46 e 47 del GDPR del Regno Unito.
[12] Cfr. *Schrems II*.

investigativi da parte delle autorità preposte all'applicazione della legge, ma anche da parte dei servizi di intelligence. A quanto risulta all'EDPB, l'IPT funziona quindi come un vero e proprio tribunale ai sensi dell'articolo 47 della Carta dei diritti fondamentali dell'Unione europea (di seguito "Carta dell'UE").

26. Inoltre, l'EDPB riscontra positivamente il significativo miglioramento rappresentato dall'introduzione dei "commissari giudiziari" (judicial commissioner) nella legge Investigatory Powers Act 2016 (di seguito "IPA 2016"). A quanto risulta all'EDPB, un'importante funzione dei commissari giudiziari è approvare *ex ante* nei singoli casi le differenti misure di sorveglianza, tra cui l'intercettazione mirata e l'acquisizione di massa di dati di comunicazione (cosiddetta procedura "double lock").

27. Tuttavia, al fine di valutare l'efficacia di questo ulteriore livello di vigilanza, l'EDPB ritiene necessario chiarire ulteriormente gli scenari in cui è possibile un'intercettazione lecita senza approvazione da parte dell'Investigatory Powers Commissioner (di seguito "IPC") o dei commissari giudiziari, e invita la Commissione europea a esaminare ulteriormente e dimostrare che, anche nei casi in cui non si applichi la procedura "double lock", il quadro giuridico del Regno Unito fornisce le opportune garanzie, anche attraverso un'efficace vigilanza *ex post*, e offre ai cittadini possibilità di ricorso, assicurando quindi un livello di protezione sostanzialmente equivalente a quello previsto nell'UE.

28. Inoltre, l'EDPB esorta la Commissione europea a valutare ulteriormente le condizioni in cui è possibile invocare una condizione di urgenza, e presentare dei chiarimenti per quanto concerne i possibili percorsi di esercizio dei diritti per gli interessati e i possibili mezzi di ricorso offerti loro nel contesto delle operazioni di interferenza nelle apparecchiature, in particolare in caso di deroga alla procedura "double lock".

29. Inoltre, l'EDPB ritiene che vi sia l'esigenza di un ulteriore chiarimento e un'ulteriore valutazione rispetto alle intercettazioni di massa, con particolare riguardo alla selezione e all'applicazione dei selettori, al fine di chiarire in che misura l'accesso ai dati personali soddisfi i criteri stabiliti dalla Corte, e quali garanzie esistono per tutelare i diritti fondamentali dei cittadini i cui dati sono intercettati in questo contesto, anche in merito ai periodi di conservazione dei dati. Sarebbe particolarmente utile una valutazione indipendente da parte delle competenti autorità di vigilanza del Regno Unito. L'EDPB sottolinea anche che appare quanto mai critico che le "comunicazioni relative all'estero", che ricadono nell'ambito di applicazione delle pratiche di intercettazione di massa, sembrino implicare la possibilità per il Regno Unito di intercettare e raccogliere ingenti quantità di dati direttamente nell'UE, compresi i dati in transito tra l'UE e il Regno Unito, aspetto che ricadrebbe nell'ambito di applicazione del progetto di decisione. Alla luce dell'importanza di questo aspetto, l'EDPB invita la Commissione europea a seguire da vicino gli sviluppi al riguardo.

30. Sempre in relazione alle intercettazioni di massa, l'EDPB sottolinea la valutazione uniforme espressa dalla Corte EDU e dalla Corte, e ribadisce i timori manifestati in relazione ai dati secondari, che dovrebbero beneficiare di garanzie specifiche in virtù della loro sensibilità. L'EDPB invita quindi la Commissione europea a valutare attentamente se le garanzie previste dalla normativa del Regno Unito per questa categoria di dati personali garantiscano un livello di protezione sostanzialmente equivalente a quello garantito nel SEE.

31. In questo contesto, l'EDPB è consapevole del fatto che la relazione pubblica dell'Intelligence and Security Committee del 2016 riguardante l'uso dei poteri di massa[13] riguarda le pratiche previste dal precedente quadro giuridico, che è stato successivamente sostituito dall'IPA 2016. Ciononostante, ritiene necessaria un'ulteriore valutazione indipendente e una vigilanza sul ricorso a strumenti di trattamento automatizzato da parte delle competenti autorità di vigilanza del Regno Unito, e invita la Commissione europea a valutare ulteriormente questo aspetto e le garanzie che sarebbero e/o potrebbero essere offerte agli interessati del SEE in questo contesto.

32. L'EDPB condivide il parere espresso dall'IPC secondo il quale occorrono ulteriori valutazioni e attività di monitoraggio per accertarsi che siano mantenute e continuino ad essere migliorate le garanzie applicate in pratica dalle competenti autorità nel campo della sicurezza nazionale e dell'intelligence al fine di rimediare alle difformità nell'applicazione della relativa normativa. L'EDPB accoglie anche con favore il fatto che, di conseguenza, l'IPC abbia condotto un esame del suo approccio all'ispezione delle intercettazioni di massa nel 2019 "*che ha previsto un attento esame dei meccanismi tecnicamente complessi con cui si realizzano effettivamente le intercettazioni di massa*" e che si sia impegnato a prevedere "*un esame approfondito dei selettori e dei criteri di ricerca a cui accennava sopra la Corte EDU*" nelle ispezioni delle intercettazioni di massa a partire dal 2020. Alla luce dell'importanza di questo aspetto, l'EDPB esprime la propria preoccupazione per il fatto che l'IPC non abbia ancora condotto un esame dettagliato dei selettori e dei criteri di ricerca, e invita la Commissione europea a seguire attentamente gli sviluppi al riguardo, soprattutto poiché rimane da chiarire la forma concreta che assumerà questa vigilanza.

33. L'EDPB sottolinea che, per quanto concerne le comunicazioni verso l'estero, l'applicazione dell'esenzione ai fini di sicurezza nazionale prevista nel diritto del Regno Unito potrebbe determinare l'assenza di garanzie che assicurino anche il rispetto dei principi di limitazione delle finalità, necessità e proporzionalità, o l'assenza o il mancato rispetto di sufficienti diritti per i cittadini, di strumenti di vigilanza e di ricorso nel paese terzo di destinazione. L'EDPB raccomanda quindi alla Commissione europea di esaminare ulteriormente le garanzie complessive fornite dalla normativa del Regno Unito per quanto concerne le comunicazioni verso l'estero, in particolare alla luce dell'applicazione delle esenzioni ai fini di sicurezza nazionale.

34. Infine, l'EDPB esprime la propria preoccupazione per altre forme di condivisione e diffusione delle informazioni, sulla base di altri strumenti, in particolare i vari accordi internazionali conclusi dal Regno Unito con altri paesi terzi, soprattutto laddove questi strumenti non sono accessibili al pubblico, come ad esempio l'accordo tra Regno Unito e Stati Uniti sull'intelligence delle comunicazioni. Gli effetti prodotti da questo accordo potrebbero determinare un'elusione delle garanzie individuate in relazione all'accesso e all'uso dei dati personali per finalità di sicurezza nazionale. L'EDPB ritiene che la conclusione di accordi bilaterali o multilaterali con paesi terzi per finalità di cooperazione di intelligence, che forniscono una base giuridica per l'intercettazione e l'acquisizione dirette di dati personali o per il trasferimento di dati personali verso questi paesi possono anche incidere significativamente sulle condizioni per un ulteriore utilizzo delle informazioni raccolte, poiché questi accordi potrebbero incidere sul quadro giuridico del Regno Unito in materia di protezione dei dati testé esaminato.

[13] Cfr. Report of the bulk powers review, dell'Independent Reviewer of Terrorism Legislation, agosto 2016, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

1.3. Conclusioni

35. L'EDPB ritiene che la valutazione di adeguatezza del Regno Unito sia un *unicum* alla luce della sua precedente appartenenza all'Unione europea come Stato membro. Inoltre, si tratterebbe della prima decisione di adeguatezza che preveda una clausola di temporaneità.

36. Per questo motivo, l'EDPB rileva molte aree di convergenza tra i quadri normativi del Regno Unito e dell'Unione europea in materia di protezione dei dati. Al contempo, tuttavia, e a seguito di un'attenta analisi del progetto di decisione della Commissione europea e della normativa del Regno Unito sulla protezione dei dati, l'EDPB ha individuato alcune problematiche, diffusamente esaminate nel presente parere. In questo contesto, l'EDPB desidera sottolineare il ruolo importantissimo che la Commissione europea riveste nell'osservare di tutti gli sviluppi rilevanti nel Regno Unito.

37. Alla luce di quanto precede, l'EDPB raccomanda alla Commissione europea di affrontare le problematiche sollevate nel presente parere. L'EDPB invita inoltre la Commissione europea a monitorare con attenzione tutti gli sviluppi rilevanti nel Regno Unito che potrebbero avere ripercussioni sul livello di sostanziale equivalenza della protezione dei dati personali, adottando rapidamente le misure opportune, ove necessarie.

2. INTRODUZIONE

2.1. Quadro giuridico del Regno Unito in materia di protezione dei dati

38. Il quadro giuridico del Regno Unito in materia di protezione dei dati è in gran parte basato sul quadro giuridico di protezione dei dati personali dell'UE (in particolare il GDPR e la LED), in quanto il Regno Unito è stato un membro dell'Unione europea fino al 31 gennaio 2020. Inoltre, la legge Data Protection Act 2018 del Regno Unito, che è entrata in vigore il 23 maggio 2018 e che ha abrogato la legge Data Protection Act 1998 del Regno Unito, specifica ulteriormente che nel diritto del Regno Unito si applica il GDPR, oltre a recepire la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie dell'UE e a conferire poteri e imporre obblighi all'autorità nazionale di controllo della protezione dei dati, ICO.

39. Come indicato nel considerando 12 del progetto di decisione della Commissione europea, il governo del Regno Unito ha adottato la legge "European Union (Withdrawal) Act 2018" che incorpora nel diritto del Regno Unito la legislazione direttamente applicabile dell'UE. Questa legge prevede la possibilità per i ministri del Regno Unito di introdurre legislazione secondaria, attraverso atti normativi, al fine di apportare le modifiche necessarie al diritto UE mantenuto successivamente al recesso del Regno Unito dall'Unione europea, per adeguarlo al contesto nazionale.

40. Per questo motivo, il pertinente quadro giuridico applicabile nel Regno Unito al termine del periodo di transizione è composto dalle seguenti norme[14]:

- l'United Kingdom General Data Protection Regulation (regolamento generale sulla protezione dei dati del Regno Unito, di seguito "GDPR del Regno Unito"), incorporato nel diritto del Regno Unito in forza della legge European Union (Withdrawal) Act 2018, come modificata dal

[14] La fine del periodo di transizione è fissata al 31 dicembre 2020; dopo tale data nel Regno Unito non si applicherà più il diritto dell'Unione europea. Il "periodo ponte", la cui fine è fissata a non oltre il 30 giugno 2021, costituisce l'ulteriore periodo durante il quale la trasmissione di dati personali dal SEE verso il Regno Unito non è considerata un trasferimento di dati ai sensi del GDPR.

regolamento DPPEC (Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019;

- la Data Protection Act 2018 (legge del 2018 sulla protezione dei dati, di seguito "DPA 2018"), come modificata dal regolamento DPPEC Regulations 2019, e il regolamento Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020; e
- l'Investigatory Power Act 2016 (legge del 2016 sui poteri di indagine, di seguito "IPA 2016")

(congiuntamente "il quadro giuridico del Regno Unito in materia di protezione dei dati").

2.2. Ambito della valutazione dell'EDPB

41. Il progetto di decisione della Commissione europea è il risultato di una valutazione condotta sul quadro giuridico del Regno Unito in materia di protezione dei dati, a cui è seguito un confronto con il governo del Regno Unito. Come previsto dall'articolo 70, paragrafo 1, lettera s) del GDPR, l'EDPB è tenuto a esprimere un parere indipendente sui riscontri della Commissione europea, individuare eventuali criticità nel quadro di adeguatezza e presentare proposte per la risoluzione di tali criticità.

42. Come indicato nei Criteri di riferimento per l'adeguatezza: "*le informazioni fornite dalla Commissione europea dovrebbero essere esaustive e permettere all'EDPB di effettuare la propria valutazione del livello di protezione dei dati nel paese terzo*"[15].

43. Al riguardo, si osserva che l'EDPB ha ricevuto per tempo solo alcuni documenti rilevanti per l'esame del quadro giuridico del Regno Unito. La maggior parte della normativa del Regno Unito a cui si fa riferimento nel progetto di decisione è stata ottenuta dall'EDPB tramite i collegamenti ipertestuali presenti nel progetto di decisione stesso. La Commissione europea non è stata in grado di fornire all'EDPB una spiegazione scritta né impegni da parte del Regno Unito in relazione alle interlocuzioni tra le autorità del Regno Unito e la Commissione europea che rilevano ai fini di questa attività[16].

44. Tenuto conto di quanto precede, e alla luce dei tempi ristretti (2 mesi) concessi per adottare questo parere, l'EDPB ha scelto di concentrarsi su alcuni specifici punti nel progetto di decisione, fornendo al riguardo la propria analisi e il proprio parere.

[15] Cfr. WP254 rev.01, pag. 3.

[16] Per quanto riguarda: l'articolo 48 del GDPR (nota a piè di pagina 78 del progetto di decisione); garanzie rafforzate e misure di sicurezza applicate dai titolari del trattamento durante il trattamento nel contesto della sicurezza nazionale (nota a piè di pagina 64 del progetto di decisione); l'obbligo del titolare del trattamento di valutare l'eventuale esigenza di fare ricorso all'esenzione caso per caso anche quando sia stato rilasciato un certificato di sicurezza nazionale (considerando 126 e nota a piè di pagina 172 del progetto di decisione); il fatto che le protezioni previste dall'accordo quadro UE-USA si applicheranno a tutte le informazioni personali prodotte o conservate secondo l'Accordo UK-US CLOUD Act, indipendentemente dalla natura o tipologia dell'organismo che effettua la richiesta, con riguardo ai dettagli della concreta attuazione delle garanzie di protezione dei dati ancora oggetto di discussione tra il Regno Unito e gli Stati Uniti, la conferma che le autorità del Regno Unito consentiranno a questo accordo di entrare in vigore unicamente quando saranno certe che la sua attuazione rispetti gli obblighi legali da esso previsti, anche in merito alla chiarezza relativa al rispetto delle norme di protezione dei dati per i dati richiesti nell'ambito di questo accordo (considerando 153 del progetto di decisione); i casi in cui i dati vengono trasferiti dall'UE al Regno Unito nell'ambito del progetto di decisione, e il fatto che vi sarebbe sempre una "connessione con le isole britanniche" e che l'eventuale interferenza nelle apparecchiature che interessa questi dati sarebbe quindi soggetta all'obbligo inderogabile di mandato ai sensi della sezione 13(1) della IPA 2016 (considerando 206 del progetto di decisione); e gli esempi di finalità operative previste (considerando 216 e nota a piè di pagina 369 del progetto di decisione).

45. Analizzando la normativa e le pratiche di un paese terzo che è stato membro dell'Unione europea fino a poco tempo fa, evidentemente l'EDPB ha individuato molti aspetti sostanzialmente equivalenti. Alla luce del suo ruolo nel processo di determinazione dell'adeguatezza e della quantità delle disposizioni e delle pratiche da analizzare, l'EDPB ha deciso di concentrarsi sugli aspetti che a suo giudizio richiedevano una maggiore attenzione. Inoltre, in linea con la giurisprudenza della Corte, una parte rilevante dell'analisi riguarda il regime giuridico dell'accesso per scopi di sicurezza nazionale ai dati personali trasferiti verso il Regno Unito, e le prassi adottate dall'apparato di sicurezza nazionale nel Regno Unito. Si è comunque tenuto conto del fatto che la sicurezza nazionale è un'area in cui la legislazione degli Stati membri non è armonizzata a livello dell'UE e può quindi presentare differenze in termini di normativa e di prassi.

46. L'EDPB ha tenuto conto del quadro europeo di protezione dei dati applicabile, tra cui gli articoli 7, 8 e 47 della Carta dell'UE, che riguardano rispettivamente la protezione del diritto alla vita privata e familiare, il diritto alla protezione dei dati personali, e il diritto a un ricorso effettivo e un giudice imparziale; e l'articolo 8 della Convenzione europea dei diritti dell'uomo (di seguito "CEDU"), che tutela il diritto alla vita privata e alla vita familiare. In aggiunta a quanto precede, l'EDPB ha considerato gli obblighi previsti dal GDPR, nonché la giurisprudenza pertinente.

47. L'obiettivo di questa attività è presentare alla Commissione europea un parere sulla valutazione dell'adeguatezza del livello di protezione nel Regno Unito. Il concetto di "livello di protezione adeguato", che già esisteva nella direttiva 95/46/CE, è stato ulteriormente sviluppato dalla Corte. È importante richiamare la norma stabilita dalla Corte in *Schrems I*, ovvero che, benché il "livello di protezione" nel paese terzo debba essere "sostanzialmente equivalente" a quello garantito nell'UE, "*gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all'interno dell'Unione*"[17]. Per questo motivo l'obiettivo non è rispecchiare punto per punto la legislazione europea, ma stabilire i requisiti essenziali e fondamentali della normativa in esame. L'adeguatezza può essere conseguita anche attraverso la combinazione fra diritti riconosciuti agli interessati, obblighi in capo a chi effettua il trattamento o esercita il controllo sul trattamento, e il controllo esercitato da parte di organismi indipendenti. Le norme in materia di protezione dei dati, tuttavia, sono efficaci solo se sono azionabili e sono rispettate nella pratica. È pertanto necessario considerare non solo il contenuto delle norme applicabili ai dati personali trasferiti verso un paese terzo o un'organizzazione internazionale, ma anche il sistema in atto per garantirne l'efficacia. La presenza di meccanismi di enforcement efficienti è di fondamentale importanza per garantire l'efficacia delle norme sulla protezione dei dati[18].

2.3. Osservazioni generali e criticità

2.3.1. Impegni internazionali assunti dal Regno Unito

48. Secondo l'articolo 45, paragrafo 2, lettera c) del GDPR e i Criteri di riferimento per l'adeguatezza[19], nel valutare l'adeguatezza del livello di protezione di un paese terzo, la Commissione europea deve tenere conto, tra l'altro, degli impegni internazionali assunti dal paese terzo, o degli altri obblighi derivanti dalla partecipazione di quest'ultimo a sistemi multilaterali o regionali, con particolare riguardo alla protezione dei dati personali, nonché l'attuazione di tali obblighi. Inoltre, si dovrebbe tenere in considerazione l'adesione dei paesi terzi alla Convenzione del Consiglio d'Europa, del

[17] Cfr. Corte di giustizia dell'Unione europea, C-362/14, *Maximilian Schrems contro Data Protection Commissioner*, 6 ottobre 2015, ECLI:EU:C:2015:650 (di seguito "*Schrems I*"), paragrafi 73-74.
[18] Cfr. WP254 rev.01, pag. 2.
[19] Cfr. WP254 rev.01, pag. 2.

28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (di seguito "Convenzione 108")[20] e relativo protocollo addizionale[21].

49. **Al riguardo, l'EDPB accoglie con favore l'adesione da parte del Regno Unito alla CEDU e il fatto che il paese sia soggetto alla giurisdizione della Corte EDU. Inoltre, il Regno Unito ha aderito anche alla Convenzione 108 e al relativo protocollo addizionale, nel 2018 ha firmato la Convenzione 108+[22] e attualmente sta procedendo alla sua ratifica.**

2.3.2. Possibile futura divergenza del quadro giuridico del Regno Unito in materia di protezione dei dati

50. Come indicato nel considerando 281 del progetto di decisione, la Commissione europea deve considerare che, con la fine del periodo di transizione previsto dall'accordo di recesso[23], il Regno Unito amministra, applica e fa applicare il proprio regime in materia di protezione dei dati, e non appena la disposizione provvisoria prevista dall'articolo FINPROV.10A dell'accordo sugli scambi commerciali e la cooperazione UE-Regno Unito[24] cesserà di applicarsi, potranno determinarsi in particolare modifiche o variazioni del quadro giuridico sulla protezione dei dati preso in esame nel progetto di decisione, oltre ad altri sviluppi rilevanti.

51. La Commissione europea ha quindi deciso di inserire una clausola di temporaneità nel suo progetto di decisione[25], che ne fissa la data di scadenza a quattro anni dopo l'entrata in vigore.

52. È importante osservare, inoltre, che la possibilità per i ministri del Regno Unito e per il Segretario di Stato del Regno Unito di introdurre legislazione secondaria dopo il termine del periodo ponte può determinare in futuro una significativa divergenza tra il quadro giuridico del Regno Unito in materia di protezione dei dati e quello dell'UE.

