Parere 15/2021 relativo al progetto di decisione di esecuzione della Commissione europea a norma della direttiva (UE) 2016/680 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 51, paragrafo 1, lettera g), della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio[1] ("direttiva sulla protezione dei dati"),

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO IL SEGUENTE PARERE:

1 SINTESI

1. Il 19 febbraio 2021 la Commissione europea ha approvato il progetto di decisione di esecuzione sull'adeguata protezione dei dati personali da parte del Regno Unito a norma della direttiva sulla protezione dei dati ("progetto di decisione")[2]. In seguito la Commissione europea ha avviato la procedura per la sua adozione formale.

2. Alla stessa data la Commissione europea ha chiesto il parere del comitato europeo per la protezione dei dati ("EDPB")[3]. La valutazione dell'EDPB sull'adeguatezza del livello di protezione garantito nel Regno Unito si è basata sull'esame del progetto di decisione stesso, oltre che sull'analisi della documentazione messa a disposizione dalla Commissione europea.

3. Come principale riferimento per questo lavoro, l'EDPB ha fatto ricorso alle raccomandazioni sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati[4] adottate il 2 febbraio 2021, nonché alla giurisprudenza pertinente riportata nelle raccomandazioni 2/2020 relative alle garanzie essenziali europee per le misure di sorveglianza[5].

4. L'obiettivo principale dell'EDPB è fornire un parere alla Commissione europea sull'adeguatezza del livello di protezione offerto alle persone nel Regno Unito. È importante precisare che il comitato non si aspetta che il quadro giuridico del Regno Unito riproduca la normativa europea sulla protezione dei dati.

5. Tuttavia l'EDPB ricorda che, secondo l'articolo 36 della direttiva sulla protezione dei dati e la giurisprudenza della Corte di giustizia dell'Unione europea ("la Corte"), affinché il paese terzo in esame venga considerato in grado di fornire un livello adeguato di protezione la sua legislazione dev'essere sostanzialmente equivalente ai principi fondamentali sanciti dalla direttiva stessa. Nell'ambito della protezione dei dati, l'EDPB osserva che il quadro giuridico configurato dalla direttiva sulla protezione

[1] GU L 119 del 4.5.2016, pag. 89.
[2] Cfr. 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] Cfr. Raccomandazioni 1/2021 dell'EDPB sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, adottate il 2 febbraio 2021, https://edpb.europa.eu/system/files/2021-05/recommendations012021onart.36led.pdf_it.pdf.
[5] Cfr. Raccomandazioni 2/2020 dell'EDPB relative alle garanzie essenziali europee per le misure di sorveglianza, adottate il 10 novembre 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_it.

dei dati e il quadro giuridico del Regno Unito sono fortemente allineati su alcune disposizioni fondamentali, ad esempio le nozioni ("dati personali", "trattamento dei dati personali", "titolare del trattamento"), i presupposti per la liceità e la correttezza del trattamento per scopi legittimi, la limitazione delle finalità, la qualità e la proporzionalità dei dati, la conservazione, la sicurezza e la riservatezza dei dati, la trasparenza, le categorie particolari di dati e il processo decisionale automatizzato e la profilazione.

6. L'EDPB raccomanda alla Commissione europea di integrare la sua analisi con informazioni sull'esistenza di un meccanismo per informare le autorità competenti degli Stati membri in merito a trattamenti o comunicazioni ulteriori effettuati da parte delle autorità del Regno Unito a cui hanno trasferito i dati personali e di determinare l'efficacia di un tale meccanismo nel quadro dell'ordinamento giuridico britannico.

7. L'EDPB ritiene che le disposizioni di cui al capo 5 della parte 3 del Data Protection Act 2018 ("legge del 2018 sulla protezione dei dati") prevedano, in linea di principio, un livello di protezione sostanzialmente equivalente a quello garantito dal diritto dell'UE per quanto riguarda il trasferimento di dati personali da un'autorità di contrasto del Regno Unito a un paese terzo.

8. Pur prendendo atto della capacità del Regno Unito, nell'ambito del suo quadro giuridico, di riconoscere che determinati territori forniscono un livello adeguato di protezione dei dati alla luce del quadro giuridico britannico in materia, l'EDPB desidera sottolineare che ciò potrebbe comportare rischi per quanto riguarda la protezione dei dati personali trasferiti dall'UE, specialmente se, in futuro, il quadro britannico di protezione dei dati dovesse discostarsi dall'*acquis* dell'UE. **Per le suddette situazioni è opportuno che la Commissione europea svolga il suo ruolo di monitoraggio e, qualora non sia mantenuto un livello di protezione sostanzialmente equivalente dei dati trasferiti dall'UE, consideri la possibilità di modificare la decisione di adeguatezza per introdurre garanzie specifiche per i dati trasferiti dall'UE e/o di sospendere la decisione di adeguatezza.**