53. Infatti, il governo del Regno Unito ha segnalato l'intenzione di definire politiche distinte e indipendenti in materia di protezione dei dati, con la possibilità quindi di discostarsi dalla normativa dell'UE in materia di protezione dei dati[26]. Secondo le intenzioni dichiarate, ciò comprende

[20] Cfr. Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Convenzione 108, 28 gennaio 1981.
[21] Cfr. Protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, concernente le autorità di controllo e i flussi transfrontalieri, la cui firma è stata aperta l'8 novembre 2001.
[22] Cfr. Protocollo di emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale ("Convenzione 108+"), 18 maggio 2018.
[23] Cfr. accordo sul recesso del Regno Unito di Gran Bretagna e Irlanda del Nord dall'Unione europea e dalla Comunità europea dell'energia atomica (GU L 029 del 31.1.2020, pag. 7).
[24] Cfr. accordo sugli scambi commerciali e la cooperazione tra l'Unione europea e la Comunità europea dell'energia atomica, da una parte, e il Regno Unito di Gran Bretagna e Irlanda del Nord, dall'altra (GU L 444 del 31.12.2020, pag. 14).
[25] Cfr. articolo 4 del progetto di decisione. Cfr. anche considerando 282 del progetto di decisione.
[26] La National Data Strategy del Regno Unito, (ultimo aggiornamento il 9 dicembre 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) prevede come una delle sue missioni la seguente: "*Difesa dei flussi internazionali di dati. Il flusso di informazioni tra le frontiere alimenta le attività commerciali globali, le catene di fornitura e gli scambi commerciali, promuovendo la crescita mondiale. Assolve inoltre un più ampio ruolo sociale. Il trasferimento di dati personali garantisce il pagamento delle retribuzioni delle persone, e le aiuta a tenersi in contatto a distanza con i loro cari. E, come ha dimostrato la pandemia di coronavirus, la condivisione di dati sanitari può aiutare la fondamentale ricerca scientifica sulle malattie e unire al contempo le nazioni nella risposta alle emergenze sanitarie globali.* ***Avendo lasciato l'Unione europea, il Regno Unito difenderà i benefici che possono derivare dai dati.*** *Promuoveremo le migliori pratiche nazionali e collaboreremo con partner internazionali* ***per assicurarci che i dati non siano***

l'inserimento di aspetti relativi ai dati personali negli accordi commerciali[27], una pratica che comporta il rischio di abbassamento del livello di protezione dei dati personali previsto dal Regno Unito[28].

54. Infine, non solo dalla conclusione del periodo transitorio il Regno Unito non è più vincolato dalla giurisprudenza della Corte, ma anche le sentenze già adottate dalla Corte, e considerate giurisprudenza acquisita nel quadro giuridico del Regno Unito, potrebbero non essere più vincolanti per il Regno Unito in quanto, in particolare, esso ha la possibilità di modificare il diritto UE mantenuto successivamente al termine del periodo ponte e la sua Supreme Court non è vincolata dalla giurisprudenza UE acquisita[29].

55. **Alla luce dei rischi relativi al possibile scostamento del quadro giuridico del Regno Unito in materia di protezione dei dati rispetto all'acquis dell'Unione dopo la fine del periodo ponte, l'EDPB accoglie con favore la decisione della Commissione europea di introdurre una clausola di temporaneità di quattro anni per il progetto di decisione. L'EDPB desidera tuttavia sottolineare in questo caso l'importanza del ruolo di monitoraggio svolto dalla Commissione europea[30]. Infatti, la Commissione europea dovrebbe tenere sotto costante e permanente osservazione tutti gli sviluppi rilevanti nel Regno Unito che potrebbero incidere sull'equivalenza sostanziale del livello di protezione dei dati personali trasferiti nell'ambito della decisione di adeguatezza relativa al Regno Unito dal momento in cui quest'ultima entrerà in vigore. Inoltre, la Commissione europea dovrebbe adottare le misure opportune per sospendere, modificare o abrogare la decisione di adeguatezza, alla luce delle circostanze del caso qualora, successivamente alla sua adozione, rilevi che nel Regno Unito non è più garantito un livello di protezione adeguato.**

56. Da parte sua, l'EDPB si adopererà al meglio per informare la Commissione europea di attività rilevanti intraprese dalle autorità di controllo della protezione dei dati degli Stati membri (di seguito "autorità di controllo"), nel settore privato o pubblico, in particolare per quanto concerne i reclami avanzati da interessati nel SEE relativamente al trasferimento di dati personali dal SEE al Regno Unito.

***inopportunamente limitati dalle frontiere nazionali e dalla frammentazione dei regimi normativi**, in modo che possano essere sfruttati al massimo della loro potenzialità*" (grassetto aggiunto).

[27] Ibidem: "*Agevolare i flussi di dati transfrontalieri: **lavoreremo per rimuovere a livello mondiale le barriere non necessarie ai flussi internazionali di dati. Concorderemo disposizioni ambiziose in materia di dati nelle nostre trattative commerciali** e sfrutteremo il nostro nuovo seggio indipendente nell'Organizzazione mondiale del commercio per influenzare in meglio le regole commerciali relative ai dati. **Elimineremo gli ostacoli ai trasferimenti internazionali di dati** che favoriscono la crescita e l'innovazione, sviluppando anche una nuova capacità del Regno Unito che realizzi meccanismi nuovi e innovativi di trasferimento internazionale dei dati. Lavoreremo anche con i partner del G20 per realizzare un'interoperabilità tra i regimi nazionali dei dati al fine di contenere al minimo le frizioni nel trasferimento dei dati tra differenti nazioni*" (grassetto aggiunto).

[28] Cfr. risoluzione del Parlamento europeo del 12 dicembre 2017 "*Verso una strategia per il commercio digitale*" (2017/2065(INI)), sezione V, in cui si sottolinea che "*la protezione dei dati personali non è negoziabile negli accordi commerciali [dell'Unione]*", disponibile all'indirizzo: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_IT.pdf.
Cfr. anche, risoluzione del Parlamento europeo del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione, paragrafo 28, in cui si afferma: *"è favorevole all'approccio della Commissione consistente nell'affrontare la protezione dei dati e i flussi di dati personali separatamente dagli accordi commerciali"*, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_IT.html.

[29] Cfr. sezione 6(3)–(6) della legge EU (Withdrawal) Act 2018.

[30] Cfr. articolo 45, paragrafo 4, del GDPR.

3. ASPETTI GENERALI RELATIVI ALLA PROTEZIONE DEI DATI

3.1. Principi di contenuto

57. Il capitolo 3 dei Criteri di riferimento per l'adeguatezza è dedicato ai "principi di contenuto". Il sistema di un paese terzo deve prevederli affinché il suo livello di protezione dei dati possa essere considerato sostanzialmente equivalente a quello garantito nell'UE. L'EDPB prende atto del fatto che il Regno Unito non possiede una costituzione codificata in quanto non esiste un documento che stabilisca le regole fondamentali della sua forma di governo. Tuttavia, il diritto al rispetto della vita privata e familiare (e il diritto alla protezione dei dati nell'ambito di questo diritto) e il diritto a un equo processo[31] sono inclusi nella legge Human Rights Act 1998, il cui valore costituzionale è stato riconosciuto dai tribunali britannici. Di fatto, la legge Human Rights Act 1998 integra i diritti previsti nella CEDU[32]. Inoltre, la legge Human Rights Act 1998 afferma un principio molto importante secondo il quale qualunque atto delle autorità pubbliche deve essere compatibile con la CEDU[33].

58. A parte alcune differenze strutturali e formali tra la legislazione del Regno Unito e quella dell'UE, l'EDPB osserva, come ci si potrebbe attendere, che l'approccio del Regno Unito alla protezione dei dati è simile a quello nell'UE, poiché il Regno Unito era uno Stato membro dell'UE fino al 31 gennaio 2020. Di conseguenza, molti principi di contenuto sono coerenti con quelli del GDPR, e prevedono quindi un livello di protezione sostanzialmente equivalente a quello previsto dall'UE. L'EDPB ha deciso di non sviluppare ulteriormente l'esame di quei principi di contenuto che sono coerenti con la legislazione dell'UE, ed è soddisfatto dell'analisi presentata dalla Commissione europea nel suo progetto di decisione. I principi di contenuto in questione sono ad esempio i seguenti: definizioni di base (ad esempio "dati personali"; "trattamento dei dati personali"; "titolare del trattamento"); motivi di lecito e corretto trattamento per finalità legittime; limitazione delle finalità; qualità e proporzionalità dei dati; conservazione, sicurezza e riservatezza dei dati; trasparenza; categorie particolari di dati; marketing diretto; processi decisionali automatizzati e profilazione. L'EDPB riscontra inoltre che il GDPR del Regno Unito e la DPA 2018 prevedono principi di contenuto che vanno oltre quelli imposti dai Criteri di riferimento per l'adeguatezza, e rispecchiano i principi inclusi nel GDPR, innalzando quindi il livello di protezione previsto nel Regno Unito. I principi di contenuto in questione sono, ad esempio, quelli concernenti le notifiche delle violazioni dei dati personali, il responsabile della protezione dei dati, le valutazioni d'impatto sulla protezione dei dati e la protezione dei dati fin dalla progettazione e per impostazione predefinita.

59. Tuttavia, come menzionato nell'introduzione, nel presente parere l'EDPB desidera affrontare specificamente alcuni punti su cui nutre perplessità e su cui desidera chiarimenti dalla Commissione europea.

3.1.1. Diritti di accesso, rettifica, cancellazione e opposizione

60. La cosiddetta "esenzione per motivi di immigrazione" prevista **dall'allegato 2 alla DPA 2018, parte 1**, paragrafo 4, consente ai titolari del trattamento che partecipano al "controllo dell'immigrazione" di non applicare alcuni diritti degli interessati previsti dalla DPA 2018 se così facendo "*pregiudicherebbero il mantenimento di un efficace controllo sull'immigrazione*" o per "*l'indagine o*

[31] Cfr. articoli 6 e 8 CEDU (allegato 1 alla legge Human Rights Act 1998).
[32] Per maggiori informazioni, vedere i considerando 8-10 del progetto di decisione.
[33] Cfr. Art. 6 della legge Human Rights Act 1998.

la rilevazione di attività che potrebbero compromettere il mantenimento dell'effettivo controllo dell'immigrazione".

61. Come riconosciuto dalla Commissione europea nel suo progetto di decisione[34], e come menzionato nel parere della commissione LIBE del Parlamento europeo, nella conclusione, per conto dell'UE, dell'accordo sugli scambi commerciali e la cooperazione UE-Regno Unito[35], questa esenzione ha una **formulazione "ampia"**. Essa si applica ai seguenti diritti: diritto a essere informati; diritto di accesso; diritto alla cancellazione; diritto alla limitazione del trattamento; e diritto all'opposizione al trattamento.

62. Inoltre, è importante osservare che questa esenzione vale anche nel caso di dati personali non raccolti ai fini del controllo dell'immigrazione da parte di un titolare del trattamento ("titolare 1"), ma comunque da esso messi a disposizione di un altro titolare del trattamento ("titolare 2") che li sottopone a trattamento per scopi di controllo dell'immigrazione (ad esempio l'Home Office del Regno Unito)[36].

63. In *Open Rights Group & Anor, R (On the Application Of) contro Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (3 ottobre 2019)*, i ricorrenti hanno contestato la legittimità dell'esenzione per motivi di immigrazione ritenendo che fosse contraria all'articolo 23 del GDPR e incompatibile con i diritti garantiti dagli articoli 7 e 8 della Carta dell'UE relativi alla sfera

---

[34] Cfr. i considerando da 62 a 65 del progetto di decisione.

[35] Al riguardo, sulla **formulazione ampia** dell'esenzione per motivi di immigrazione, vedere il parere della commissione per le libertà civili, la giustizia e gli affari interni, per conto dell'Unione, dell'accordo sugli scambi commerciali e la cooperazione tra l'Unione europea e la Comunità europea dell'energia atomica, da una parte, e il Regno Unito di Gran Bretagna e Irlanda del Nord, dall'altra, e dell'accordo tra l'Unione europea e il Regno Unito di Gran Bretagna e Irlanda del Nord sulle procedure di sicurezza per lo scambio e la protezione di informazioni classificate (2020/0382(NLE)), 5 febbraio 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_IT.pdf, paragrafo 10: *"ricorda, a tale riguardo, le risoluzioni del Parlamento del febbraio e del giugno 2020, nelle quali viene evidenziata **l'esenzione ampia e generalizzata** per quanto riguarda il trattamento dei dati personali ai fini dell'immigrazione prevista dalla legge del Regno Unito in materia di protezione dei dati"*, e paragrafo 11: *"ritiene che, prima di poter emettere una decisione di adeguatezza valida, sia necessario modificare l'esenzione **ampia e generalizzata** per quanto riguarda il trattamento dei dati personali ai fini dell'immigrazione prevista dalla legge del Regno Unito in materia di protezione dei dati [...];"* (grassetto aggiunto).

[36] Cfr. esempio fornito nella "Guide to the General Data Protection Regulation (GDPR)" dell'ICO, versione 1 gennaio 2021, pag. 307 (grassetto aggiunto): *"Un'organizzazione privata (titolare del trattamento 1) segnala all'Home Office (titolare 2) un dipendente che ritiene abbia presentato documenti falsi per dimostrare la propria identità e le qualifiche per ottenere un'occupazione. Il datore di lavoro mette a disposizione dell'Home Office le relative informazioni. Il diritto della persona a essere informato del trasferimento dei propri dati personali all'Home Office è limitato nella misura in cui potrebbe pregiudicare le indagini.*
*Il **datore di lavoro non è quindi obbligato a informare l'interessato che le informazioni sono state trasmesse all'Home Office**, e per suo conto **l'Home Office** non è obbligato a trasmettere all'interessato un'informativa sulla privacy che comunichi il trattamento da parte sua dei suoi dati personali. Questa esenzione vale per entrambi i titolari del trattamento in eguale misura.*
*Tuttavia, il lavoratore richiede una copia dei suoi dati personali all'Home Office che sta eseguendo degli accertamenti sul suo conto. **L'Home Office può avvalersi dell'esenzione** per non comunicare parte dei dati se la loro comunicazione potrebbe pregiudicare l'indagine. Qualora il lavoratore dovesse presentare un'analoga richiesta al **proprio datore di lavoro, anche quest'ultimo potrebbe applicare l'esenzione** nella stessa misura".*
In altre parole, come chiarito a pag. 300: *"Nella maggior parte dei casi, l'Home Office, o una delle sue agenzie o dei suoi appaltatori, sarà il titolare del trattamento che applica questa esenzione. È però importante osservare che l'applicazione di questa esenzione non è limitata al solo Home Office. Essa può avere rilevanza anche per altri titolari del trattamento quali datori di lavoro, università e autorità di polizia, che si interfacciano con l'Home Office per questioni relative all'immigrazione".*

privata e alla protezione dei dati personali. La High Court of England and Wales (di seguito "High Court") ha valutato la legittimità dell'esenzione per motivi di immigrazione contenuta nel paragrafo 4 della parte 1 dell'allegato 2 della DPA 2018, concludendo a favore della sua legittimità.

64. La High Court ha considerato in particolare che:

- *"[…] l'esenzione per motivi di immigrazione rappresenta chiaramente una questione di "importante interesse pubblico" e persegue una finalità legittima. […]"*, paragrafo 30;
- *"l'esenzione per motivi di immigrazione soddisfa i requisiti previsti affinché una misura sia "conforme alla legge". […]"*, paragrafo 38;
- *"È possibile fare ricorso all'esenzione per motivi di immigrazione unicamente se e nella misura in cui il rispetto delle "disposizioni elencate del GDPR"* ***potrebbe pregiudicare*** *il mantenimento di un efficace controllo dell'immigrazione oppure l'investigazione o la rilevazione di attività che potrebbero pregiudicare il mantenimento dell'effettivo controllo dell'immigrazione. Le parole "potrebbero pregiudicare", nel contesto della legge Data Protection Act 1998 (che ha preceduto la DPA 2018) sono state interpretate come "una probabilità molto significativa e seria di pregiudizio per lo specifico interesse pubblico. Il grado di rischio deve essere tale per cui "potrebbe senz'altro manifestarsi" un pregiudizio per questi interessi, anche se il rischio non è particolarmente probabile […]."*, paragrafo 39 (grassetto aggiunto).

65. Occorre osservare che questa sentenza è, per quanto noto all'EDPB, non definitiva ed è stata impugnata.

66. Come specificato nelle "Guidelines on restrictions under Article 23 GDPR" dell'EDPC ("linee guida sull'articolo 23 del GDPR")[37] *"[...] in un contesto di GDPR, le limitazioni sono* ***previste in un atto legislativo****, riguardano un* ***numero limitato di diritti degli interessati e/o obblighi del titolare del trattamento****, elencati nell'articolo 23 del GDPR,* ***rispettano l'essenza*** *dei diritti fondamentali e delle libertà in questione, rappresentano una* ***misura necessaria e proporzionata*** *in una società democratica e tutelano una delle motivazioni previste dall'articolo 23, paragrafo 1 del GDPR [...]"*[38].

67. L'EDPB richiama anche il considerando 41 del GDPR in cui si afferma che *"[q]ualora il presente regolamento faccia riferimento a* ***una base giuridica o a una misura legislativa****, ciò non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento, fatte salve le prescrizioni dell'ordinamento costituzionale dello Stato membro interessato. Tuttavia, tale base giuridica o misura legislativa dovrebbe essere* ***chiara e precisa, e la sua applicazione prevedibile, per le persone che vi sono sottoposte****, in conformità della giurisprudenza della Corte di giustizia dell'Unione europea [...] e della Corte europea dei diritti dell'uomo" (grassetto aggiunto).*

68. Anche se la Corte EDU ha specificato che "*[i]noltre, per quanto concerne le parole "previsto dalla legge" e "stabilito dalla legge" che compaiono negli articoli da 8 a 11 della Convenzione, la [CEDU] osserva di aver sempre inteso il termine "legge" in senso "sostanziale" e non "formale"; esso comprende sia "la legge scritta", che include l'emanazione di atti normativi di livello inferiore e misure regolamentari adottate dagli organismi di regolamentazione professionale nell'ambito di poteri regolamentari indipendenti delegati loro dal Parlamento, e le leggi non scritte. Il termine "legge" deve essere inteso come comprendente sia la legge emanata dal legislatore sia la* ***"legge" derivante dalla***

[37] Cfr. Guidelines 10/2020 on restrictions under Article 23 GDPR dell'EDPB, versione 1.0, adottate il 15 dicembre 2020, attualmente in fase di definizione a seguito di consultazione pubblica, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_it.
[38] Cfr. linee guida sull'articolo 23 del GDPR, paragrafo 9, pag. 5.

giurisprudenza"[39], le linee guida sull'articolo 23 del GDPR ricordano che *"[s]econdo la giurisprudenza della Corte, qualunque **misura legislativa** adottata sulla base dell'articolo 23, paragrafo 1 [del] GDPR deve, in particolare, **rispettare gli specifici requisiti stabiliti nell'articolo 23, paragrafo 2 del GDPR**. L'articolo 23, paragrafo 2 [del] GDPR afferma che le misure legislative che impongono restrizioni ai diritti degli interessati e agli obblighi dei titolari del trattamento devono contenere, ove rilevante, **disposizioni specifiche sui vari criteri delineati di seguito**. Di norma, tutti i requisiti specificati di seguito **dovrebbero essere inclusi nella misura legislativa** che impone limitazioni secondo l'articolo 23 [del] GDPR*"[40].

69. Si può osservare al riguardo che **l'esenzione per motivi di immigrazione** stessa **non specifica i seguenti elementi di cui all'articolo 23, paragrafo 2 del GDPR**:

- "le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti" (d);
- "il titolare del trattamento o le categorie di titolari" (e)[41];
- "i rischi per i diritti e le libertà degli interessati" (g);
- "il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa" (h).

70. La "Guide to the General Data Protection Regulation (GDPR)"[42] dell'ICO, che prevede un capitolo sull'"esenzione per motivi di immigrazione", offre chiarimenti sull'esenzione per motivi di immigrazione, ma di per sé **non può** stabilire regole vincolanti a integrazione delle norme relative.

---

[39] Cfr. Corte EDU, *Sanoma Uitgevers B.V. contro Paesi Bassi*, 14 settembre 2010, EC:ECHR:2010:0914JUD003822403, paragrafo 83 (grassetto aggiunto).

[40] Cfr. linee guida sull'articolo 23 del GDPR, paragrafi 45 e 46, pag. 11. Secondo l'articolo 52, paragrafo 3 della Carta dell'UE, *"[l]addove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa"*. Sulla nozione di "**previste dalla legge**" di cui all'articolo 52, paragrafo 1 della Carta dell'UE, i criteri sviluppati dalla Corte EDU dovrebbero essere utilizzati come suggerito in diverse conclusioni dell'avvocato generale della Corte, vedere ad esempio le conclusioni nelle cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:572, paragrafi 137-154, e nella causa C-70/10, *Scarlet Extended*, ECLI:EU:C:2011:255, paragrafi 88-114. È quindi possibile fare riferimento, tra l'altro, alla decisione della Corte EDU in *Weber e Saravia contro Germania*, paragrafo 84: *"La Corte ribadisce che l'espressione "**prevista dalla legge**" ai sensi dell'articolo 8, paragrafo 2 [della CEDU] impone, in primo luogo, che la misura impugnata debba presentare qualche fondamento nel **diritto interno**; fa riferimento anche alla **qualità della legge** in questione, esigendo che essa debba essere accessibile alla persona interessata, la quale inoltre deve poter prevedere le conseguenze per la sua persona, ed essere compatibile con lo Stato di diritto"* (grassetto aggiunto).
Cfr. anche il considerando 41 del GDPR: *"Tale [base giuridica o] misura legislativa dovrebbe essere **chiara** e **precisa**, e la sua applicazione **prevedibile, per le persone che vi sono sottoposte**, in conformità della giurisprudenza della Corte di giustizia dell'Unione europea (...) e della Corte europea dei diritti dell'uomo"* (grassetto aggiunto).

[41] Cfr. la summenzionata causa dinanzi alla High Court, paragrafo 54: *"A mio giudizio non vi è nulla di illecito nella possibilità per **tutti i titolari del trattamento** che sottopongono a trattamento dati per specifiche finalità di avvalersi dell'esenzione per motivi di immigrazione. Come evidenziano le parti convenute, senza i paragrafi 4(3)–(4) l'esenzione per motivi di immigrazione sarebbe inefficace nei casi in cui i dati fossero ottenuti da terzi (ad esempio un'autorità locale oppure l'agenzia fiscale e delle dogane) ai fini del mantenimento dell'effettivo controllo dell'immigrazione."* (grassetto aggiunto), confermando quindi l'applicazione **generalizzata** delle restrizioni.

[42] "Guide to the General Data Protection Regulation (GDPR)" dell'ICO, versione 1 gennaio 2021, pagg. 299-307.

Inoltre, la questione della "qualità della legge" è particolarmente rilevante alla luce dell'importanza dei diritti sottoposti a limitazioni e della portata dell'esenzione[43].

71. *A fortiori*, il "**test del pregiudizio**" non stabilisce le garanzie per prevenire l'abuso o l'accesso o il trasferimento non autorizzato, e che devono essere applicate ad esempio dall'Home Office.

---

[43] Cfr. paragrafo 57 della summenzionata causa dinnanzi alla High Court: *"Il sig. Knight mi informa che il Commissioner sta definendo gli orientamenti sull'esenzione, ma essi avranno uno status "legale" solo nel senso di essere emanati in forza delle facoltà del Commissioner previste dall'articolo 57, paragrafo 1 del GDPR. Non avranno uno status legale ai sensi della legge DPA 2018".*
Il motivo alla base dell'introduzione degli orientamenti giuridicamente vincolanti supportati dall'ICO è presentato in particolare nei paragrafi 56-60 della sentenza:
"56. Infine, passo all'osservazione del Commissioner secondo la quale, in assenza di orientamenti legali che forniscono garanzie in merito al significato e all'applicazione dell'esenzione per motivi di immigrazione, l'esenzione non rappresenterebbe un'applicazione proporzionata dell'articolo 23, paragrafo 1 del GDPR. Il sig. Knight afferma che, con l'integrazione di questi orientamenti, la disposizione è proporzionata.
57. Il sig. Knight mi informa che il Commissioner sta definendo gli orientamenti sull'esenzione, ma essi avranno uno status "legale" solo nel senso di essere emanati in forza delle facoltà del Commissioner previste dall'articolo 57, paragrafo 1 del GDPR. Non avranno uno status legale ai sensi della legge DPA 2018. Mi risulta che anche l'Home Office abbia prodotto dei progetti di linee guida interne per il personale sull'esenzione per motivi di immigrazione (cfr. [22] sopra). Nella pratica, gli orientamenti emanati dal Commissioner sono influenti, indipendentemente dalla loro base giuridica. Tuttavia, il Commissioner non ha alcun potere di emanare orientamenti "vincolanti" del tipo considerato dalla Supreme Court nella causa Christian Institute (punto [101] e [107]). A quanto pare sarebbe necessaria una legislazione primaria qualora si dovesse ritenere necessaria la presenza di orientamenti sull'esenzione per motivi di immigrazione con lo stesso status dei codici di pratiche attualmente previsti negli articoli 121–124 della DPA 2018.
58. Nella sua argomentazione a favore di orientamenti legali, il sig. Knight sostiene che il contesto in cui si ricorrerà all'uso dell'esenzione per motivi di immigrazione delinea necessariamente i timori circa la necessità e proporzionalità della sua esistenza e del suo uso. In particolare, attira l'attenzione su due aspetti nel contesto giuridico. In primo luogo, con ogni probabilità i dati personali a cui si applica l'esenzione per motivi di immigrazione riguardano intrinsecamente una categoria speciale di dati ai sensi dell'articolo 9, paragrafo 1 del GDPR (dati che "rivelano l'origine razziale o etnica"). Questi dati sono identificati nel GDPR perché richiedono una protezione più elevata (parere 1/15 [2019] 3 C.M.L.R. 25 punto [141]). In secondo luogo, è un principio fondamentale della normativa sulla protezione dei dati che il diritto di accesso dell'interessato, in particolare, sia di grande importanza quale strumento per poter esercitare gli altri diritti previsti per gli interessati (cfr. YS contro Minister voor Immigratie, Integratie en Asiel (C-141/12) EU:C:2014:2081; [2015] 1 C.M.L.R. 18 punto [44]).
59. Il sig. Knight individua quattro punti di ordine pratico. In primo luogo, quando il titolare del trattamento non illustra all'interessato di aver fatto ricorso a un'esenzione legale e non presenta un'ampia sintesi delle relative motivazioni, l'interessato non sarà a conoscenza dell'applicazione dell'esenzione e non potrà quindi contestarla efficacemente. In secondo luogo, gli interessati faranno particolare affidamento sul fatto che i titolari del trattamento applichino l'esenzione con diligenza e unicamente nella misura necessaria. Benché qualunque interessato possa presentare reclamo presso il Commissioner in merito all'applicazione dell'esenzione, oppure promuovere una causa legale in sede giudiziaria, è probabile che l'interessato non sia a conoscenza dei propri diritti e che non disponga di fondi per adire le vie legali, nelle circostanze in cui vi sia un'esigenza di tempestivo e preciso rispetto dei diritti di protezione dei dati. In terzo luogo, in quanto immigrato, probabilmente l'interessato si trova in una posizione vulnerabile. In quarto luogo, non si tratta di una questione astratta, alla luce degli elementi presentati dalle parti convenute in merito all'uso dell'esenzione per motivi di immigrazione (vedere punto [4] sopra).
60. Il sig. Knight suggerisce che vi sia uno stretto parallelismo tra l'attuale contestazione dell'esenzione per motivi di immigrazione e il ragionamento formato dalla Corte in Christian Institute [2016] UKSC 51. Come in Christian Institute, sostiene che l'esenzione per motivi di immigrazione sia ampia, usi termini non definiti, applichi una soglia bassa, sia soggetta a controlli non evidenti dal testo della disposizione e si applichi a un ampio spettro di contesti e di diritti. A differenza di Christian Institute, sull'esenzione per motivi di immigrazione non esistono orientamenti disponibili al pubblico, men che meno uno status legale, a cui poter fare riferimento".

72. Alla luce di tutto quanto precede, l'EDPB osserva che occorrono ulteriori chiarimenti sull'applicazione dell'esenzione per motivi di immigrazione.

73. Inoltre, l'EDPB nota l'assenza di uno strumento giuridicamente vincolante che chiarisca l'esenzione per motivi di immigrazione per quanto concerne la sua eventuale sostanziale equivalenza con l'articolo 23 del GDPR e gli articoli 7 e 8 della Carta dell'UE. Allo stesso tempo, l'EDPB ritiene che la necessità e la proporzionalità dell'ampia portata *ratione personae* dell'esenzione per motivi di immigrazione debbano essere ulteriormente dimostrate dalla Commissione europea e supportate da evidenze ulteriori.

74. **In conclusione, l'EDPB invita la Commissione europea a verificare l'avanzamento del procedimento *Open Rights Group & Anor, R (On the Application Of) contro Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* di cui sopra, e, poiché questa sentenza non è definitiva (*res judicata*), a verificare se essa sarà confermata o rivista da una sentenza d'appello, tenendo conto di eventuali aggiornamenti al riguardo, e specificandolo nella decisione di adeguatezza. L'EDPB invita inoltre la Commissione europea a fornire ulteriori informazioni sulla necessità e sulla proporzionalità dell'esenzione per motivi di immigrazione, in particolare per quanto concerne l'ampio ambito di applicazione *ratione personae*.**

75. **Al contempo, l'EDPB esorta la Commissione europea a verificare ulteriormente se nel quadro giuridico del Regno Unito esistano o potrebbero essere previste ulteriori garanzie, ad esempio, attraverso strumenti giuridicamente vincolanti a integrazione dell'esenzione per motivi di immigrazione, che ne migliorino la prevedibilità e le garanzie per gli interessati, consentendo anche un migliore e più rapido esame e monitoraggio dei requisiti di necessità e proporzionalità.**

3.1.2. Restrizioni ai trasferimenti successivi

76. L'articolo 44 del GDPR prevede che i trasferimenti e i trasferimenti successivi di dati personali possano avvenire unicamente a condizione che non sia pregiudicato il livello di protezione delle persone fisiche garantito dal GDPR. Per questo motivo, i dati personali trasferiti dal SEE al Regno Unito sulla base della decisione di adeguatezza dovranno godere di un livello di protezione sostanzialmente equivalente a quello previsto dal quadro giuridico dell'UE in materia di protezione dei dati. **Questo significa che non solo la legislazione del Regno Unito debba essere "sostanzialmente equivalente" alla legislazione UE per quanto concerne il trattamento dei dati personali trasferiti nel Regno Unito nell'ambito del progetto di decisione, ma anche che le regole che si applicano nel Regno Unito ai trasferimenti successivi di questi dati verso paesi terzi debbano assicurare che continuerà a essere garantito un livello di protezione sostanzialmente equivalente.**

77. Per questo motivo, per garantire la continuità della protezione offerta dalla legislazione dell'UE, è importante che qualunque trasferimento successivo dal Regno Unito a un altro paese terzo di dati personali dal SEE sia correttamente protetto con garanzie, oppure avvenga nel rispetto delle regole sulle deroghe[44]. **Infatti, qualora non sia possibile offrire questa protezione, non dovrebbero avvenire ulteriori trasferimenti successivi di dati personali dal SEE.**

78. L'EDPB riconosce che il Regno Unito ha incorporato in buona parte il capo V del GDPR nel proprio GDPR del Regno Unito (articoli 44-49) e nella DPA 2018[45]. **L'EDPB ha tuttavia individuato alcuni**

[44] Cfr. articolo 49 del GDPR del Regno Unito.
[45] Cfr. artt. 17A, 17B, 17C e 18 della DPA 2018.

aspetti del quadro giuridico del Regno Unito relativi ai trasferimenti successivi che possono compromettere il livello di protezione dei dati personali trasferiti dal SEE.

79. **La prima criticità** individuata dall'EDPB riguarda il riconoscimento da parte del Regno Unito, secondo la procedura delineata nella DPA 2018, di paesi terzi, organizzazioni internazionali o territori[46] come destinatari adeguati. Infatti, sulla base di una futura possibile regolamentazione dell'adeguatezza del Regno Unito, potrebbero verificarsi trasferimenti successivi di dati personali del SEE dal Regno Unito verso paesi terzi[47].

80. Più nello specifico, come specificato nel considerando 77 del progetto di decisione, il Segretario di Stato del Regno Unito ha facoltà di riconoscere che un paese terzo (o un territorio o un settore all'interno di un paese terzo), un'organizzazione internazionale, o una descrizione del paese, del territorio, del settore o dell'organizzazione in questione garantisce un livello adeguato di protezione dei dati personali, previa consultazione con l'ICO[48]. Nel valutare l'adeguatezza del livello di protezione, il Segretario di Stato del Regno Unito deve considerare gli stessi elementi che la Commissione europea è tenuta a valutare ai sensi dell'articolo 45, paragrafo 2, lettere a) -c) del GDPR, interpretate alla luce del considerando 104 del GDPR e della giurisprudenza UE acquisita. Ciò significa che, nel valutare il livello adeguato di protezione di un paese terzo, il metro di valutazione rilevante sarà se il paese in questione garantisce un livello di protezione "sostanzialmente equivalente" a quello garantito nel Regno Unito. Pur osservando la possibilità per il Regno Unito, ai sensi del GDPR del Regno Unito, di riconoscere territori che offrono un livello adeguato di protezione dei dati secondo il quadro giuridico del Regno Unito in materia di protezione dei dati, l'EDPB desidera sottolineare che questi territori potrebbero non beneficiare al momento di una decisione di adeguatezza emessa dalla Commissione europea e potrebbero non garantire un livello di protezione "sostanzialmente equivalente" a quello garantito nell'UE. Questo potrebbe determinare rischi per la protezione dei dati personali trasferiti dal SEE in particolare se, in futuro, il quadro giuridico del Regno Unito in materia di protezione dei dati dovesse discostarsi dall'acquis dell'Unione. Si osserva che a luglio 2020, il *leading case Schrems II*[49] dinanzi alla Corte ha portato all'annullamento della decisione sullo scudo UE-USA per la privacy in quanto, secondo la Corte, non era possibile ritenere che il quadro giuridico degli Stati Uniti offrisse un livello di protezione sostanzialmente equivalente a quello dell'UE. Tuttavia, le sentenze già adottate dalla Corte, e considerate giurisprudenza acquisita nel quadro giuridico del Regno Unito, potrebbero non essere più vincolanti per il Regno Unito in quanto, in particolare, successivamente al termine del periodo ponte esso ha la possibilità di modificare il diritto UE mantenuto e la sua Supreme Court non è vincolata dalla giurisprudenza UE acquisita[50].

81. **L'EDPB invita la Commissione europea a tenere sotto attenta osservazione il processo di valutazione dell'adeguatezza e i criteri adottati dalle autorità del Regno Unito con riguardo a paesi terzi, con particolare attenzione ai paesi terzi non riconosciuti adeguati dall'UE nell'ambito del GDPR. Qualora la Commissione europea rilevi che un paese terzo considerato adeguato dal Regno Unito non offra un livello di protezione sostanzialmente equivalente a quello garantito nell'UE, l'EDPB esorta la Commissione europea ad adottare ogni misura necessaria tra cui, a titolo**

[46] Cfr. art. 17A della DPA 2018.
[47] L'equivalente del Regno Unito di una decisione di adeguatezza nel quadro del GDPR.
[48] Cfr. art. 182(2) della DPA 2018. Cfr. anche il memorandum di intesa sul ruolo dell'ICO in relazione alle nuove valutazioni di adeguatezza del Regno Unito, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.
[49] Cfr. *Schrems II*.
[50] Cfr. art. 6(3)–(6) della legge EU (Withdrawal) Act 2018.

esemplificativo, modificare la decisione di adeguatezza del Regno Unito al fine di introdurre specifiche garanzie per i dati personali provenienti dal SEE, e/o valutare la sospensione della decisione di adeguatezza se i dati personali trasferiti dal SEE verso il Regno Unito sono oggetto di trasferimenti successivi verso il paese terzo in questione sulla base di una norma di adeguatezza del Regno Unito.

82. **La seconda criticità** riguarda la prevista revisione delle decisioni di adeguatezza già prese dalla Commissione europea secondo la direttiva 95/46/CE. A seguito di questa revisione, la Commissione europea potrà decidere che alcuni paesi che fino a questo momento hanno beneficiato di una decisione di adeguatezza non offrono più un livello di protezione sostanzialmente equivalente, alla luce della normativa UE attuale e della giurisprudenza recente. Tuttavia, come previsto nel paragrafo 4, allegato 21 della DPA 2018, il Regno Unito ha già riconosciuto come adeguato il livello di protezione offerto da questi paesi. Benché il Segretario di Stato del Regno Unito debba condurre una revisione di questi riconoscimenti di adeguatezza entro un termine di quattro anni, nel progetto di decisione la Commissione europea osserva che questi atti di riconoscimento dell'adeguatezza non cesseranno automaticamente di esistere nel caso in cui il Segretario di Stato del Regno Unito non svolga la necessaria revisione entro il termine stabilito di quattro anni[51].

83. **L'EDPB invita la Commissione europea a monitorare se, una volta terminata la revisione delle decisioni di adeguatezza già esistenti da parte dell'UE, un paese che si ritiene non offrire più un livello di protezione adeguato sia invece ancora considerato adeguato dal Regno Unito. In questa eventualità, l'EDPB esorta la Commissione europea, sulla base dei considerando da 277 a 280 del progetto di decisione, ad adottare i correttivi appropriati, ad esempio modificando la decisione di adeguatezza al fine di aggiungere specifici requisiti per i dati personali provenienti dal SEE, e/o sospendendo la decisione di adeguatezza se i dati personali trasferiti dal SEE verso il Regno Unito sono oggetto di trasferimenti successivi verso il paese in questione. L'EDPB invita la Commissione europea a svolgere questa attività di monitoraggio per l'intera durata della decisione di adeguatezza del Regno Unito.**

84. **La terza criticità** riguarda il trasferimento successivo di dati personali dal SEE verso paesi non adeguati sulla base di strumenti di trasferimento previsti dagli articoli 46 e 47 del GDPR del Regno Unito. Benché il GDPR del Regno Unito preveda gli stessi strumenti di trasferimento previsti dal GDPR, l'EDPB evidenzia la necessità di accertarsi che le garanzie in essi contenute prevedano un'efficace protezione nel paese terzo, in particolare alla luce della sentenza *Schrems II*.

85. A seguito della decisione *Schrems II*, in cui la Corte ricorda che la protezione garantita ai dati personali nell'UE deve seguire i dati nei loro spostamenti, l'EDPB ha già adottato raccomandazioni iniziali sulle misure supplementari[52] per assistere gli esportatori, ove necessario, nell'accertarsi che gli interessati ricevano un livello di protezione sostanzialmente equivalente a quello garantito nell'UE.

86. Secondo la Corte, gli esportatori di dati sono tenuti a verificare, caso per caso, ove opportuno, in collaborazione con l'importatore dei dati nel paese terzo, se le leggi o le pratiche del paese terzo ledono l'efficacia delle garanzie adeguate contenute negli strumenti di trasferimento previsti

[51] Cfr. considerando 82 del progetto di decisione.

[52] Cfr. Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE, adottate il 10 novembre 2020, attualmente in fase di definizione a seguito di consultazione pubblica, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_it.pdf.

dall'articolo 46 del GDPR[53]. In questa eventualità, gli esportatori di dati dovrebbero applicare misure supplementari per colmare tali lacune di protezione, ripristinando il livello richiesto dalla normativa UE.

87. **L'EDPB invita la Commissione europea, al fine di assicurare la continuità della protezione, a introdurre nel progetto di decisione rassicurazioni sul fatto che, in caso di utilizzo degli strumenti di trasferimento previsti negli articoli 46 e 47 del GDPR del Regno Unito da parte degli esportatori di dati nel Regno Unito per trasferimenti successivi verso paesi terzi di dati trasferiti dal SEE, gli esportatori di dati valuteranno caso per caso il quadro giuridico in materia di protezione dei dati del paese terzo, e se necessario adotteranno misure finalizzate a garantire l'efficace rispetto delle garanzie contenute nello strumento di trasferimento scelto, al fine di assicurare un livello di protezione sostanzialmente equivalente a quello garantito nell'UE. In assenza di queste rassicurazioni, l'EDPB sottolinea l'esistenza di un rischio che il livello di protezione sostanzialmente equivalente a quello garantito nell'UE possa essere diluito dai trasferimenti successivi di dati a partire dal Regno Unito.**

88. **La quarta criticità** relativa ai trasferimenti successivi riguarda gli accordi internazionali conclusi, o che saranno conclusi in futuro, dal Regno Unito, e il possibile accesso diretto ai dati personali provenienti dal SEE da parte di autorità di paesi terzi aderenti a tali accordi. Infatti, l'EDPB nutre forti preoccupazioni in relazione all'Accordo UK-US CLOUD Act già concluso, e la stessa Commissione europea riconosce questa criticità sottolineando che "*la possibile entrata in vigore di questo accordo potrebbe influenzare il livello di protezione valutato in questa decisione*"[54]. Infatti, nel momento in cui entrerà in vigore, questo accordo prevede che i dati personali trasferiti dal SEE verso il Regno Unito nel quadro del progetto di decisione saranno soggetti alle disposizioni dell'accordo, il quale prevede alcune condizioni per l'accesso diretto da parte delle autorità statunitensi, influenzando il quadro giuridico del Regno Unito in materia di protezione dei dati, comprese le disposizioni sui trasferimenti successivi. In conseguenza di ciò, il livello di protezione offerto ai dati trasferiti dal SEE potrebbe essere significativamente influenzato dalle disposizioni dell'accordo concluso con gli Stati Uniti, incidendo sul livello di protezione di questi dati. L'EDPB osserva al riguardo che, nel considerando 153 del suo progetto di decisione, la Commissione europea rimanda alle spiegazioni offerte dalle autorità del Regno Unito, senza citare né fornire alcuna concreta assicurazione scritta o impegno, e senza indicare le specifiche disposizioni del diritto del Regno Unito che darebbero sostanza a tali spiegazioni.

89. L'EDPB ha sollevato in precedenza queste preoccupazioni in una lettera inviata al Parlamento europeo il 15 giugno 2020[55]. In quella sede, l'EDPB aveva sottolineato che sulla base dell'"*acquis dell'Unione nel campo della protezione dei dati, e in particolare il GDPR e la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie*" nutre delle riserve in merito all'applicazione delle garanzie nell'accordo per l'accesso ai dati personali nel Regno Unito in alcune circostanze che impongono obblighi di comunicazione verso gli Stati Uniti, e sulla sufficienza di queste garanzie alla luce delle norme dell'UE per non pregiudicare il livello di protezione previsto nell'UE.

90. Inoltre, le disposizioni dell'Accordo UK-US CLOUD Act possono influenzare significativamente le condizioni sostanziali e procedurali nell'ambito delle quali i dati personali detenuti da titolari o

[53] Cfr. *Schrems II*, paragrafo 134.
[54] Cfr. considerando 153 del progetto di decisione.
[55] Cfr. risposta dell'EDPB ai deputati al Parlamento europeo Sophie in't Veld e Moritz Körner sull'accordo tra Stati Uniti e Regno Unito nel quadro della legge US Cloud Act, adottata il 15 giugno 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

responsabili del trattamento nel Regno Unito possono essere oggetto di accesso diretto da parte delle autorità statunitensi, andando così a incidere sul livello di protezione garantito dalla legge del Regno Unito. Per fornire un livello di protezione sostanzialmente equivalente a quello garantito nel diritto dell'UE, ad esempio è "*essenziale che le garanzie previste da tale accordo prevedano obbligatoriamente un'autorizzazione giudiziaria preventiva quale garanzia essenziale per accedere ai metadati e ai dati di contenuto. Sulla base della sua valutazione preliminare, pur osservando che l'accordo fa riferimento all'applicazione della legge nazionale, l'EDPB non è stato in grado di individuare una disposizione chiara nell'accordo concluso tra il Regno Unito e gli Stati Uniti*"[56].