9. **Infine, per quanto riguarda gli accordi internazionali conclusi tra il Regno Unito e i paesi terzi,** si invita la Commissione europea a esaminare l'interazione tra il quadro di protezione dei dati del Regno Unito e i suoi impegni internazionali, in particolare per garantire la continuità del livello di protezione quando i dati personali sono trasferiti dall'UE al Regno Unito sulla base della decisione di adeguatezza del Regno Unito e vengono successivamente trasferiti verso altri paesi terzi, nonché a monitorare costantemente e a intervenire, ove necessario, nel caso in cui la conclusione di accordi internazionali tra il Regno Unito e paesi terzi rischi di compromettere il livello di protezione dei dati personali previsto nell'UE.

10. A questo proposito, l'EDPB sottolinea che l'entrata in vigore dell'accordo tra il Regno Unito e gli Stati Uniti sull'accesso ai dati elettronici per contrastare i reati gravi ("UK-US CLOUD Act Agreement")[6] può incidere sui trasferimenti successivi da parte delle autorità di contrasto del Regno Unito, in particolare per quanto riguarda l'emissione e la trasmissione di ordini conformemente all'articolo 5 del suddetto accordo.

11. L'EDBP raccomanda inoltre che la Commissione europea controlli costantemente se la conclusione di futuri accordi con paesi terzi per la cooperazione in materia di contrasto, che costituiscano il fondamento giuridico per il trasferimento di dati personali a tali paesi, possa influire sulle condizioni applicabili alla condivisione successiva delle informazioni raccolte. Si raccomanda alla Commissione di

[6] Cfr. Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington DC, Stati Uniti, 3 ottobre 2019.

monitorare in particolare se le disposizioni di tali accordi internazionali possano incidere sull'applicazione della legislazione britannica in materia di protezione dei dati e comportare ulteriori limitazioni o deroghe in relazione all'uso e alla comunicazione all'estero delle informazioni raccolte a fini di contrasto. L'EDPB ritiene che tali elementi informativi e valutazioni siano fondamentali per consentire un esame completo del livello di protezione offerto dalle norme e dalle prassi vigenti nel Regno Unito in relazione alla comunicazione di dati all'estero.

2 INTRODUZIONE

2.1 Quadro normativo in materia di protezione dei dati del Regno Unito

12. Poiché il Regno Unito era uno Stato membro dell'UE fino al 31 gennaio 2020, il suo quadro normativo in materia di protezione dei dati si basa in gran parte su quello dell'UE, in particolare sulla direttiva sulla protezione dei dati e sul 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 ("GDPR"). Inoltre la legge del 2018 sulla protezione dei dati, che è entrata in vigore il 23 maggio 2018 e ha abrogato la legge del 1998 sulla protezione dei dati, recepisce nella parte 3 la direttiva sulla protezione dei dati, oltre a specificare ulteriormente l'applicazione del GDPR nel diritto britannico, e a conferire poteri e compiti all'autorità nazionale di controllo della protezione dei dati, ossia l'Ufficio del commissario all'informazione del Regno Unito (Information Commissioner's Office, ICO).

13. Come indicato nel considerando 12 del progetto di decisione, il governo del Regno Unito ha promulgato l'"European Union (Withdrawal) Act 2018" (legge del 2018 relativa al recesso dall'Unione europea), che incorpora la legislazione dell'UE direttamente applicabile nel diritto del Regno Unito. In virtù di tale legge, i ministri del Regno Unito hanno il potere di adottare atti di diritto derivato, tramite strumenti legislativi, per apportare al diritto dell'UE mantenuto in seguito al recesso del Regno Unito dall'UE le modifiche necessarie per adattarlo al contesto nazionale.

14. Di conseguenza il quadro giuridico applicabile nel Regno Unito dopo la fine del periodo di transizione[7] comprende:

- il regolamento generale sulla protezione dei dati del Regno Unito ("GDPR del Regno Unito"), incorporato nel diritto del Regno Unito in virtù della legge del 2018 relativa al recesso dall'Unione europea, modificato dai regolamenti DPPEC del 2019 (Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019);
- la legge del 2018 sulla protezione dei dati, modificata dai regolamenti DPPEC 2019, e i regolamenti DPPEC 2020 (Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020); e
- la legge del 2016 sui poteri di indagine (Investigatory Powers Act 2016, "IPA 2016"),

che nel loro insieme formano il quadro normativo in materia di protezione dei dati del Regno Unito.

2.2 Ambito della valutazione dell'EDPB

[7] La fine del periodo di transizione è fissata al 31 dicembre 2020, data dopo la quale il diritto dell'UE non trova più applicazione nel Regno Unito. La fine del "periodo di grazia" è fissata al più tardi al 30 giugno 2021 e si riferisce al periodo aggiuntivo durante il quale la trasmissione dei dati personali dall'UE al Regno Unito non è considerata un trasferimento.