91. Benché la Commissione europea evidenzi che i dati ottenuti nell'ambito di questo accordo beneficerebbero di protezioni equivalenti alle garanzie specifiche previste nel cosiddetto "accordo quadro UE-USA", l'EDPB teme che l'inserimento di queste garanzie nell'Accordo UK-US CLOUD Act mediante un semplice riferimento applicabile *mutatis mutandis* possa non soddisfare i criteri di chiarezza, precisione e accessibilità delle norme in tema di accesso ai dati personali, o che possa non sancire queste garanzie in modo sufficiente a renderle efficaci e azionabili secondo il diritto del Regno Unito.

92. **L'EDPB raccomanda quindi che la Commissione europea chiarisca in quale modalità e sulla base di quale strumento giuridico avrebbero efficacia e natura vincolante nel diritto del Regno Unito le tutele equivalenti alle specifiche garanzie previste dall'accordo quadro UE-USA.**

93. L'EDPB osserva, inoltre, che le disposizioni dell'Accordo UK-US CLOUD Act, in combinato disposto con l'art. 3 della legge US CLOUD Act[57], sollevano dubbi sull'effettiva applicazione delle garanzie offerte dall'accordo per l'accesso, da parte delle autorità statunitensi preposte all'applicazione della legge, ai dati personali nel Regno Unito trattati da fornitori di servizi di comunicazioni elettroniche o di calcolo remoto (di seguito "CSP") che ricadono nella giurisdizione degli Stati Uniti. Infatti, qualora un CSP sito nel Regno Unito sia soggetto alla legge degli Stati Uniti (ad esempio in quanto società controllata di una società statunitense), rimane da accertare se le autorità statunitensi siano tenute ad applicare l'Accordo UK-US CLOUD Act per ottenere tali dati. Mentre la Commissione europea fa notare che *"[s]i presterà particolare attenzione all'applicazione e all'adattamento delle protezioni previste dall'accordo quadro alla specifica tipologia di trasferimenti oggetto dell'accordo tra Regno Unito e Stati Uniti",* l'EDPB sottolinea che dalla sua valutazione preliminare non è chiaro se le garanzie sancite nell'Accordo UK-US CLOUD Act, e quindi quelle previste dall'accordo quadro UE-USA, si applicherebbero a tutte le eventuali richieste di accesso ai dati nel Regno Unito effettuate dalle autorità statunitensi nel quadro della legge US CLOUD Act.

94. In futuro il Regno Unito potrà concludere altri accordi o impegni internazionali con paesi terzi, che si applicherebbero ai dati personali trasferiti dal SEE verso il Regno Unito nell'ambito del progetto di decisione[58]. A seconda delle disposizioni previste da tali accordi e dall'applicazione di specifiche clausole di salvaguardia, questi accordi internazionali, influenzando il quadro giuridico del Regno Unito in materia di protezione dei dati, potranno incidere significativamente anche sulle condizioni sostanziali e procedurali per l'accesso ai dati personali nel Regno Unito da parte di autorità di paesi terzi. Ciò vale in modo particolare per il progetto di secondo protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica (di seguito "Convenzione di Budapest") attualmente in fase di negoziazione tra le parti aderenti alla Convenzione, tra cui diversi paesi terzi. Infatti, il progetto di protocollo prevede alcune clausole che potranno essere attivate

[56] Cfr. la suddetta lettera dell'EDPB.
[57] Cfr. US CLOUD Act, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.
[58] Cfr. precedente sezione 2.3.3.

discrezionalmente dalle parti, ad esempio per quanto concerne l'autorizzazione a consentire l'accesso o meno ai dati di contenuto. Mentre tutti gli Stati membri dell'UE attiverebbero le clausole nel rispetto delle regole UE sulla protezione dei dati, non è stata data alcuna garanzia relativa al Regno Unito, che potrebbe discostarsi sostanzialmente dal livello di protezione in quel momento offerto nell'UE. Un altro esempio delle criticità presentate in precedenza è l'accordo tra il Regno Unito e il Giappone per un partenariato economico completo[59] ("CEPA"), il primo accordo commerciale del Regno Unito dopo la Brexit, entrato in vigore il 1 gennaio 2021[60] e che prevede disposizioni in materia di dati personali[61]. L'EDPB sottolinea inoltre che il 1 febbraio 2021 il Regno Unito ha formalmente annunciato la propria richiesta di aderire all'accordo globale e progressivo di partenariato transpacifico ("CPTPP"), che comprende l'accordo di partenariato transpacifico ("TPP")[62].

95. L'EDPB osserva che, a parte l'Accordo UK-US CLOUD Act, gli accordi internazionali sopra citati non sono esaminati nel progetto di decisione.

96. **L'EDPB esorta la Commissione europea a:**

- **esaminare l'interazione tra il quadro giuridico del Regno Unito in materia di protezione dei dati e i suoi impegni internazionali, oltre all'Accordo UK-US CLOUD Act, in particolare al fine di garantire la continuità del livello di protezione nel caso di trasferimenti successivi di dati personali dal SEE al Regno Unito sulla base della decisione di adeguatezza relativa al Regno Unito; e a monitorare costantemente e intervenire, ove necessario, nel caso siano conclusi altri accordi internazionali tra il Regno Unito e paesi terzi che rischiano di compromettere il livello di protezione dei dati personali previsto nell'UE;**

- **presentare all'EDPB impegni scritti assunti dalle autorità del Regno Unito e individuare le specifiche disposizioni nel diritto del Regno Unito in relazione ai chiarimenti forniti con riguardo alla possibile applicazione e attuazione dell'Accordo UK-US CLOUD Act, come indicato nel considerando 153 del progetto di decisione;**

- **al riguardo, monitorare se, in aggiunta alle garanzie che potrebbero essere fornite da un'adeguata applicazione dell'adattamento dell'accordo quadro UE-USA, l'Accordo UK-US CLOUD Act garantisce adeguate garanzie supplementari che tengano conto del livello di sensibilità delle categorie di dati interessati e dei requisiti particolarissimi previsti per il trasferimento di prove elettroniche direttamente dai CSP anziché tra autorità;**

- **valutare l'impatto e i possibili rischi delle disposizioni sui dati personali contenute negli accordi internazionali recentemente siglati dal Regno Unito, come il CEPA.**

---

[59] Cfr. UK/Japan: Agreement for a Comprehensive Economic Partnership [CS Japan No.1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] Cfr. orientamenti del governo del Regno Unito sugli accordi commerciali del Regno Unito con paesi terzi, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] Secondo l'articolo 8.80, paragrafo 5 del CEPA, le parti si impegnano a incoraggiare lo sviluppo di meccanismi intesi a promuovere la compatibilità dei loro differenti approcci giuridici alla protezione dei dati (personali). Secondo l'articolo 8.84, le parti si impegnano a non vietare e non limitare il trasferimento transfrontaliero di informazioni con strumenti elettronici, compresi i dati personali, quando questa attività è finalizzata allo svolgimento dell'attività d'impresa di un soggetto regolamentato ai sensi della CEPA.

[62] Ai sensi dell'articolo 14.11 paragrafo 2 del TPP, ciascuna parte consente il trasferimento transfrontaliero di informazioni con strumenti elettronici, compresi i dati personali, quando questa attività è finalizzata allo svolgimento dell'attività commerciale di un soggetto regolamentato.

97. **La quinta criticità** individuata riguarda l'applicazione di deroghe ai trasferimenti di dati personali verso paesi terzi. Benché le deroghe disponibili nel quadro del GDPR del Regno Unito siano le stesse previste dal GDPR, è importante che l'ICO applichi e continui ad applicare un'interpretazione relativa al ricorso a queste deroghe che sia in linea con quella dell'EDPB. In caso contrario, o qualora il Regno Unito si discosti in futuro da questa interpretazione, potrebbe sorgere il rischio di compromettere il livello di protezione dei dati trasferiti dal SEE verso paesi terzi attraverso il Regno Unito.

98. **L'EDPB invita la Commissione europea, nell'ambito della sua attività di monitoraggio, a verificare nello specifico che l'interpretazione del Regno Unito sul ricorso alle deroghe rimanga in linea con quella dell'UE. Qualora invece il Regno Unito segua un'interpretazione differente sul ricorso alle deroghe tale da pregiudicare il livello di protezione, è essenziale che la Commissione europea si attivi modificando la decisione di adeguatezza per accertarsi che il livello di protezione offerto ai dati personali del SEE trasferiti nel Regno Unito non sia compromesso nel caso in cui questi dati siano oggetto di un trasferimento successivo dal Regno Unito verso paesi terzi sulla base di un'interpretazione differente delle deroghe in questione.**

99. **La sesta criticità,** l'ultima di questa sezione, riguarda l'assenza, nel quadro giuridico del Regno Unito in materia di protezione dei dati, delle protezioni previste dall'articolo 48 del GDPR.

100. Nel suo progetto di decisione la Commissione europea chiarisce infatti che in assenza di regole sull'adeguatezza o di garanzie adeguate, un trasferimento è possibile unicamente sulla base delle deroghe previste dall'articolo 49 del GDPR del Regno Unito "*con l'eccezione dell'articolo 48 del regolamento (UE) 2016/679 che il Regno Unito ha deciso di non includere nel GDPR del Regno Unito"*[63]*.* L'assenza, nel quadro giuridico del Regno Unito in materia di protezione dei dati, di una disposizione sostanzialmente equivalente all'articolo 48 del GDPR, che riguardi i trasferimenti o le comunicazioni a seguito di una sentenza di un'autorità giurisdizionale o di una decisione di un'autorità amministrativa di un paese terzo, può dare origine a incertezza giuridica sulla possibilità che il livello di protezione dei dati personali trasferiti dal SEE verso il Regno Unito nell'ambito del progetto di decisione possa essere significativamente compromesso.

101. Nei suoi Criteri di riferimento per l'adeguatezza, l'EDPB sottolinea che, per quanto concerne i trasferimenti successivi, "*ulteriori trasferimenti dei dati personali da parte del destinatario del primo trasferimento dovrebbero essere consentiti soltanto quando anche il secondo destinatario è soggetto a norme che assicurano un livello di protezione adeguato e prevedono il rispetto delle istruzioni pertinenti durante il trattamento dei dati per conto del titolare del trattamento*"[64]. Inoltre, l'EDPB sottolinea che "*spetta al primo destinatario dei dati trasferiti dall'UE assicurare che siano previste garanzie adeguate per i trasferimenti successivi dei dati in mancanza di una decisione di adeguatezza. Tali trasferimenti successivi di dati dovrebbero essere possibili soltanto per finalità determinate e limitate e purché sussista una base giuridica per il trattamento*"[65]. All'interno del capo V del GDPR, l'articolo 48 deve essere considerato appieno nel valutare se il quadro giuridico del Regno Unito assicuri un livello di protezione sostanzialmente equivalente al riguardo[66].

102. Al riguardo, l'EDPB sottolinea la giurisprudenza della Corte relativa al rischio di uso improprio o accesso e utilizzo illecito dei dati, affermando in particolare che "*Quanto al livello di protezione delle*

[63] Cfr. nota a piè di pagina 78 del progetto di decisione.
[64] Cfr. WP254 rev.01, pag. 6.
[65] Cfr. WP254 rev.01, pag. 6.
[66] Cfr. articolo 44 del GDPR, ultima frase, in particolare: "*Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato*".

libertà e dei diritti fondamentali garantito all'interno dell'Unione, una normativa della medesima che comporta un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta deve prevedere, secondo la giurisprudenza costante della Corte, regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi"[67].

103. L'EDPB fa notare al riguardo che, sulla base delle informazioni disponibili nel progetto di decisione, il quadro giuridico del Regno Unito in materia di protezione dei dati non stabilisce chiaramente che la sentenza di una corte o un tribunale o la decisione di un'autorità amministrativa di un paese terzo che impone a un titolare del trattamento o un responsabile del trattamento il trasferimento o la comunicazione di dati personali possa essere riconosciuta o comunque azionabile unicamente se basata su un accordo internazionale in essere tra il paese terzo richiedente e il Regno Unito. L'articolo 48 del GDPR rappresenta una disposizione essenziale nel capo V del GDPR in quanto impone che il trasferimento o la comunicazione di dati personali a seguito di sentenza o decisione di una corte, di un tribunale o un'autorità amministrativa di un paese terzo possano essere riconosciuti o azionabili unicamente se basati su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o uno Stato membro, fatti salvi gli altri motivi di trasferimento previsti dal capo V del GDPR. L'EDPB ricorda infatti che "*una richiesta proveniente da un'autorità estera non costituisce di per sé base giuridica per il trasferimento. L'ordine può essere riconosciuto unicamente "se basato su un accordo internazionale come, ad esempio, un trattato di mutua assistenza giudiziaria in vigore tra il paese terzo richiedente e l'Unione o uno Stato membro*""[68]. È quindi fondamentale poter individuare nel diritto del Regno Unito disposizioni sostanzialmente equivalenti.

104. Nel progetto di decisione, la Commissione europea riferisce le spiegazioni fornite dalle autorità del Regno Unito secondo le quali a norma della legge (scritta o non scritta), una sentenza estera che richieda di fornire dati non è azionabile nel Regno Unito senza un accordo internazionale, e qualunque trasferimento di dati su richiesta di un tribunale o un'autorità amministrativa estera necessita di uno strumento di trasferimento, come, ad esempio, una norma sull'adeguatezza o garanzie adeguate, salvo ove si applichi la deroga prevista dall'articolo 49 del GDPR del Regno Unito. Non essendogli state messe a disposizione le interlocuzioni tra la Commissione europea e le autorità del Regno Unito[69] al riguardo, l'EDPB non è quindi in grado di analizzare e valutare in modo indipendente se le garanzie previste dalle autorità del Regno Unito siano sufficienti ad assicurare un livello di protezione sostanzialmente equivalente in relazione alle garanzie contenute nell'articolo 48 del GDPR.

105. **L'EDPB invita la Commissione europea a presentare ulteriori assicurazioni e specifici riferimenti alla normativa del Regno Unito che garantiscano che il livello di protezione previsto dal quadro giuridico del Regno Unito sia sostanzialmente equivalente a quello garantito nel SEE. Per questo motivo l'EDPB esorta la Commissione europea a presentare spiegazioni scritte e impegni assunti**

[67] Cfr. *Schrems I*, paragrafo 91.
[68] Cfr. l'allegato alla Risposta congiunta di EDPB e GEPD alla Commissione LIBE sulle implicazioni della legge US CLOUD Act sul quadro giuridico europeo per la protezione dei dati, adottata il 10 luglio 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.
[69] Cfr. nota a piè di pagina 78 del progetto di decisione.

da parte delle autorità del Regno Unito in merito all'applicazione di tutele sostanzialmente equivalenti a quelle previste dall'articolo 48 del GDPR.

106. **L'EDPB ritiene che l'individuazione di disposizioni nel diritto del Regno Unito che assicurino un livello di protezione sostanzialmente equivalente in relazione alle garanzie contenute nell'articolo 48 del GDPR sia tanto più importante alla luce delle criticità sollevate in precedenza rispetto alle richieste di accesso ai dati nel Regno Unito presentate da autorità statunitensi o di altri paesi terzi, e considerato che, in forza della decisione di adeguatezza, i dati personali potrebbero essere trasferiti dal SEE verso il Regno Unito senza altre garanzie o impegni vincolanti del destinatario in relazione alle richieste di accesso ai dati presentate da altre autorità di paesi terzi.**

3.2. Meccanismi procedurali e di *enforcement*

107. Sulla base dei criteri stabiliti nei Criteri di riferimento per l'adeguatezza, l'EDPB ha analizzato i seguenti aspetti del quadro giuridico del Regno Unito in materia di protezione dei dati trattati nel progetto di decisione: l'esistenza e l'effettivo funzionamento di un'autorità di controllo indipendente; l'esistenza di un sistema che garantisce un buon livello di conformità; e un sistema di accesso a opportuni meccanismi di ricorso che conferiscono ai cittadini nel SEE gli strumenti per far valere i propri diritti e presentare ricorso senza incontrare onerose barriere per un ricorso amministrativo e giudiziario.

3.2.1 Autorità di controllo indipendente competente

108. L'EDPB accoglie con favore gli sforzi profusi dalla Commissione europea per esaminare estesamente l'istituzione, il funzionamento e i poteri dell'autorità di controllo del Regno Unito nel capitolo 2.6. del progetto di decisione. Nel Regno Unito, l'Information Commissioner (di seguito "IC") è incaricato di vigilare su e far applicare il GDPR del Regno Unito e la DPA 2018. Secondo l'allegato 12 della DPA 2018, l'IC è una "Corporation Sole", ovvero un soggetto con personalità giuridica distinta costituito da un'unica persona, supportato da un ufficio, l'ICO.

109. Per quanto concerne l'indipendenza dell'IC, l'EDPB sottolinea che l'articolo 51 del GDPR del Regno Unito non chiarisce espressamente che l'IC sia un'autorità pubblica indipendente, come invece specificato nell'articolo 51 del GDPR per le autorità di controllo. L'EDPB riconosce comunque che nel suo articolo 52 il GDPR del Regno Unito riprende in modo simile le corrispondenti regole in materia di indipendenza previste dall'articolo 52, paragrafi da 1 a 3 del GDPR.

110. Inoltre, l'EDPB segnala che l'articolo 52 del GDPR del Regno Unito non presenta obblighi corrispondenti all'articolo 52, paragrafi da 4 a 6 del GDPR che assicurino espressamente che alla rispettiva autorità di controllo siano messe a disposizione le risorse necessarie per l'effettivo svolgimento dei suoi compiti e l'esercizio dei suoi poteri. L'EDPB riconosce tuttavia che la DPA 2018 contiene disposizioni tese a garantire un adeguato finanziamento dell'ICO[70], e la circostanza che, a oggi, l'ICO è una delle autorità di controllo più grandi rispetto a quelle all'interno dell'UE e del SEE. Poiché la costante destinazione di risorse adeguate, in particolare per quanto concerne il personale e gli stanziamenti[71], è essenziale per assicurare il corretto funzionamento di un'autorità di controllo che possa adempiere tutte le attività ad essa assegnate, come anche evidenziato di recente dal

[70] Cfr. artt. 137, 138, 182 e allegato 12, paragrafo 9 della DPA 2018.
[71] Cfr. WP 254 rev.01, pag. 7.

Parlamento europeo[72], l'EDPB ritiene essenziale prestare particolare attenzione agli sviluppi futuri su questo fronte.

111. **Pertanto, l'EDPB invita la Commissione europea a monitorare gli eventuali sviluppi relativi all'assegnazione di risorse all'ICO che potrebbero compromettere l'effettivo svolgimento delle attività dell'ICO.**

3.2.2. Esistenza di un sistema di protezione dei dati che garantisce un buon livello di conformità

112. Il progetto di decisione contiene un esame approfondito dei poteri conferiti all'ICO dall'articolo 58 del GDPR del Regno Unito e dalla DPA 2018 con lo scopo di assicurare il monitoraggio e l'applicazione della legislazione. L'EDPB riconosce che l'articolo 58 del GDPR del Regno Unito presenta forti analogie con le corrispondenti regole relative ai poteri delle autorità di controllo stabiliti nell'articolo 58 del GDPR. Per quanto concerne la facoltà di imporre sanzioni amministrative a seconda delle circostanze di ogni specifico caso, l'articolo 83 del GDPR del Regno Unito prevede disposizioni e importi massimi simili a quelle previste dall'articolo 83 del GDPR. Per questo motivo, sotto questo aspetto, l'EDPB ritiene che il quadro giuridico del Regno Unito sia attualmente allineato alle norme stabilite nel diritto dell'UE in materia. Al riguardo, l'EDPB sottolinea comunque che l'esistenza di sanzioni *efficaci* è importante per assicurare il rispetto delle regole[73].

113. **Alla luce di quanto precede, l'EDPB invita la Commissione a monitorare l'efficacia delle sanzioni e dei relativi rimedi nel quadro giuridico del Regno Unito in materia di protezione dei dati.**

3.2.3. Il sistema di protezione dei dati deve offrire supporto e assistenza agli interessati per l'esercizio dei loro diritti e opportuni meccanismi di ricorso

114. Un efficace meccanismo di supervisione, che consenta un esame indipendente dei reclami al fine di individuare e punire nella pratica le violazioni dei diritti degli interessati, e strumenti efficaci di ricorso amministrativo e giudiziario (compreso il risarcimento del danno a seguito di trattamento illecito dei dati personali dell'interessato) sono elementi essenziali per valutare se un sistema di protezione dei dati offra un livello adeguato di protezione.

115. L'EDPB constata con favore che sul suo sito web l'ICO presenta dettagliate informazioni e indicazioni, con l'obiettivo di sensibilizzare i titolari e i responsabili del trattamento in merito ai loro obblighi e doveri, e aiutare gli interessati a informarsi sui propri diritti relativi ai dati personali e far valere i propri diritti come previsti dal GDPR del Regno Unito e dalla DPA 2018.

116. **Ciò nonostante, l'EDPB esorta la Commissione europea a tenere sotto costante osservazione il livello di supporto offerto dall'ICO, in particolare alle persone fisiche i cui dati sono stati trasferiti nel Regno Unito nell'ambito della decisione di adeguatezza, per aiutarle ad esercitare i loro diritti come previsti dal regime di protezione dei dati del Regno Unito.**

[72] Risoluzione del Parlamento europeo del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione, paragrafo 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_IT.html.
[73] Cfr. WP 254 rev.01, pag. 7.

4. ACCESSO E UTILIZZO DI DATI PERSONALI TRASFERITI DALL'UE DA PARTE DELLE AUTORITÀ PUBBLICHE NEL REGNO UNITO

4.1. Accesso e utilizzo da parte delle autorità pubbliche del Regno Unito per finalità di contrasto in materia penale

4.1.1. Basi giuridiche e limitazioni/garanzie applicabili

117. Per quanto concerne la valutazione eseguita dalla Commissione europea e documentata nei considerando 132 e seguenti del progetto di decisione **in merito all'accesso per finalità di contrasto**, la Commissione europea presenta informazioni specifiche e dettagliate, e in generale giunge a conclusioni comprensibili. Per questo motivo l'EDPB si astiene dal riprodurre nel presente parere la maggior parte dei riscontri fattuali e delle valutazioni. Vi sono tuttavia alcuni casi in cui l'illustrazione dei fatti o la spiegazione delle conclusioni non sono sufficienti per consentire all'EDPB di supportarle appieno.

4.1.1.1. Uso del consenso

118. L'EDPB osserva che nella nota a piè di pagina 184 del progetto di decisione[74] la Commissione europea asserisce che **il ricorso al consenso** non è rilevante in uno scenario di adeguatezza, in quanto nelle situazioni di trasferimento la raccolta dei dati da parte di un'autorità di contrasto del Regno Unito non avviene direttamente presso l'interessato sulla base del consenso. Per questo motivo, la Commissione europea non valuta l'uso del consenso come base giuridica nelle attività di contrasto.

119. Al riguardo, l'EDPB ricorda che l'articolo 45, paragrafo 2, lettera a) del GDPR impone di valutare un ampio ventaglio di elementi che non si limitano alla sola situazione di trasferimento tra cui "*lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di [...] diritto penale*".

120. L'EDPB osserva, anche sulla base delle informazioni fornite dalla Commissione europea nel considerando 38 del progetto di decisione di esecuzione a norma della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio relativa all'adeguata protezione dei dati personali da parte del Regno Unito (di seguito "progetto di decisione di adeguatezza secondo la LED"), che l'uso del consenso, come delineato nel regime del Regno Unito nel contesto dell'attività di contrasto, richiederebbe sempre l'esistenza di una base giuridica. Ciò significa che anche se le autorità di polizia sono autorizzate per legge a trattare i dati per scopi di indagine, in alcune circostanze specifiche (ad esempio per raccogliere un campione di DNA), possono ritenere opportuno chiedere il consenso dell'interessato.

121. **L'EDPB invita la Commissione europea a introdurre nella decisione di adeguatezza la propria analisi sul possibile uso del consenso in un contesto di attività di contrasto, previsto nel progetto di decisione di adeguatezza secondo la LED**.

4.1.1.2. Mandati di perquisizione e ordini di esibizione

122. Pur in assenza di osservazioni da parte dell'EDPB sul reperimento di elementi di prova da parte delle autorità di polizia attraverso mandati di perquisizione e ordini di esibizione in generale, dal considerando 136 del progetto di decisione emerge che la Commissione europea ha concentrato le proprie valutazioni relative all'accesso per motivi di contrasto sulle autorità di polizia, e che invece è

[74] Cfr. pag. 37 del progetto di decisione.

stato esaminato in minor misura il trattamento di dati personali da parte di altre agenzie preposte all'applicazione della legge.

123. Ad esempio, nell'Explanatory Framework for Adequacy Discussions del Regno Unito, Section F: Law Enforcement[75], a pagina 11 si suggerisce che **la National Crime Agency** (di seguito "NCA") potrebbe essere un'agenzia preposta all'applicazione della legge di particolare interesse, che svolge tra l'altro una più ampia funzione di intelligence criminale. La NCA descrive la propria missione come l'aggregazione di informazioni provenienti da varie fonti per massimizzare le opportunità di analisi, valutazione e tattiche, anche dall'intercettazione tecnica delle comunicazioni, da partner per il contrasto nel Regno Unito e all'estero, da agenzie di sicurezza e di intelligence[76]. La NCA è anche uno dei principali interlocutori dei partner internazionali di contrasto, e ha un ruolo fondamentale nello scambio di informazioni di intelligence criminale[77].

124. L'EDPB prende inoltre nota del fatto che anche la Government Communications Headquarters (di seguito "GCHQ"), le cui attività ricadono solitamente nell'ambito della parte 4 della DPA 2018, ovvero la sicurezza nazionale, svolge anche un ruolo attivo nel ridurre il danno sociale e finanziario che la criminalità grave e organizzata causa nel Regno Unito, collaborando da vicino con l'Home Office, la NCA, l'HM Revenue and Customs ("HMRC") e altri enti della pubblica amministrazione[78]. Le sue attività riguardano il contrasto all'abuso sessuale su minori; frodi; altre tipologie di reati economici, tra cui il riciclaggio di denaro; uso criminale delle tecnologie; criminalità informatica; criminalità organizzata relativa all'immigrazione, tra cui la tratta di esseri umani; e attività illecite di contrabbando di droghe, armi e altro.

125. **L'EDPB invita la Commissione europea a integrare la sua analisi con un'analisi delle agenzie attive nel campo del contrasto per le quali la raccolta e l'analisi di dati, anche di dati personali, sembrino un aspetto centrale dell' operatività quotidiana, in particolare la NCA. Inoltre, l'EDPB invita la Commissione europea a esaminare con maggiore attenzione le agenzie come la GCHQ, le cui**

[75] Cfr. governo del Regno Unito, Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement, 13 marzo 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[76] Cfr. sito web della National Crime Agency, Intelligence: enhancing the picture of serious organised crime affecting the UK, https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[77] Benché non tutti i dati di intelligence elaborati dalla NCA costituiscano dati personali, una buona parte potrebbe essere rappresentata da informazioni personali e le attività qui descritte differiscono dalle classiche attività di polizia, pertanto un'analisi dell'accesso ai dati personali da parte delle autorità di contrasto nel Regno Unito non sarebbe completa senza un'approfondita valutazione delle attività della NCA. Sembra ragionevole accertarsi che i principi di protezione dei dati abbiano il medesimo significato in tutte le agenzie preposte all'applicazione della legge, gettando quindi una luce su un'agenzia particolarmente orientata ai dati come la NCA. Inoltre, "guardando al futuro", continua la spiegazione, *"[s]iamo alla costante ricerca di nuove opportunità per raccogliere, sviluppare e migliorare capacità tradizionali al fine di incrementare la quantità e la qualità delle informazioni di intelligence disponibili da sfruttare sia nel Regno Unito sia all'estero". "Nell'ambito di ciò, stiamo sviluppando la nuova capacità nazionale di utilizzo dei dati, sfruttando le facoltà conferite all'agenzia dalla legge Crime and Courts Act, al fine di collegare insieme, accedere e sfruttare i dati posseduti da vari enti della pubblica amministrazione*". [...] "*Tutto ciò migliorerà la nostra agilità e flessibilità nel rispondere alle nuove minacce e agire in modo proattivo, raccogliere e analizzare informazioni e informazioni di intelligence sulle minacce emergenti, in modo da poter intervenire prima che si concretizzino*".

[78] Cfr. sito web della GCHQ, Mission, Serious and Organised Crime, https://www.gchq.gov.uk/section/mission/serious-crime.

attività ricadono nel campo del contrasto e della sicurezza nazionale, e il quadro giuridico a cui sono sottoposte in tema di trattamento dei dati personali.

4.1.1.3. Poteri investigativi per finalità di contrasto

126. Secondo il capitolo 4 dei Criteri di riferimento per l'adeguatezza "Garanzie sostanziali nei **paesi terzi per l'accesso a fini di contrasto** e di sicurezza nazionale allo scopo di limitare le ingerenze nei diritti fondamentali", l'EDPB ricorda che *"[a] tale proposito, la Corte ha anche osservato in tono critico che la precedente decisione "Safe Harbor" "non contiene alcuna dichiarazione quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione europea verso gli Stati Uniti**, ingerenze che entità statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi**, come la sicurezza nazionale*""[79]. Nei suoi Criteri di riferimento, l'EDPB afferma che **tutti i paesi terzi devono rispettare le quattro garanzie essenziali europee**[80] **affinché l'accesso ai dati, sia per** finalità di sicurezza nazionale sia **per finalità di contrasto, possa essere considerato adeguato**, e in particolare **deve essere dimostrata la necessità e la proporzionalità con riguardo ai legittimi obiettivi perseguiti.**

127. In questa sezione del progetto di decisione, la Commissione europea conclude che (considerando 139) "*poiché i poteri investigativi previsti dall'IPA 2016 sono identici a quelli a disposizione delle agenzie di sicurezza nazionale, le condizioni, le limitazioni e le garanzie applicabili a questi poteri sono trattate in dettaglio nella sezione relativa all'accesso e all'uso dei dati personali da parte delle autorità pubbliche del Regno Unito per finalità di sicurezza nazionale*". Ad ogni modo, dalla giurisprudenza della Corte deriva che, in sede di applicazione del test della necessità e della proporzionalità alla legislazione degli Stati membri che autorizza la conservazione e l'accesso ai dati personali da parte delle autorità pubbliche, le finalità legittime, come ad esempio la sicurezza nazionale o il contrasto alla criminalità grave, sono differenti, e pertanto un certo tipo di interferenza potrebbe essere giustificato, mentre un altro non esserlo[81].

128. **L'EDPB accoglierebbe pertanto con favore, all'interno della decisione, una valutazione specifica della necessità e della proporzionalità delle condizioni, limitazioni e garanzie di cui ai considerando 174 e seguenti – che è una sezione dedicata alle misure che perseguono obiettivi di sicurezza nazionale – quando si tratta di applicare tali condizioni, limitazioni e garanzie nel contesto di una misura che persegue un obiettivo di contrasto. Invita quindi la Commissione europea a chiarire ulteriormente se la conservazione descritta di dati personali e l'accesso ad essi per finalità di contrasto sono sufficientemente limitati per assicurare un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE.**

4.1.2. Ulteriore uso delle informazioni raccolte per finalità di contrasto (considerando 140-154)

129. L'EDPB osserva che il quadro giuridico del Regno Unito in materia di protezione dei dati prevede garanzie e limitazioni simili a quelle previste dalla normativa UE in relazione all'ulteriore uso delle informazioni raccolte per finalità di contrasto.

[79] Cfr. WP254 rev.01, pag. 9.
[80] Cfr. Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza dell'EDPB.
[81] Cfr. Corte di giustizia dell'Unione europea, cause congiunte C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*, 6 ottobre 2020, ECLI:EU:C:2020:791.

4.1.2.1. Ulteriore uso per altre finalità di contrasto

130. La DPA 2018 prevede infatti che i dati personali raccolti da un'autorità competente per finalità di contrasto possono essere ulteriormente trattati (dal titolare del trattamento originario o da un altro titolare del trattamento) per qualunque altra finalità di contrasto, a condizione che il titolare del trattamento sia autorizzato per legge a trattare i dati per l'altra finalità, e il trattamento sia necessario e proporzionato per quella finalità. La Commissione europea osserva che al trattamento eseguito dall'autorità ricevente si applicano tutte le garanzie previste dalla parte 3 della DPA 2018. L'EDPB sottolinea invece che, nella parte 3 della DPA 2018, gli articoli 44(4), 45(4), 48(3) e 68(7) prevedono la possibilità di limitare i diritti dell'interessato, e che l'art. 79 prevede la possibilità di rilasciare dei certificati che attestano la necessità e proporzionalità di una restrizione quale misura per proteggere la sicurezza nazionale. **L'EDPB raccomanda quindi alla Commissione europea di valutare ulteriormente il possibile impatto di queste restrizioni sul livello di protezione dei dati personali in relazione all'ulteriore utilizzo delle informazioni raccolte. Analogamente, dovrebbero essere forniti ulteriori chiarimenti anche in relazione al quadro giuridico del Regno Unito che consente questa successiva condivisione, in particolare la legge Digital Economy Act 2017, e la legge Crime and Courts Act 2013 che consente la condivisione delle informazioni con la NCA.**

4.1.2.2. Ulteriore uso per finalità diverse dal contrasto nel Regno Unito

131. La DPA 2018 prevede anche che i dati personali raccolti per qualunque finalità di contrasto possano essere trattati per finalità che non costituiscono contrasto se il trattamento è consentito dalla legge. In questa eventualità, la base giuridica che autorizza la condivisione è rappresentata dall'art. 19 della legge Counter-Terrorism Act 2008. In proposito, l'EDPB osserva che l'ambito di applicazione e le disposizioni dell'art. 19 della legge Counter-Terrorism Act non sono esaminati pienamente nella valutazione della Commissione europea, e che tale articolo potrebbe implicare un ulteriore utilizzo più ampio, in particolare per quanto concerne il paragrafo (2) dell'art. 19, il quale prevede che "*[l]e informazioni ottenute da qualunque servizio di intelligence in relazione all'esercizio di una delle sue funzioni possono essere utilizzate da quel servizio in relazione all'esercizio di qualunque altra sua funzione*".

132. L'EDPB osserva inoltre che il riferimento da parte della Commissione europea al fatto che le autorità competenti siano autorità pubbliche che devono agire nel rispetto della CEDU, compreso il relativo articolo 8, assicurando quindi che tutte le condivisioni di dati tra le agenzie preposte alle attività di contrasto e i servizi di intelligence siano conformi alla normativa sulla protezione dei dati, e alla CEDU, potrebbe essere ulteriormente comprovato individuando le pertinenti leggi e gli atti normativi nell'ordinamento giuridico del Regno Unito che stabiliscono chiaramente e precisamente queste limitazioni.

4.1.2.3. Ulteriore uso nel contesto di trasferimenti successivi al di fuori del Regno Unito

133. Benché la Commissione europea abbia menzionato il fatto che l'Accordo UK-US CLOUD Act possa influenzare i trasferimenti successivi verso gli Stati Uniti da CSP presenti nel Regno Unito, l'EDPB sottolinea che l'entrata in vigore di questo accordo potrebbe influenzare anche l'ulteriore uso delle informazioni raccolte, attraverso trasferimenti successivi dalle autorità di contrasto nel Regno Unito, in particolare in relazione all'emanazione e alla trasmissione di ordini a norma dell'articolo 5 dell'Accordo UK-US CLOUD Act.

134. Più in generale, l'EDPB ritiene che la conclusione di futuri accordi bilaterali con paesi terzi per finalità di cooperazione in ambito di contrasto, che prevedono una base giuridica per il trasferimento di dati personali verso questi paesi, possano incidere anche significativamente sulle condizioni dell'ulteriore utilizzo delle informazioni raccolte, poiché questi accordi possono influenzare il quadro giuridico del

Regno Unito in materia di protezione dei dati esaminato. L'EDPB consiglia quindi alla Commissione europea di valutare ulteriormente questo aspetto, individuando l'esistenza di accordi internazionali, e chiarire se le disposizioni di questi accordi possano influenzare l'applicazione della normativa del Regno Unito in materia di protezione dei dati e se prevedono altre limitazioni o esenzioni in relazione all'ulteriore uso e alla diffusione all'estero di informazioni raccolte per finalità di contrasto. L'EDPB ritiene che queste informazioni e la valutazione siano essenziali per consentire una valutazione completa del livello di protezione offerto dal quadro giuridico del Regno Unito e dalle relative prassi con riguardo alla trasmissione dei dati all'estero e al loro ulteriore utilizzo.

4.1.3. Vigilanza

135. L'EDPB osserva che la vigilanza sulle agenzie di contrasto in materia penale è assicurata da una combinazione di diversi Commissioner, in aggiunta all'ICO. Il progetto di decisione di adeguatezza menziona l'IPC, il Commissioner for the Retention and Use of Biometric Material, e il Surveillance Camera Commissioner. In proposito, occorre far notare che la Corte ha ripetutamente sottolineato l'esigenza di una vigilanza indipendente. Particolarmente importante per l'aspetto dell'accesso ai dati personali trasferiti verso il Regno Unito è l'IPC. A quanto risulta all'EDPB, l'IPC è un cosiddetto "commissario giudiziario" (judicial commissioner), come altri commissari giudiziari, a cui si fa riferimento nel contesto del capitolo sulla sicurezza nazionale, e che questi commissari giudiziari godono dell'indipendenza propria dei giudici, anche quando svolgono funzioni di commissario. Per quanto concerne la funzione dell'IPC, nel considerando 245 del progetto di decisione la Commissione europea spiega che esso funziona in modo indipendente, come "organismo parastatale" (arm's length body), pur essendo finanziato dall'Home Office.

136. L'EDPB non ha rilevato nel progetto di decisione ulteriori indicazioni per valutare l'indipendenza del Commissioner for the Retention and Use of Biometric Material, né del Surveillance Camera Commissioner.

137. **La Commissione europea è invitata a valutare ulteriormente l'indipendenza dei commissari giudiziari, anche nei casi dove il commissario non svolge (più) funzioni giudicanti, e a valutare l'indipendenza del Commissioner for the Retention and Use of Biometric Material e del Surveillance Camera Commissioner.**

4.2. Quadro giuridico generale in materia di protezione dei dati nel campo della sicurezza nazionale

4.2.1. Certificati di sicurezza nazionale

138. A norma dell'art. 111 della DPA 2018, i titolari del trattamento possono richiedere certificati di sicurezza nazionale che sono rilasciati da un ministro, membro del governo, dal Procuratore generale o dall'Avvocato generale per la Scozia, e attestano che le esenzioni dagli obblighi e dai diritti sanciti nelle parti da 4 a 6 della DPA 2018 rappresentano una misura necessaria e proporzionata per la protezione della sicurezza nazionale. Questi certificati intendono dare ai titolari del trattamento maggiore certezza giuridica, e rappresenteranno prova definitiva del fatto che il trattamento dei dati personali ricade nel campo della sicurezza nazionale. Tuttavia, occorre menzionare che questi

certificati non sono obbligatori per potersi avvalere delle esenzioni ai fini di sicurezza nazionale, ma al contrario rappresentano una misura di trasparenza[82].

139. Dall'allegato 20 della DPA 2018, sezione 17 e 18 l'EDPB deduce che l'efficacia di un certificato di sicurezza nazionale rilasciato a norma della legge Data Protection Act 1998 (di seguito "vecchio certificato") era stata estesa fino al 25 maggio 2019 al trattamento dei dati personali a norma della DPA 2018. Fino a quella data, salvo sostituzione o revoca, i vecchi certificati sono stati trattati come se fossero stati rilasciati a norma della DPA 2018.

140. Tuttavia, in assenza di una data di scadenza specificata nel certificato di sicurezza nazionale rilasciato a norma della legge Data Protection Act 1998, l'EDPB deduce che tale certificato continuerà ad applicarsi al trattamento eseguito ai sensi della legge Data Protection Act 1998, salvo revoca o annullamento del certificato[83]. Anche se la protezione offerta da questi vecchi certificati è limitata al trattamento dei dati personali nell'ambito della legge Data Protection Act 1998, l'EDPB osserva che, a norma della legge Data Protection Act 1998, possono essere rilasciati nuovi certificati di sicurezza nazionale per i dati personali che sono stati trattati nel quadro di questa legge[84].

141. **Ai fini di completezza, l'EDPB invita la Commissione europea a chiarire nel suo progetto di decisione che è ancora possibile rilasciare certificati nazionali a norma della legge Data Protection Act 1998. Inoltre, la esorta a descrivere nel suo progetto di decisione i meccanismi di ricorso e di vigilanza relativi ai certificati rilasciati a norma della legge Data Protection Act 1998. Infine, la invita a inserire nel progetto di decisione il numero di certificati esistenti rilasciati a norma della legge Data Protection Act 1998, e a tenere sotto attenta osservazione questo aspetto.**

4.2.2. Diritto di rettifica e cancellazione

142. Con riguardo al diritto di rettifica e cancellazione, l'EDPB osserva che, come previsto dall'art. 100 e dall'art. 149 della DPA 2018, gli interessati hanno la possibilità di rivolgersi alla High Court (in Scozia, la Court of Session) per ordinare a un titolare del trattamento di rettificare o cancellare i loro dati senza ingiustificato ritardo.

143. **L'EDPB sottolinea che l'esercizio dei diritti degli interessati deve essere assicurato in modo efficace; invita quindi la Commissione europea a descrivere nel suo progetto di decisione in che modo l'art. 100 della DPA 2018 operi nella pratica, e a monitorare attentamente l'applicazione di tale articolo.**

4.2.3. Esenzioni per scopi di sicurezza nazionale

144. L'EDPB desidera attirare l'attenzione sull'art.110 della DPA 2018, e in particolare l'allegato 11, che stabilisce le finalità specifiche per le quali i servizi di intelligence possono derogare a taluni principi

[82] Cfr. Home Office, The Data Protection Act 2018, National Security Certificates guidance, agosto 2020, paragrafo 4, pag. 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.
[83] Cfr. Home Office, The Data Protection Act 2018, National Security Certificates guidance, agosto 2020, pag. 5.
[84] Cfr. Home Office, The Data Protection Act 2018, National Security Certificates guidance, agosto 2020, paragrafo 8, pag. 5.

di protezione dei dati, anche in relazione ai diritti degli interessati, e non sono obbligati a comunicare all'ICO le violazioni dei dati personali[85].

145. L'**EDPB invita la Commissione europea a chiarire ulteriormente l'ambito delle esenzioni, non essendo chiaro se tutte le esenzioni previste dall'allegato 11 della DPA 2018 siano rilevanti per l'attività dei servizi di intelligence, e se esse assicurano l'equivalenza con il principio di necessità e proporzionalità**. In particolare, **l'EDPB invita la Commissione europea a fornire ulteriori chiarimenti in merito alle circostanze in cui un servizio di intelligence potrebbe applicare l'art. 10 dell'allegato 11 della DPA 2018, il quale afferma che "*[l]e disposizioni elencate non si applicano ai dati personali che consistono di registrazioni delle intenzioni del titolare del trattamento in relazione a trattative con l'interessato nella misura in cui l'applicazione delle disposizioni elencate potrebbe pregiudicare le trattative*".**

4.3. Accesso e uso da parte delle autorità pubbliche del Regno Unito per finalità di sicurezza nazionale

146. Come osservazione generale, l'EDPB prende atto che gli Stati hanno un ampio margine di discrezionalità nelle questioni di sicurezza nazionale, come riconosciuto anche dalla Corte EDU. L'EDPB ricorda inoltre che, come sottolineato nelle sue raccomandazioni aggiornate sulle garanzie essenziali europee per le misure di sorveglianza[86], l'articolo 6, paragrafo 3 del trattato sull'Unione europea stabilisce che i diritti fondamentali sanciti nella CEDU costituiscono principi generali del diritto dell'UE. Tuttavia, come ricorda la Corte nella sua giurisprudenza, quest'ultima non costituisce, fintanto che l'UE non vi avrà aderito, uno strumento giuridico formalmente incorporato nel diritto dell'UE[87]. Il livello di protezione dei diritti fondamentali richiesto dall'articolo 45 del GDPR deve essere determinato sulla base delle disposizioni di quel regolamento, lette alla luce dei diritti fondamentali sanciti nella Carta dell'UE. Ciò detto, secondo l'articolo 52, paragrafo 3 della Carta dell'UE, i diritti in essa specificati che corrispondono ai diritti garantiti dalla CEDU devono avere lo stesso significato e ambito di applicazione di quelli previsti dalla CEDU. Per questo motivo, come ricordato dalla Corte, occorre considerare la giurisprudenza della Corte EDU per quanto concerne i diritti che sono previsti anche nella Carta dell'UE quale soglia minima di protezione per interpretare i corrispondenti diritti nella Carta dell'UE[88]. Secondo l'ultima frase dell'articolo 52, paragrafo 3 della Carta dell'UE, tuttavia, *"[l]a presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa*".

147. Per questo motivo, nella valutazione che segue, l'EDPB ha tenuto conto della giurisprudenza della Corte EDU, nella misura in cui la Carta dell'UE, come interpretata dalla Corte, non fornisce un livello di protezione più elevato che prescrive obblighi diversi rispetto a quelli della giurisprudenza della Corte EDU.

---

[85] Queste finalità sono la prevenzione e la rilevazione dei "reati", "informazioni che devono essere comunicate per legge ecc. o in relazione a procedimenti legali", "privilegio parlamentare", "procedimenti giudiziari", "onori e dignità reali", "forze armate", "benessere economico", "privilegio professionale legale", "negoziati", "referenze riservate date dal titolare del trattamento", "elaborati e voti d'esame", "ricerca e statistiche" e "archiviazione nell'interesse pubblico".

[86] Cfr. Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza dell'EDPB.

[87] Cfr. *Schrems II*, paragrafo 98.

[88] Cfr. Corte di giustizia dell'Unione europea, cause congiunte C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*, 6 ottobre 2020, ECLI:EU:C:2020:791, paragrafo 124.

4.3.1. Basi giuridiche, limitazioni e garanzie - Poteri investigativi esercitati nel contesto della sicurezza nazionale

4.3.1.1. Osservazioni generali

148. L'EDPB ricorda che l'IPA 2016 è una norma recente che ha modificato diverse disposizioni della legge Intelligence Services Act 1994. Essa specifica in quale misura si possa ricorrere ad alcuni poteri investigativi per interferire nella sfera privata[89]. Nonostante due relazioni dell'IPC che forniscono informazioni utili concernenti l'applicazione di questo nuovo quadro giuridico, manca ancora un esame di alcuni aspetti, in particolare quelli che riguardano i selettori e i criteri di ricerca utilizzati.

149. Inoltre, come osservazione generale sull'IPA 2016 e sul suo ambito di applicazione, l'EDPB evidenzia i quattro punti indicati di seguito.

150. In relazione al **primo punto di attenzione**, relativamente alle caratteristiche della legge, l'EDPB desidera sottolineare due aspetti.

151. In primo luogo, l'EDPB osserva che la legislazione fa riferimento alle ampie finalità per il ricorso a procedure previste nell'IPA 2016 e non alle categorie di persone che possono essere interessate dalla raccolta di dati sulla base delle parti da 2 a 7 dell'IPA 2016. Al riguardo, l'EDPB ricorda che dovrebbe esistere un collegamento tra le categorie di persone che possono essere oggetto di misure di sorveglianza e le finalità perseguite dalla legislazione al fine di definire il campo di applicazione soggettivo della legge.

152. Inoltre, l'EDPB sottolinea che le definizioni di "operatori di telecomunicazioni", "servizio di telecomunicazioni" e "sistema di telecomunicazioni", che definiscono l'ambito di applicazione della legge, sono anch'esse molto ampie e non del tutto chiare. Infatti, l'EDPB sottolinea che questi concetti, nel campo dell'IPA 2016, devono essere intesi in modo molto più ampio rispetto alle legislazioni sulle telecomunicazioni, come definite ad esempio nel codice europeo delle comunicazioni elettroniche[90]. L'EDPB osserva che le definizioni di "servizi di telecomunicazioni" e "sistema di telecomunicazioni" nella legge sono indicate come intenzionalmente ampie in modo da rimanere rilevanti anche alla luce di nuove tecnologie. Analogamente, la definizione di un operatore di telecomunicazioni è anch'essa molto ampia, e potrebbe comprendere ad esempio videogiochi online con inclusa una funzione di chat, oppure altri siti web online che presentano semplicemente analoghe finestre di chat[91].

153. Inoltre, mentre in genere sono previste le procedure e la vigilanza concernenti la valutazione della necessità e della proporzionalità della raccolta e dell'accesso ai dati, i criteri per procedere alla

[89] Cfr. art. 1 della IPA 2016.

[90] Cfr. articolo 2, paragrafo 5 del codice europeo delle comunicazioni elettroniche, che definisce. ad esempio, un "servizio di comunicazione interpersonale" come *"un servizio di norma a pagamento che consente lo scambio diretto interpersonale e interattivo di informazioni tramite reti di comunicazione elettronica tra un numero limitato di persone, mediante il quale le persone che avviano la comunicazione o che vi partecipano ne stabiliscono il destinatario o i destinatari e non comprende i servizi che consentono le comunicazioni interpersonali e interattive esclusivamente come elemento accessorio meno importante e intrinsecamente collegato a un altro servizio*".

[91] Cfr. Home Office, Code of practice on the interception of communications, marzo 2018, paragrafi 2.5 e seguenti, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

valutazione non sono invece definiti nella legge stessa. Ulteriori elementi possono essere individuati in altri documenti, come, ad esempio, i codici di buone prassi.

154. Tuttavia, come ricordato nelle Raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza, la Corte ha indicato che "*il requisito secondo cui qualsiasi limitazione nell'esercizio dei diritti fondamentali deve essere prevista dalla legge implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato*"[92]. Più specificamente, la Corte ha chiarito che "*[p]er soddisfare al requisito di proporzionalità, una normativa deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente tali dati contro il rischio di abusi. Tale normativa dev'essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale e, in particolare, indicare in quali circostanze e a quali condizioni una misura che preveda il trattamento di tali dati possa essere adottata, garantendo così che l'ingerenza sia limitata allo stretto necessario*"[93].

155. La Corte EDU ha sottolineato anche l'importanza della chiarezza della legge per dare ai cittadini "*un'indicazione adeguata delle circostanze in cui e delle condizioni alle quali le autorità pubbliche sono autorizzate a ricorrere a misure di questo genere*"[94].

156. **L'EDPB invita quindi la Commissione a valutare ulteriormente questi aspetti concernenti la precisione, la chiarezza e l'esaustività della legge pertinente, fornendo ulteriori elementi che dimostrino che essa garantisce un livello di protezione essenzialmente equivalente a quello garantito nell'UE con riguardo alle caratteristiche della legge. L'EDPB sottolinea anche che le ampie definizioni in essa previste dovrebbero essere valutate in relazione alla proporzionalità delle misure di intercettazione.**

157. Inoltre, benché diversi codici interni delle autorità di intelligence competenti sviluppino in parte alcuni di questi elementi, ad esempio per quanto concerne la valutazione della necessità e della proporzionalità della raccolta dei dati, l'EDPB sottolinea che i requisiti della Corte relativi alla natura della legge implicano che gli elementi fondamentali, anche affinché gli interessati possano fare affidamento su di essi nel contesto di un ricorso, devono essere stabiliti nella legislazione che prevede diritti azionabili[95]. Infatti, l'allegato 7, paragrafo 6 dell'IPA 2016 menziona il fatto che i tribunali (e le autorità di controllo) "*tengono conto della mancata considerazione da parte di una persona di un codice nel decidere una questione in questo tipo di procedimenti*" senza chiarire se le persone possano far valere una violazione dei codici davanti ai tribunali (o le autorità di controllo). Inoltre, gli elementi forniti finora nel progetto di decisione riguardano il riconoscimento da parte della Corte EDU della prevedibilità delle regole previste[96] in questi codici, invece della loro

[92] Cfr. *Schrems II*, paragrafo 175; e la giurisprudenza citata, nonché Corte di giustizia dell'Unione europea, causa C-623/17, *Privacy International contro Secretary of State for Foreign and Commonwealth Affairs e a.*, 6 ottobre 2020, ECLI:EU:C:2020:790 (di seguito "Privacy International"), paragrafo 65.
[93] Cfr. *Privacy International*, paragrafo 68.
[94] Cfr. Corte EDU, *Zakharov contro Russia*, 4 dicembre 2015, CE:ECHR:2015:1204JUD004714306, paragrafo 229.
[95] In proposito, la Corte di giustizia dell'Unione europea ha valutato ad esempio che negli Stati Uniti la PPD 28 non rispondesse ai requisiti, benché prevedesse alcune limitazioni relative alla raccolta in massa, cfr. *Schrems II*, paragrafo 181.
[96] Cfr. Corte EDU, *Big Brother Watch e a. contro Regno Unito*, 13 settembre 2018, ECLI:CE:CEDU:2018:0913JUD005817013 (di seguito "Big Brother Watch"), paragrafo 325: "*Poiché il codice IC è un documento pubblico, sottoposto all'approvazione di entrambe le camere del Parlamento, e deve essere*

"azionabilità" in sede giudiziaria, come richiesto dalla Corte, oppure il fatto che in alcuni casi i tribunali del Regno Unito hanno fatto riferimento a codici, mentre nessuno dei casi menzionati segnala la possibilità per i cittadini di azionare diritti derivanti dai codici stessi. **Qualora si concludesse che il diritto del Regno Unito non indica a sufficienza le circostanze e le condizioni nelle quali può essere adottata una misura e che questi elementi sono di fatto previsti da codici interni delle autorità della comunità di intelligence**, **l'EDPB inviterebbe la Commissione europea a valutare ulteriormente se le limitazioni e le garanzie previste nei differenti codici interni delle autorità della comunità di intelligence possano essere azionati da cittadini davanti a un tribunale e fatte applicare.**

158. **Il secondo punto di attenzione** riguarda il fatto che le disposizioni contenute nell'IPA 2016 o in altre norme, come ad esempio la legge Intelligence Services Act 1994 o la legge Regulation of Investigatory Powers Act 2000, relative, da una parte, all'acquisizione mirata e alla conservazione di dati delle comunicazioni e, dall'altra, alla raccolta in massa, si applicheranno anche ai dati trasferiti dall'UE al Regno Unito. Per quanto concerne la raccolta in massa, l'EDPB sottolinea che le rilevanti disposizioni del diritto del Regno Unito consentono la raccolta di dati al di fuori del Regno Unito; e potrebbero quindi comprendere dati in transito trasferiti dal SEE verso il Regno Unito sulla base della decisione di adeguatezza[97]. Inoltre, l'EDPB rileva che la Commissione europea indica che "*[o]ccorre osservare che normalmente la conservazione e l'acquisizione di dati delle comunicazioni non riguardano dati personali degli interessati dell'UE trasferiti verso il Regno Unito nell'ambito della presente decisione. L'obbligo di conservare o divulgare dei dati delle comunicazioni a norma della parte 3 e 4 dell'IPA 2016 riguarda i dati raccolti dagli operatori di telecomunicazioni nel Regno Unito direttamente dagli utilizzatori di un servizio di telecomunicazioni*"[98]. Ciononostante, l'EDPB sottolinea la mancanza di chiarezza in merito al fatto che solo gli stabilimenti di questi operatori situati nel Regno Unito possono ricevere richieste dalle autorità competenti del Regno Unito, poiché la definizione di operatore di telecomunicazioni prevista nella sezione 261(10) dell'IPA 2016 stabilisce che "per operatore di telecomunicazioni si intende un soggetto che offre o fornisce servizi di telecomunicazioni a soggetti nel Regno Unito *o che controlla o fornisce un sistema di telecomunicazioni che è (totalmente o parzialmente) situato nel Regno Unito o controllato da questo paese*". Potrebbero essere quindi effettivamente coinvolti i dati personali di interessati del SEE, ad esempio, nel caso di dati raccolti o generati da uno stabilimento di un operatore di telecomunicazioni nel Regno Unito situato nel SEE che siano trasferiti a uno stabilimento del medesimo operatore situato nel Regno Unito sulla base della decisione di adeguatezza (per finalità commerciali), e quindi raccolti, all'interno del Regno Unito, dalle autorità pubbliche competenti.

159. **L'EDPB ritiene quindi che valutare queste disposizioni sia rilevante anche ai fini della valutazione del livello di adeguatezza del quadro giuridico del Regno Unito in materia di protezione dei dati e invita la Commissione europea a chiarire questo aspetto e a determinare in che misura ciò corrisponda al vero. In particolare, l'EDPB esorta la Commissione europea a chiarire la propria interpretazione dell'ambito di applicazione di questa legislazione, indicando anche quale sia l'estensione del concetto di "utilizzatori di servizi di telecomunicazioni" e se possano essere richiesti dati agli stabilimenti di operatori di telecomunicazioni al di fuori del Regno Unito, nella**

preso in considerazione sia da coloro che svolgono compiti di intercettazione sia dalle corti e dai tribunali, il tribunale ha espressamente accettato che le sue disposizioni possano essere prese in considerazione nel valutare la prevedibilità del regime RIPA".

[97] Cfr. paragrafo 183 e seguenti di *Schrems II* sulla valutazione di una legislazione che prevede l'accesso ai dati in transito tra l'UE e un paese terzo nel contesto di una decisione di adeguatezza.

[98] Cfr. considerando 196 del progetto di decisione.

misura in cui siano coinvolti dati di interessati del SEE, vista l'ampissima definizione di "operatori di telecomunicazioni".

160. **Il terzo punto di attenzione** riguarda la procedura "double lock". L'EDPB rileva che nell'IPA 2016 è stata introdotta una nuova procedura "double lock". Ciononostante, a quanto risulta all'EDPB, anche se, in linea di principio, la raccolta dei dati o il loro accesso per finalità di sicurezza nazionale o intelligence può avvenire unicamente con un mandato approvato da un commissario giudiziario, l'IPA 2016 prevede che "*in specifici casi limitati sia possibile un'intercettazione legittima senza mandato e che sia richiesta unicamente la preventiva autorizzazione delle competenti autorità IC [cfr. infra sezione sulla vigilanza], anche per le intercettazioni secondo richieste estere (articolo 52 dell'IPA 2016)*". Come sottolineato più avanti, anche questo contribuisce ai timori dell'EDPB per quanto concerne in particolare la comunicazione all'estero. Inoltre, l'EDPB osserva che per l'interferenza nelle apparecchiature, mirata o di massa, è possibile anche una deroga alla procedura "double lock", e che il commissario giudiziario è unicamente autorizzato ad approvare il rinnovo per i mandati di massa dopo un periodo iniziale massimo di 6 mesi. **L'EDPB invita la Commissione a un'analisi più approfondita e a dimostrare che anche nei casi in cui non si applica la procedura "double lock", il quadro giuridico del Regno Unito fornisce opportune garanzie, tra cui l'efficace vigilanza *ex post* e possibilità di ricorso offerte alle persone fisiche, per assicurare che il livello di protezione fornito sia sostanzialmente equivalente a quello previsto nell'UE (cfr. anche infra sezione 4.3.3 sulla vigilanza).**

161. Inoltre, nonostante l'effettiva introduzione della procedura "double lock" con l'IPA 2016, l'EDPB conferma i propri timori circa alcune caratteristiche della nuova legislazione. A seguito della presentazione delle corrispondenti sezioni del progetto di decisione, l'EDPB ha analizzato le seguenti tipologie di raccolta e di accesso ai dati nel medesimo ordine presentato dalla Commissione europea. L'ordine degli elementi valutati non rispecchia quindi una gerarchia in termini di livello di preoccupazione per l'EDPB.

4.3.1.2. Acquisizione mirata e conservazione di dati delle comunicazioni

162. L'EDPB osserva che esistono due funzionari in grado di concedere autorizzazioni mirate per ottenere dati delle comunicazioni: il funzionario autorizzante dell'Office for Communications Data Authorisations (di seguito "IPC") e un funzionario di alto rango incaricato (una persona che svolge una funzione o ricopre una carica prescritta in un'autorità pubblica competente), in aggiunta all'approvazione da parte di un commissario giudiziario in alcuni casi. Per l'EDPB rimane però da chiarire, a norma della legge e del relativo codice, quale funzionario autorizza esattamente quale tipo di acquisizione mirata di dati delle comunicazioni, e in quale misura un funzionario incaricato sarebbe sufficientemente indipendente[99].

163. **L'EDPB invita quindi la Commissione europea a valutare ulteriormente questo aspetto e a fornire chiarimenti su questi elementi.**

164. Per quanto concerne la notifica che richiede la conservazione dei dati delle comunicazioni, l'EDPB osserva anche che queste notifiche possono essere inviate a "una categoria di operatori". Questa nozione sembra indicare la possibilità di richiedere a più operatori di conservare tutti i dati allo stesso tempo. Infatti, la natura mirata dell'acquisizione non riguarda il numero di operatori, ma il nome o la descrizione delle persone, delle organizzazioni, delle sedi o dei gruppi di persone che costituiscono il "target", una descrizione della natura dell'indagine e una descrizione delle attività per cui sono

[99] Cfr. anche in infra per quanto concerne la valutazione della procedura "double lock" e l'indipendenza del commissario giudiziario.

utilizzate le apparecchiature. L'EDPB evidenzia quindi che, a seconda del numero di operatori interessati da questa "categoria di operatori", la notifica può essere più ampia rispetto a quanto la procedura di conservazione mirata sembri eventualmente implicare. **L'EDPB invita la Commissione europea a valutare ulteriormente questo aspetto, e a fornire ulteriori rassicurazioni che, anche nel caso in cui le notifiche siano inviate a più operatori, rimangano limitate a quanto strettamente necessario e proporzionato.**

4.3.1.3. Interferenza nelle apparecchiature

165. L'EDPB osserva che l'"interferenza nelle apparecchiature" può derogare alla procedura "double lock" in caso di urgenza[100]. L'EDPB teme quindi che le finalità per le quali questa interferenza nelle apparecchiature possa essere richiesta siano estese, mentre rimangono da chiarire i criteri di urgenza (condizione nella quale il commissario giudiziario non è tenuto a fornire un'autorizzazione *ex ante* a seguito di una valutazione della necessità e della proporzionalità dell'interferenza nelle apparecchiature). Poiché in quest'ultima situazione "il mandato cessa di produrre effetti e non può essere rinnovato" nel caso in cui il commissario giudiziario non approvi l'interferenza nelle apparecchiature *ex post*, all'EDPB risulta che i dati raccolti nel frattempo rimangano comunque lecitamente raccolti. Affinché questi dati siano cancellati, può essere emanato uno specifico ordine del commissario giudiziario[101].

166. **L'EDPB invita la Commissione europea a valutare ulteriormente le condizioni alle quali è possibile invocare l'urgenza e a fornire chiarimenti in merito alle possibili vie di esercizio dei diritti per gli interessati e ai possibili mezzi di ricorso loro offerti nel contesto delle operazioni di interferenza nelle apparecchiature, in particolare quando si svolgono in un contesto di urgenza che porta a una deroga alla procedura "double lock".**

4.3.1.4. Intercettazione di massa di dati dai canali

167. Come descritto nella relazione di revisione dei poteri di massa[102] *"[l']intercettazione di massa prevede solitamente la raccolta di comunicazioni nel momento in cui transitano da specifici canali (collegamenti di comunicazione)*". La scheda informativa ufficiale dell'IPA 2016 descrive l'"intercettazione di massa" come "*il processo di raccolta di un volume di comunicazioni seguito dalla selezione di specifiche comunicazioni da leggere, ricercare o ascoltare ove necessario e proporzionato*". L'EDPB riscontra che l'"intercettazione di massa" di dati implica effettivamente la raccolta di dati anche prima dell'eventuale filtraggio da parte di selettori (semplice nel contesto del monitoraggio di persone fisiche già note per rappresentare una minaccia, o complesso, nel contesto dell'individuazione di nuove minacce e di persone di interesse non precedentemente note).

168. L'acquisizione di dati di comunicazione in massa è stata anche una delle tematiche esaminate dalla Corte nel caso Privacy International, che ha portato a una sentenza della Grande Sezione emanata il 6 ottobre 2020 (che ha valutato anche se questa raccolta di dati fosse stata eseguita nel contesto del diritto dell'UE, anche per finalità di sicurezza nazionale). L'IPA 2016 ha sostituito la normativa che era oggetto di questa sentenza.

169. L'EDPB osserva che, con l'introduzione nel diritto del Regno Unito dell'IPA 2016, ora è richiesto un mandato anche per l'intercettazione in massa di dati. Il processo di rilascio del mandato si basa sulla determinazione delle "finalità operative". L'elenco di queste finalità operative è stabilito dai vertici dei servizi di intelligence, e quindi approvato dal Segretario di Stato. Questa decisione è a sua volta

[100] Cfr. art. 109 della IPA 2016.
[101] Cfr. art. 110, paragrafo 3, lettera b) della IPA 2016.
[102] Cfr. Report of the bulk powers review, dell'Independent Reviewer of Terrorism Legislation, agosto 2016.

verificata da un commissario giudiziario indipendente, il quale deve valutare se il mandato è necessario e proporzionato per le finalità operative. A quanto risulta all'EDPB, il commissario giudiziario non ha il potere di valutare le finalità operative in sé, bensì se il mandato sia necessario e proporzionato per le finalità operative in esso elencate. Il Parliamentary Intelligence and Security Committee riceve una copia dell'elenco ogni tre mesi, e il primo ministro esamina almeno una volta l'anno l'elenco delle finalità operative.

170. Tuttavia, sulla base degli elementi forniti dalla Commissione europea nel progetto di decisione, sembra difficile valutare il perimetro di queste finalità operative previste nell'elenco e se la raccolta di dati che essi consentono soddisfi la soglia fissata dalla Corte (ad esempio la circoscrizione della raccolta dei dati a un'area geografica potrebbe limitarsi a poche strade, ma estendersi anche all'intero SEE).

171. Inoltre, l'EDPB sottolinea che i dati raccolti in massa possono essere conservati per periodi prolungati (affinché siano disponibili per l'accesso ai fini di ulteriore esame). Infatti, l'EDPB osserva che l'IPA 2016 all'art. 150, paragrafi 5 e 6 prevede solo la distruzione delle copie dei dati raccolti, e unicamente se la loro conservazione non è necessaria, oppure non è probabile che diventi necessaria, negli interessi della sicurezza nazionale o per qualunque altra motivazione che ricade nell'ambito dell'art. 138(2) IPA 2016, oppure se la conservazione non è necessaria per varie altre finalità[103]. L'EDPB sottolinea che queste motivazioni si presentano molto ampie, e che in ogni caso sono menzionate unicamente le copie dei dati ottenuti.

172. Inoltre, l'EDPB osserva che in casi urgenti l'IPA 2016 consente anche la modifica dei mandati senza preventiva approvazione di un commissario giudiziario, e che in questa eventualità, qualora il commissario giudiziario consultato *ex post* entro tre giorni lavorativi dalla modifica rifiuti di approvarla, il mandato dovrebbe produrre solo gli effetti precedenti la modifica, ma i dati raccolti nel frattempo si considerano comunque legittimamente raccolti[104]. Affinché questi dati siano cancellati, può essere emanato uno specifico ordine del commissario giudiziario[105].

173. **L'EDPB esorta quindi la Commissione europea a fornire ulteriori chiarimenti e a effettuare un'ulteriore valutazione delle intercettazioni di massa, con particolare riguardo alla selezione e all'applicazione dei selettori nel contesto di queste procedure di intercettazione di massa, al fine di precisare in che misura l'accesso ai dati personali soddisfi i criteri fissati dalla Corte (cfr. anche infra sezione 4.3.1.7., in particolare sulla vigilanza sui selettori), e quali garanzie esistono per tutelare i diritti fondamentali dei cittadini i cui dati sono intercettati in questo contesto, anche in merito ai periodi di conservazione dei dati. Sarebbe particolarmente utile una valutazione indipendente da parte delle autorità di vigilanza competenti del Regno Unito.**

174. **L'EDPB sottolinea inoltre che appare quanto mai critico che le "comunicazioni relative all'estero", che ricadono nell'ambito di applicazione delle pratiche di intercettazione di massa, sembrino implicare la possibilità per il Regno Unito di intercettare e raccogliere ingenti quantità di dati direttamente nel SEE, compresi i dati in transito tra il SEE e il Regno Unito, aspetto che ricadrebbe nell'ambito di applicazione del progetto di decisione (cfr. infra sezione 4.3.2. sull'ulteriore uso delle informazioni raccolte per finalità di sicurezza nazionale e comunicazione all'estero).**

[103] Cfr. paragrafi 3 e 6 dell'art. 150 della IPA 2016.
[104] Cfr. art. 147 della IPA 2016 (parte 6, capitolo I).
[105] Cfr. art. 181, paragrafo 3, lettera b) della IPA 2016.

4.3.1.5. Protezione e garanzie per i dati secondari

175. Inoltre, l'EDPB teme che la legislazione del Regno Unito relativa alle intercettazioni di massa non preveda il medesimo livello di protezione per tutti i dati di comunicazione. Per "dati secondari", che possono essere ottenuti con un mandato di massa, si intendono secondo l'art. 137 dell'IPA 2016 sia i "dati di sistema", "*compresi nella comunicazione, inclusi come parte di essa, allegati ad essa o logicamente associati ad essa (dal mittente o in altro modo)*", sia i "dati identificativi", "*compresi nella comunicazione, inclusi come parte di essa, allegati ad essa o logicamente associati ad essa (dal mittente o in altro modo), che possono essere logicamente separati dalla restante parte della comunicazione, e se così separati, non rivelerebbero alcunché che possa essere agevolmente considerato essere l'eventuale significato della comunicazione, ignorando qualunque significato derivante dall'esistenza della comunicazione o da qualunque dato relativo alla trasmissione della comunicazione*"[106].

176. L'EDPB osserva che questi "dati secondari", detti anche "metadati"[107], raccolti in massa, sembrano non beneficiare delle stesse garanzie previste per i dati raccolti con un mandato mirato, ma nemmeno di quelle previste per i dati di contenuto raccolti in massa. Infatti, l'EDPB riscontra che la selezione di qualunque contenuto intercettato beneficia di maggiori garanzie[108] rispetto alla selezione dei dati secondari[109].

177. Inoltre, l'EDPB sottolinea che sia la Corte EDU[110] sia la Corte[111] hanno messo in dubbio che questi dati siano meno sensibili rispetto ad altri, e in particolare rispetto ai dati di contenuto. Infatti, il codice di buone pratiche concernente le intercettazioni presenta esempi di "dati secondari" (sia "dati di sistema" come le configurazioni dei router, gli indirizzi e-mail o gli identificativi utente, ma anche identificativi alternativi di account, sia di "dati identificativi", come la localizzazione di un incontro in un appuntamento in calendario, informazioni ricavabili dalle fotografie, come ad esempio, l'orario, la data e la posizione in cui sono state scattate). **L'EDPB sottolinea quindi la valutazione uniforme espressa dalla Corte EDU e dalla Corte, e ribadisce i timori formulati in relazione ai dati secondari, che dovrebbero beneficiare di garanzie specifiche in virtù della loro sensibilità. L'EDPB invita la**

---

[106] I "dati di sistema" e "dati identificativi" sono definiti nell'art. 263 della IPA 2016.

[107] Cfr. Report of the bulk powers review, dell'Independent Reviewer of Terrorism Legislation, agosto 2016.

[108] Cfr. art. 152, paragrafo 1, lettera c) e paragrafi 3 e seguenti della IPA 2016.

[109] Cfr. art. 152, paragrafo 1, lettere a) e b) della IPA 2016.

[110] Cfr. Corte EDU, *Big Brother Watch*, paragrafo 357, deferita alla Grande Sezione: "*Quindi, benché la Corte non dubiti che i relativi dati delle comunicazioni siano uno strumento essenziale per i servizi di intelligence nella lotta al terrorismo e ai reati gravi, non ritiene che le autorità abbiano trovato un corretto equilibrio tra i contrastanti interessi pubblici e privati esonerandoli integralmente dalle garanzie previste per la ricerca e l'esame del contenuto. Anche se la Corte non suggerisce che i relativi dati delle comunicazioni debbano essere accessibili unicamente allo scopo di determinare se una persona fisica si trova o meno nelle Isole britanniche, perché a tale scopo sarebbe necessaria l'applicazione ai dati delle comunicazioni di norme più rigide rispetto a quanto previsto per il contenuto, dovrebbero tuttavia esistere garanzie sufficienti per assicurare che l'esenzione dei relativi dati delle comunicazioni dagli obblighi previsti dalla sezione 16 RIPA sia limitata alla misura necessaria per determinare se una persona fisica si trova in quel momento nelle Isole britanniche*".

[111] Cfr. Corte di giustizia dell'Unione europea, *Privacy International*, paragrafo 71: "*L'ingerenza nel diritto fondamentale sancito dall'articolo 7 della Carta che la trasmissione dei dati relativi al traffico e dei dati relativi all'ubicazione ai servizi di sicurezza e di intelligence comporta dev'essere considerata particolarmente grave, alla luce in particolare del carattere sensibile delle informazioni che possono fornire tali dati e, in particolare, della possibilità di stabilire, sulla base di questi ultimi, il profilo delle persone interessate, informazione, questa, tanto sensibile quanto il contenuto stesso delle comunicazioni. Inoltre, essa può ingenerare nelle persone interessate la sensazione che la loro vita privata costituisca l'oggetto di una sorveglianza continua (v., per analogia, sentenze dell'8 aprile 2014, Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti 27 e 37, nonché del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punti 99 e 100)*".

Commissione europea a valutare attentamente se le tutele previste dalla normativa del Regno Unito per questa categoria di dati personali garantiscano un livello di protezione essenzialmente equivalente a quello garantito nell'UE.

4.3.1.6. Trattamento automatizzato dei dati delle comunicazioni

178. L'EDPB osserva che le autorità della comunità di intelligence non solo utilizzano selettori semplici o complessi per filtrare i dati acquisiti in massa, ma possono anche avvalersi di altri strumenti automatizzati di elaborazione per analizzare "*grandi volumi di informazioni, che consentono alle agenzie anche di individuare connessioni, schemi, associazioni o comportamenti che possono dimostrare una grave minaccia che richiede un'indagine*" secondo la relazione del 2015 dell'Intelligence and Security Committee[112]. **L'EDPB è consapevole del fatto che questa relazione pubblica riguarda le pratiche seguite nell'ambito del precedente quadro giuridico, che è stato successivamente sostituito dall'IPA 2016. Ciononostante, ritiene necessaria un'ulteriore valutazione indipendente e un monitoraggio in merito al ricorso a strumenti di elaborazione automatizzati da parte delle competenti autorità di vigilanza del Regno Unito, e invita la Commissione europea a valutare ulteriormente questo aspetto e le garanzie che sarebbero e/o potrebbero essere offerte agli interessati del SEE in questo contesto**.

4.3.1.7. Rischi di non conformità e pratiche non conformi delle competenti autorità della comunità di intelligence

179. L'EDPB prende atto che sono disponibili relazioni dettagliate sulle attività di vigilanza che forniscono elementi preziosi in merito a quelle che si ritengono essere buone prassi ai fini della conformità, nonché ai rischi di non-conformità e alle pratiche non conformi individuate.

180. In proposito, secondo la relazione per il 2019 dell'IPC, diversi elementi che riguardano l'applicazione del quadro giuridico da parte di differenti autorità competenti hanno rivelato (rischi di) non conformità da parte di tali autorità competenti.

181. In primo luogo, l'EDPB ha rilevato che i criteri per classificare un set di dati come set di dati personali in massa o dati mirati non sembrano essere sempre chiari per gli stessi MI5 e SIS, in particolare per l'MI5, e questo può comportare la mancata applicazione di adeguate garanzie[113]. Nella sua relazione per il 2019, l'IPC suggerisce che "*la soluzione di questa problematica dovrebbe essere una priorità*"[114]. Anche in relazione ai set di dati personali in massa, l'EDPB osserva che per la GCHQ, anche se la

---

[112] Cfr. Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework, 2015, paragrafo 18, pag. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

[113] Cfr. Annual Report of the Investigatory Powers Commissioner 2019, 15 dicembre 2020, punto 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: "*Abbiamo osservato lo sviluppo positivo del [Bulk Oversight Panel (BOP)] e prendiamo nota del suo impatto sulla gestione della conformità interna. Continuiamo a cercare maggiore chiarezza in merito al processo seguito dall'MI5 per eseguire l'esame iniziale dei nuovi set di dati al fine di comprendere meglio le decisioni di classificazione dei set di dati come set di dati personali in massa o, ad esempio, dati mirati. Eravamo preoccupati per un'azione non risolta nei verbali del BOP relativa alla soluzione di discrepanze tra le assegnazioni di set di dati personali in massa tra MI5 e SIS. A causa dei differenti utilizzi dei dati e dei differenti tagli dei dati conservati, è possibile che entrambe le agenzie possano conservare il medesimo set di dati, oppure versioni dello stesso, e che essi possano essere legittimamente classificati come di massa da un'agenzia e come dati mirati da parte dell'altra agenzia. Sussiste il rischio che, qualora una delle agenzie non abbia correttamente classificato i dati conservati come dati mirati, che questi dati siano conservati senza opportuno mandato e possano non essere oggetto di garanzie adeguate*".

[114] Cfr. Annual Report of the Investigatory Powers Commissioner 2019, punto 8.39.

classificazione di set di dati personali in massa sembra essere soddisfacente (ma deve essere ancora verificata dall'IPC), nel marzo 2019 l'esame della conformità interna dei mandati da parte del team dedicato ha sollevato gravi preoccupazioni, evidenziando come il 50 % delle giustificazioni per mandati di acquisizione di massa esaminate dal team di conformità della GCHQ non rispettassero lo standard richiesto. Secondo l'IPC, il team di conformità aveva iniziato a lavorare per indagare il problema e riaddestrare il personale per migliorare questo standard. La formazione di aggiornamento sulle disposizioni dell'IPA 2016 e l'ulteriore formazione fornita dalle reti per le politiche e la conformità (di seguito "PCN") hanno migliorato la conformità della GCHQ in quest'area. L'IPC non prevede di registrare un peggioramento in questo standard nelle future ispezioni, ma continuerà a tenere sotto attenta osservazione quest'area[115]. **L'EDPB concorda quindi sull'esigenza di un'ulteriore analisi e di un monitoraggio di questi elementi da parte della Commissione europea nell'ambito della valutazione del livello di protezione, per assicurare che questo standard sia migliorato, come sottolineato nella relazione dell'IPC, e ricorda che nella valutazione della sostanziale equivalenza di un paese terzo occorre tenere in considerazione anche l'attuazione e la concreta applicazione del quadro giuridico come previsto dall'articolo 45 del GDPR.**

182. Più in generale, l'EDPB sottolinea i punti di attenzione condivisi dall'IPC concernenti le "ricerche a seguito di incarichi assegnati" condotte dai funzionari dell'MI5, che consentono a un investigatore di condurre più ricerche sui set di dati personali in massa a sua disposizione, e i "*seri rischi di conformità associati ad alcuni ambienti tecnologici utilizzati dall'MI5*", concernenti il luogo in cui i dati sono conservati nell'ambiente, le persone che hanno accesso ai dati, in quale misura i dati siano stati copiati o condivisi, i processi di cancellazione applicati, oltre a dubbi sui periodi di conservazione. Anche se l'IPC indica che sono state adottate misure e introdotte garanzie, alcune delle quali rimangono manuali e vengono eseguite individualmente e di persona, sottolinea come essenziale il fatto che "*l'MI5 continui a mantenere questi nuovi processi e a mettere a disposizione risorse sufficienti affinché funzionino efficacemente. Qualora l'MI5 individui un aumento dei comportamenti non conformi*"[116]. L'IPC si aspetta che essi siano portati alla sua attenzione nel più breve tempo possibile. **L'EDPB invita quindi la Commissione europea a tenere sotto attenta osservazione questi aspetti in futuro**.

183. Per quanto concerne la GCHQ, dalla relazione dell'IPC l'EDPB comprende anche che, per le operazioni condotte nell'ambito di mandati di massa, "*la qualità delle richieste di approvazione interna era variabile e abbiamo osservato che vi era margine di miglioramento nella modalità di presentazione delle richieste*"[117] e che per quanto concerne l'interferenza mirata nelle apparecchiature, le spiegazioni sull'uso di descrittori generali erano talvolta troppo generiche e imprecise[118]. L'EDPB osserva anche che nel contesto dell'interferenza di massa nelle apparecchiature, l'IPC raccomanda che "*le richieste dovrebbero registrare coerentemente ed esplicitamente il legame tra il destinatario e una finalità legale e requisiti di intelligence*"[119], che "*nella valutazione della proporzionalità tutte le richieste dovrebbero esaminare la possibilità di intrusione collaterale e le relative misure di mitigazione*"[120], e che l'IPC ha sottolineato come, nonostante i progressi, "*vi è ancora margine di miglioramento*"[121] e che anche in futuro servirà ulteriore attenzione.

[115] Cfr. Annual Report of the Investigatory Powers Commissioner 2019, punto 10.48.
[116] Cfr. Annual Report of the Investigatory Powers Commissioner 2019, punto 8.52.
[117] Cfr. Annual Report of the Investigatory Powers Commissioner 2019, punto 10.2.
[118] Cfr. Annual Report of the Investigatory Powers Commissioner 2019, punti 10.16 e 10.17.
[119] Cfr. Annual Report of the Investigatory Powers Commissioner 2019, punto 10.23.
[120] Cfr. Annual Report of the Investigatory Powers Commissioner 2019, punto 10.23.
[121] Cfr. Annual Report of the Investigatory Powers Commissioner 2019, punto 10.23.

184. In relazione al regime di intercettazione di massa previsto dalla legge Regulation of Investigatory Powers Act 2000 (di seguito "legge RIPA 2000"), che è stata successivamente sostituita dalle disposizioni dell'IPA 2016, l'EDPB ricorda che l'insufficiente vigilanza, sia sulla selezione dei canali Internet per l'intercettazione sia sul filtraggio, la ricerca e la selezione delle comunicazioni intercettate ai fini dell'esame, rappresenta uno dei principali aspetti che la Corte EDU ha ritenuto non conformi con l'articolo 8 della CEDU per quanto concerne la precedente legislazione sui poteri investigativi delle autorità del Regno Unito nel contesto della sicurezza nazionale nella causa *Big Brother Watch*, oggi deferita alla Grande Sezione. **L'EDPB esorta la Commissione europea a verificare lo stato del procedimento, a tenere in considerazione questi elementi, e a specificarli nella decisione di adeguatezza qualora la Commissione europea dovesse modificarla.**

185. In questa eventualità, la Corte EDU: "*non era persuasa che le garanzie che regolano la selezione dei canali per l'intercettazione e la selezione dei materiali intercettati ai fini dell'esame fossero sufficientemente robuste per fornire adeguate garanzie contro gli abusi. Desta la maggiore preoccupazione, tuttavia, l'assenza di una robusta vigilanza indipendente dei selettori e dei criteri di ricerca utilizzati per filtrare le comunicazioni intercettate*"[122]. Come evidenziato dall'IPC, "*questo riscontro ricorda una raccomandazione analoga contenuta nella relazione del Intelligence and Security Committee "Privacy and Security: A modern and transparent legal framework" del marzo 2015*"[123]. **L'EDPB accoglie con favore il fatto che di conseguenza l'IPC abbia condotto un esame del suo approccio all'ispezione delle intercettazioni di massa nel 2019 "*che ha previsto un attento esame dei modi tecnicamente complessi in cui si realizzano effettivamente le intercettazioni di massa*"[124] e che si sia impegnato a prevedere "*un esame approfondito dei selettori e dei criteri di ricerca a cui accennava sopra la Corte EDU*"[125] nelle ispezioni delle intercettazioni di massa a partire dal 2020. Alla luce dell'importanza di questo aspetto, l'EDPB esprime la propria preoccupazione per il fatto che l'IPC non abbia ancora condotto un esame dettagliato dei selettori e dei criteri di ricerca, e invita la Commissione europea a seguire attentamente gli sviluppi al riguardo, soprattutto poiché rimane da chiarire la forma concreta che assumerà questa vigilanza[126].**

4.3.2. Ulteriore uso delle informazioni raccolte per finalità di sicurezza nazionale e comunicazione all'estero

186. In tema di ulteriore uso delle informazioni raccolte per finalità di sicurezza nazionale, nella sua valutazione la Commissione europea fa riferimento all'art. 87(1) della DPA 2018, il quale prevede infatti che "*i dati personali così raccolti non devono essere elaborati in modo non compatibile con la finalità per la quale sono stati raccolti*". L'EDPB sottolinea tuttavia che questa disposizione può essere soggetta a esenzioni ai fini di sicurezza nazionale, come previsto dall'art. 110 della DPA 2018. L'EDPB sottolinea inoltre che per l'intercettazione mirata e l'esame, l'acquisizione mirata e la conservazione di dati di comunicazione, l'interferenza nelle apparecchiature mirata o l'intercettazione di massa e l'interferenza nelle apparecchiature di massa, la legislazione prevede la possibilità di "comunicazione all'estero".

[122] Cfr. Corte EDU, *Big Brother Watch*, paragrafo 347.
[123] Cfr. Annual Report of the Investigatory Powers Commissioner 2019, punto 10.28.
[124] Cfr. Annual Report of the Investigatory Powers Commissioner 2019, punto 10.28.
[125] Cfr. Annual Report of the Investigatory Powers Commissioner 2019, punto 10.28.
[126] Cfr. Annual Report of the Investigatory Powers Commissioner 2019, punto 10.28: "l'esatto formato di questa ispezione deve essere ancora concordato".

4.3.2.1. Ulteriore uso, comunicazione all'estero e quadro giuridico applicabile nel Regno Unito

187. La Commissione europea ha identificato nella parte 4 della DPA 2018, e in particolare nel suo art. 109, le disposizioni rilevanti che definiscono gli specifici requisiti per l'ulteriore utilizzo delle informazioni raccolte, e in particolare il trasferimento internazionale di dati personali da parte di servizi di intelligence verso paesi terzi od organizzazioni internazionali. Tuttavia, l'EDPB riscontra che l'art. 110 della DPA 2018 prevede un'esenzione ai fini di sicurezza nazionale, e che esso specifica che talune disposizioni della DPA 2018 non trovano applicazione se una deroga rispetto a tali disposizioni è necessaria per salvaguardare la sicurezza nazionale. Tra le disposizioni in questione che potrebbero non trovare applicazione vi sono il capitolo 2 della parte 4 della DPA 2018 relativo ai principi di protezione dei dati, compresa la limitazione di finalità, e il capitolo 3 della parte 4 della DPA 2018 relativo ai diritti degli interessati. L'articolo 109 della DPA 2018, in combinato disposto con l'art. 110 della DPA 2018, e le relative condizioni di applicazione, possono comportare un trasferimento internazionale di dati personali da parte di servizi di intelligence verso paesi terzi senza applicare le disposizioni relative ai principi di protezione dei dati e ai diritti degli interessati.

188. Come individuato dalla Commissione europea, questa esenzione deve essere valutata caso per caso, e può essere invocata unicamente se l'applicazione di una specifica disposizione avrebbe conseguenze negative per la sicurezza nazionale. Infatti, il rilascio di un certificato nazionale per i servizi di intelligence del Regno Unito intende attestare che è necessaria un'esenzione riguardo a specifici dati personali trattati allo scopo di tutelare la sicurezza nazionale. L'EDPB osserva tuttavia che nei suoi orientamenti relativi al certificato di sicurezza nazionale a norma della DPA 2018, l'Home Office del Regno Unito chiarisce che "*è importante osservare sin dall'inizio che non è necessario un certificato per avvalersi dell'esenzione ai fini di sicurezza nazionale; infatti, nella maggior parte dei casi, i titolari del trattamento decideranno autonomamente se si applichi l'esenzione ai fini di sicurezza nazionale*"[127]. Inoltre, gli orientamenti dell'Home Office del Regno Unito indicano che "*i certificati di sicurezza nazionale possono applicarsi a dati personali che possono essere specificamente identificati oppure coprire una più ampia categoria di dati personali. Possono essere sia ex ante sia ex post*"[128]. L'esenzione ai fini di sicurezza nazionale può quindi applicarsi a un trasferimento internazionale di dati personali da parte dei servizi di intelligence verso paesi terzi in assenza di un certificato di sicurezza nazionale.

189. L'EDPB osserva inoltre che, ad esempio, il certificato di sicurezza nazionale DPA/S27/Security Service[129] prevede che fino al 24 luglio 2024 i dati personali trattati "*per, per conto di, su richiesta di o con l'aiuto o l'assistenza del Security Service o*" e "*se il trattamento è necessario per agevolare il corretto espletamento delle funzioni del Security Service descritte nella sezione 1 della legge Security Service Act 1989*" sono esenti dalle disposizioni nel diritto del Regno Unito corrispondenti al capo V del GDPR in relazione ai trasferimenti di dati personali verso paesi terzi od organizzazioni internazionali. Benché gli altri certificati di sicurezza nazionale pubblicamente disponibili non prevedano un'esenzione dalle disposizioni dell'art. 109 della DPA 2018, occorre ricordare che una parte o la totalità del testo di un certificato di sicurezza nazionale può essere omessa se la sua pubblicazione sarebbe contraria agli interessi di sicurezza nazionale, sarebbe contraria all'interesse pubblico, o potrebbe compromettere la sicurezza di una persona.

[127] Cfr. Home Office, The Data Protection Act 2018, National Security Certificates guidance, agosto 2020, paragrafo 3, pag. 3.
[128] Cfr. Home Office, The Data Protection Act 2018, National Security Certificates guidance, agosto 2020, paragrafo 5, pag. 4.
[129] Cfr. DPA/S27/Security Service, art. 27 della DPA 2018, Certificate of the Secretary of State, 24 luglio 2019, https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

190. In generale, nel valutare il progetto di decisione in relazione a queste disposizioni, l'EDPB osserva che le garanzie per queste divulgazioni prevedono unicamente l'obbligo per il destinatario dei dati di rispettare i requisiti riguardanti la sicurezza dei dati, la limitazione della comunicazione all'effettiva necessità, la conservazione dei dati e le restrizioni di accesso ai dati a un numero limitato di persone. Per questo motivo, **l'EDPB sottolinea che, per quanto concerne le comunicazioni verso l'estero, l'applicazione dell'esenzione ai fini di sicurezza nazionale prevista nel diritto del Regno Unito potrebbe determinare situazioni in cui nel paese terzo di destinazione non siano totalmente previste o rispettate le garanzie che assicurano il rispetto dei principi di limitazione delle finalità, necessità e proporzionalità, o i diritti dei cittadini, gli strumenti di vigilanza e di ricorso. L'EDPB raccomanda quindi alla Commissione europea di esaminare ulteriormente le garanzie complessive fornite dalla normativa del Regno Unito per quanto concerne le comunicazioni verso l'estero, in particolare alla luce dell'applicazione delle esenzioni ai fini di sicurezza nazionale.**

4.3.2.2. Comunicazioni all'estero e condivisione di intelligence nel contesto della cooperazione internazionale

191. L'EDPB rileva anche che la Commissione europea non ha considerato, nell'ambito della sua valutazione di adeguatezza, gli accordi internazionali esistenti conclusi tra il Regno Unito e paesi terzi od organizzazioni internazionali che possono prevedere disposizioni specifiche per il trasferimento internazionale di dati personali da parte di servizi di intelligence verso paesi terzi.

192. L'EDPB sottolinea che la valutazione della Commissione europea si basa prevalentemente sull'esame della parte 4 della DPA 2018, ed esprime in particolare preoccupazione per il fatto che l'IPA 2016 si concentri sulle "richieste" di scambio di intelligence con partner stranieri, ma non tratti altre forme di condivisione di intelligence. L'EDPB osserva in proposito che il progetto di decisione della Commissione europea non fa riferimento a e non valuta l'articolazione tra il quadro giuridico del Regno Unito e l'accordo "UK-US Communication Intelligence Agreement" ("Accordo UK-US CI"). In una recente dichiarazione in occasione del 75° anniversario di questo accordo, la National Security Agency statunitense ("NSA") ha affermato che questo partenariato consente "*di condividere informazioni tra le due agenzie nella misura massima possibile, con restrizioni minime*" e che "*questo innovativo documento ha creato le politiche e le procedure per la condivisione di comunicazioni, traduzioni, analisi e informazioni per la decodifica tra i professionisti dell'intelligence del Regno Unito e degli Stati Uniti*"[130]. L'accordo è diventato anche il fondamento per altre collaborazioni di intelligence con Australia, Canada e Nuova Zelanda.

193. La natura segreta di questo accordo e delle sue disposizioni specifiche rappresentano una grave criticità in termini di chiarezza e prevedibilità della legge per quanto concerne l'ulteriore utilizzo e la comunicazione all'estero di informazioni raccolte dalle autorità del Regno Unito per finalità di sicurezza nazionale. Al riguardo, l'EDPB ricorda che per quanto concerne il livello di protezione garantito nell'UE, la Corte ha sottolineato che la legislazione che prevede un'interferenza con il diritto fondamentale alla protezione dei dati personali deve "*prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente tali dati contro il rischio di abusi. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatico ed esiste un*

[130] Cfr. comunicato stampa della NSA, GCHQ and NSA Celebrate 75 Years of Partnership, 5 febbraio 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.

rischio considerevole di accesso illecito ai dati stessi"[131]. L'EDPB ritiene quindi che la Commissione europea debba considerare l'impatto dell'Accordo UK-US CI nell'ambito della sua valutazione di adeguatezza.

194. La Corte EDU, nella sua sentenza sulla prima sezione del 13 settembre 2018, nella causa *Big Brother Watch*, ha valutato il regime di condivisione di intelligence del Regno Unito e in particolare l'Accordo UK-US CI. La Corte EDU ha affermato che "*[i]l quadro legale che consente ai servizi di intelligence del Regno Unito di richiedere materiali intercettati da agenzie di intelligence estere non è contenuto nella legge RIPA. L'Accordo UK-US Communication Intelligence del 5 marzo 1946 autorizza specificamente lo scambio di materiale tra gli Stati Uniti e il Regno Unito*"[132] e ha ritenuto che vi fosse "*un fondamento di legge per la richiesta di informazioni da agenzie di intelligence estere, e che questa legge fosse sufficientemente accessibile*"[133]. Anche se la Corte EDU ha concluso che non vi fosse una violazione dell'articolo 8[134] CEDU in relazione al regime di condivisione delle informazioni, l'EDPB osserva che questa sentenza è stata ora deferita alla Grande Sezione, di cui si attende la decisione. L'EDPB osserva anche che in un parere in parte concorde e in parte dissenziente verso questa sentenza, il giudice Koskelo, affiancato dal giudice Turković[135], ha concluso che vi sia una violazione dell'articolo 8 CEDU in relazione al regime di condivisione di informazioni, affermando che "*è facile concordare con il principio che qualunque accordo nell'ambito del quale sono ottenute informazioni su comunicazioni intercettate attraverso servizi di intelligence esteri, sulla base di richieste di esecuzione di tali intercettazioni oppure di trasferimento dei risultati, non dovrebbe consentire un'elusione delle garanzie che devono essere presenti per la vigilanza da parte delle autorità nazionali (cfr. paragrafi 216, 423 e 447). Infatti, qualunque altro approccio non sarebbe plausibile*".

195. Come sottolineato da numerose segnalazioni sui mezzi di comunicazione e da organizzazioni non governative[136,137], la versione più recente dell'Accordo UK-US CI sinora resa pubblica risale al 1956 e da allora le tecnologie delle comunicazioni e la natura dell'intelligence dei segnali hanno subito significativi cambiamenti. Notizie dei media hanno ad esempio rivelato che i dati in transito attraverso i cavi sottomarini che giungono nel Regno Unito sono intercettati dalla GCHQ e messi a disposizione della NSA[138].

196. Per l'EDPB, una questione fondamentale relativa alla condivisione di informazioni è se l'art. 109 della DPA 2018 e le disposizioni dell'IPA 2016 continuano ad applicarsi quando i servizi di intelligence del Regno Unito agiscono in conformità dell'Accordo UK-US CI. Un altro elemento fondamentale da valutare è se le disposizioni o l'effettiva applicazione di questo accordo influiscono sul livello di protezione dei dati personali in transito dal SEE verso il Regno Unito, o se consentono un accesso diretto e l'acquisizione di dati personali da parte di altri servizi di intelligence di paesi terzi.

---

[131] Cfr. *Schrems I*, paragrafo 91.
[132] Cfr. Corte EDU, *Big Brother Watch*, paragrafo 425.
[133] Cfr. Corte EDU, *Big Brother Watch*, paragrafo 427.
[134] Cfr. Corte EDU, *Big Brother Watch*, paragrafo 448.
[135] Cfr. Corte EDU, *Big Brother Watch*, parere in parte favorevole in parte dissenziente del giudice Koskelo, affiancato dal giudice Turković.
[136] Cfr. BBC, Diary reveals birth of secret UK-US spy pact that grew into Five Eyes, 5 marzo 2021, https://www.bbc.com/news/uk-56284453.
[137] Cfr. Privacy International, Policy Briefing - UK Intelligence Sharing Arrangements, aprile 2018, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.
[138] Cfr. The Guardian, GCHQ taps fibre-optic cables for secret access to world's communications, 21 giugno 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

197. Per questo motivo, oltre alle riserve espresse in merito alla "comunicazione all'estero" sulla base della parte 4 della DPA 2018 e della relativa esenzione ai fini di sicurezza nazionale, oltre che alle richieste nel quadro dell'IPA 2016, **l'EDPB nutre preoccupazioni per altre forme di condivisione di informazioni e di comunicazioni, sulla base di altri strumenti, in particolare i vari accordi internazionali conclusi dal Regno Unito con paesi terzi, specialmente quando tali strumenti non sono accessibili al pubblico, come ad esempio, l'Accordo UK-US CI. Gli effetti prodotti da questo accordo potrebbero determinare un'elusione delle garanzie individuate in relazione all'accesso e all'uso dei dati personali per finalità di sicurezza nazionale.**

198. Infatti, l'EDPB condivide il parere espresso dal relatore speciale alle Nazioni Unite, Joe Cannataci, secondo il quale "*[l]a condivisione di informazioni non deve rappresentare una scappatoia per ottenere o agevolare altri soggetti nell'ottenere informazioni senza le garanzie nazionali, né una falla che consente a governi esteri con standard inferiori di protezione della riservatezza (o di altri diritti umani) di ottenere informazioni dall'intelligence del Regno Unito che potrebbero dare origine a violazioni dei diritti umani*"[139].

199. Inoltre, **l'EDPB ritiene che la conclusione di accordi bilaterali o multilaterali con paesi terzi per finalità di cooperazione in materia di intelligence, i quali forniscono una base giuridica per l'intercettazione e l'acquisizione diretta di dati personali o il trasferimento di dati personali verso questi paesi, può incidere significativamente sulle condizioni per l'ulteriore utilizzo delle informazioni così raccolte, poiché questi accordi potrebbero influenzare il quadro giuridico del Regno Unito sulla protezione dei dati oggetto di esame.**

4.3.3. Vigilanza

200. L'EDPB sottolinea l'importanza, per un adeguato livello di protezione dei dati, di una supervisione completa da parte di autorità di controllo indipendenti. La garanzia di indipendenza delle autorità di controllo ai sensi dell'articolo 8, paragrafo 3 della Carta dell'UE è intesa ad assicurare il monitoraggio efficace e affidabile del rispetto delle regole sulla protezione delle persone fisiche relativamente al trattamento dei dati personali.

201. Quando si verifica un accesso ai dati personali e un loro utilizzo per finalità di sicurezza nazionale, la funzione di vigilanza è assolta prevalentemente dall'IPC e dai commissari giudiziari (di seguito "commissari giudiziari").

202. **In generale, l'EDPB riconosce come significativo miglioramento l'introduzione dei commissari giudiziari nell'IPA 2016.** In linea con quanto già segnalato, la Commissione europea è invitata a valutare più approfonditamente l'indipendenza dei **commissari giudiziari e in particolare in che misura l'indipendenza dell'IPC e dell'ufficio dell'IPC (di seguito "IPCO") sia garantita per legge, non risultando evidente dall'IPA 2016.** Questo aspetto è tanto più importante in virtù del fatto che l'IPC decide sui ricorsi presentati dal governo, nel caso in cui una richiesta di **misura** di sorveglianza **sia stata rigettata** da un commissario giudiziario.

203. L'IPC ha funzioni di vigilanza *ex ante* ed *ex post*. Per quanto riguarda la vigilanza *ex ante*, a quanto risulta all'EDPB la funzione dei commissari giudiziari è approvare, nei singoli casi, singole misure di sorveglianza, ivi compresa l'intercettazione mirata e l'acquisizione in massa di dati di comunicazione.

[139] Cfr. End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland, Londra, 29 giugno 2018, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

L'EDPB rileva inoltre che in base alla giurisprudenza della Corte non si può ritenere che la preventiva approvazione delle misure di sorveglianza costituisca un requisito assoluto per la proporzionalità delle misure di sorveglianza[140].

204. Per valutare l'efficacia di questo livello di vigilanza, l'EDPB ritiene comunque necessario chiarire ulteriormente gli scenari nei quali è possibile un'intercettazione legale senza una preventiva approvazione dei commissari giudiziari.

205. Nel suo progetto di decisione, nelle note a piè di pagina 201 e 266 la Commissione europea menziona "limitati casi specifici" previsti dall'IPA 2016 nei suoi articoli da 44 a 52 relativamente alle intercettazioni mirate. L'EDPB osserva che gli articoli da 45 a 51 dell'IPA 2016 prevedono esenzioni che, stando a quanto dichiarato, non verrebbero usate regolarmente dai servizi di intelligence. Inoltre, all'**EDPB risulta** che **nei casi in cui si applicano le esenzioni** (ad esempio fornitori di servizi di telecomunicazioni e postali), deve essere ottenuta la preventiva approvazione da parte dei commissari giudiziari nell'eventualità in cui le autorità di contrasto o i servizi di intelligence **chiedano** accesso a questi dati**, e invita la Commissione europea a confermare la correttezza di quanto precede nella sua decisione**.

206. L'EDPB riconosce che l'art. 44(2) dell'IPA 2016 consente l'intercettazione di comunicazioni se una delle parti (mittente o destinatario) ha acconsentito e vi è un'autorizzazione a norma della legge RIPA 2000 o della legge Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11), ossia ai sensi del quadro giuridico precedente all'istituzione dei commissari giudiziari. L'EDPB **invita** la Commissione europea a chiarire se ciò significa che nei casi in cui esiste un consenso unilaterale, la procedura di approvazione preventiva non si applichi affatto.

207. In merito alla vigilanza *ex post*, è importante anche verificare che sia assicurata un'efficiente vigilanza indipendente e senza lacune, in particolare laddove non sia prevista *ex ante*.

208. L'EDPB osserva che per quanto riguarda gli articoli da 48 a 52 dell'IPA 2016, è prevista una valutazione *ex post* da parte dei commissari giudiziari, e **invita la Commissione europea a chiarire in quali circostanze e su iniziativa di quali soggetti debba essere condotta tale revisione *ex post***.

209. Secondo l'art. 229(4) dell'IPA 2016, l'IPC non è tenuto a vigilare sull'esercizio di talune funzioni. In proposito l'EDPB esorta la Commissione europea a chiarire le disposizioni dell'art. 229(4)(d) e (e) dell'IPA 2016, relativamente al loro impatto pratico sulla competenza di supervisione dell'IPC. **All'EDPB risulta che l'ICO sia l'autorità di controllo competente quando si applicano le esenzioni di cui all'art. 229(4) dell'IPA 2016, e l'EDPB invita la Commissione europea a confermare la correttezza di quanto precede nella sua decisione.**

210. **A quanto risulta, nello svolgimento** della funzione di vigilanza *ex post* il ruolo **dell'IPC** si limita a esprimere raccomandazioni nei casi di non conformità, e a informare l'interessato, qualora l'errore sia grave e sia nell'interesse pubblico della persona essere informata. **L'EDPB invita la Commissione europea a chiarire con quali modalità l'IPCO può effettivamente assicurare il rispetto della legge.**

211. **Infine, all'EDPB risulta che le persone interessate non possono rivolgersi direttamente all'IPCO, ma devono presentare un reclamo presso l'ICO, il quale ha invece limitate competenze nel campo della**

[140] Osserva inoltre, tuttavia, che nell'annullare lo scudo per la privacy in *Schrems II*, la Corte ha preso nota del fatto che, secondo la legge degli Stati Uniti, la cosiddetta Corte FISA "*non autorizza singole misure di sorveglianza, ma piuttosto programmi di sorveglianza (quali PRISM e UPSTREAM) basandosi sulle certificazioni annuali*." (paragrafo 179).

sicurezza nazionale. L'EDPB esorta quindi la Commissione europea a chiarire ulteriormente in che modo sia garantita a termini di legge la trattazione di reclami da parte dell'IPCO in questi casi.

4.3.4. Mezzi di ricorso

212. Alla luce delle sentenze *Schrems I* e *Schrems II* della Corte, è chiaro che un'efficace protezione giudiziaria ai sensi dell'articolo 47 della Carta dell'UE è di fondamentale importanza per accertare l'adeguatezza di un paese terzo. La suddetta giurisprudenza ha inoltre evidenziato la necessità di prestare particolare attenzione, in proposito, all'effettività della tutela giudiziaria rispetto all'accesso ai dati personali per finalità di sicurezza nazionale.

213. **L'EDPB riconosce che il Regno Unito ha istituito l'IPT. L'IPT è competente per le cause relative all'uso dei poteri investigativi non solo da parte delle autorità di contrasto, ma anche da parte dei servizi di intelligence. A quanto risulta all'EDPB, l'IPT opera quindi come vero e proprio tribunale ai sensi dell'articolo 47 della Carta dell'UE. A tale riguardo, la Commissione europea è invitata a confermare che l'IPT disponga di tutti i poteri menzionati nel considerando 262 del progetto di decisione, indipendentemente dalla base giuridica in forza della quale è avanzato il reclamo.**

214. L'attuazione di forme "discrete" di sorveglianza ("discreet surveillance") da parte delle agenzie di intelligence significa che spesso l'oggetto della sorveglianza, ovvero l'interessato, è e sarà all'oscuro di tale sorveglianza. In questo contesto, nell'analizzare il diritto degli Stati Uniti, l'EDPB ha espresso molte volte la propria preoccupazione per il requisito della legittimazione ad agire in giudizio come interpretato nel diritto statunitense nei casi di sorveglianza. Alla luce di ciò, l'EDPB osserva che per la presentazione di un reclamo presso l'IPT è richiesto unicamente un test di "ragionevole convinzione", secondo il quale il reclamante deve dimostrare di essere potenzialmente a rischio di essere oggetto di una misura di sorveglianza.

215. Nella sua valutazione relativa all'IPT, l'EDPB tiene particolarmente conto del fatto che il funzionamento dell'IPT è stato ripetutamente giudicato conforme alla CEDU, come interpretata dalla Corte EDU.