15. Il progetto di decisione della Commissione europea è il risultato di una valutazione del quadro normativo in materia di protezione dei dati del Regno Unito, seguita da discussioni con il governo del Regno Unito. Ai sensi dell'articolo 51, paragrafo 1, lettera g), della direttiva sulla protezione dei dati, il comitato è tenuto a formulare un parere indipendente sulle conclusioni della Commissione europea, a individuare eventuali carenze nel quadro giuridico in materia di adeguatezza e ad adoperarsi per elaborare proposte al fine di porvi rimedio.

16. Come indicato nelle raccomandazioni sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati, "*le informazioni fornite dalla Commissione europea dovrebbero essere esaustive e consentire al comitato di effettuare una propria valutazione in merito al livello di protezione dei dati nel paese terzo*[8]".

17. A questo proposito è opportuno notare che l'EDPB ha ricevuto per tempo solo parte dei documenti pertinenti ai fini dell'esame del quadro giuridico del Regno Unito e ha ricevuto la maggior parte degli atti legislativi del Regno Unito cui si fa riferimento nel progetto di decisione attraverso i link citati in quest'ultimo. La Commissione europea non è stata in grado di fornire all'EDPB spiegazioni e impegni scritti da parte del Regno Unito in relazione agli scambi tra le autorità del Regno Unito e la Commissione stessa pertinenti ai fini di tale esercizio[9].

18. Tenendo conto di quanto sopra e a causa del tempo limitato (due mesi) concesso all'EDPB per adottare il presente parere, il comitato ha scelto di concentrarsi su alcuni punti specifici nel progetto di decisione e di fornire la propria analisi e opinione in merito. Analizzando il diritto e la prassi di un paese terzo che è stato un membro dell'UE fino a poco tempo addietro, l'EDPB ha ovviamente individuato molti elementi di equivalenza sostanziale. In considerazione del suo ruolo nella determinazione dell'adeguatezza e della quantità di atti giuridici e prassi da analizzare, l'EDPB ha deciso di concentrarsi sugli aspetti rispetto ai quali ha ravvisato maggiore necessità di approfondimento.

19. L'EDPB ha tenuto conto del quadro europeo applicabile in materia di protezione dei dati, inclusi gli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'UE ("Carta dell'UE"), che tutelano rispettivamente il diritto al rispetto della vita privata e familiare, il diritto alla protezione dei dati personali e il diritto a un ricorso effettivo e a un giudice imparziale, nonché l'articolo 8 della Convenzione europea dei diritti dell'uomo ("CEDU") che tutela il diritto al rispetto della vita privata e familiare. Oltre a quanto sopra, l'EDPB ha preso in esame le prescrizioni della direttiva sulla protezione dei dati e la giurisprudenza in materia.

20. L'obiettivo di questo esercizio è fornire alla Commissione europea un parere per la valutazione dell'adeguatezza del livello di protezione nel Regno Unito. Il concetto di "livello di protezione

[8] Cfr. Raccomandazioni 1/2021 sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, paragrafo 15, pag. 6.

[9] Si tratta delle parti in cui la Commissione europea, nel progetto di decisione, cita le spiegazioni fornite dalle autorità del Regno Unito senza allegare documentazione scritta proveniente dalle autorità stesse a sostegno di tali spiegazioni, ad esempio per quanto riguarda: gli effetti delle disposizioni transitorie e l'assenza di una norma relativa alla loro scadenza (clausola di temporaneità) (considerando 87), esempi di consenso come base appropriata per il trattamento (nota 68), il termine "inesatto" per indicare dati personali "errati o fuorvianti" (nota 79), il mandato dell'ISC (nota 245), i requisiti poco stringenti per proporre un reclamo all'IPT e il fatto che non è insolito che quest'ultimo stabilisca che il reclamante non sia mai stato realmente oggetto di indagini da parte di un'autorità pubblica (nota 263), la combinazione di poteri derivanti dal diritto positivo e dalla "common law" (nota 52), i poteri di prerogativa esercitati dal governo (nota 62), il fatto che altre organizzazioni sono libere di seguire, se lo desiderano, i principi del codice di condotta sulla gestione delle informazioni della polizia ("MoPI Code of Practice") (nota 86).

adeguato", che esisteva già nella direttiva 95/46/CE, è stato ulteriormente sviluppato dalla Corte. È importante ricordare la norma fissata dalla Corte nella sentenza *Schrems I*, secondo la quale, sebbene 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"[10]. Pertanto l'obiettivo non è quello di rispecchiare punto per punto la legislazione europea, ma di stabilire le prescrizioni essenziali e centrali della legislazione in esame. L'adeguatezza può essere conseguita anche attraverso la combinazione tra diritti riconosciuti agli interessati e obblighi posti in capo a chi effettua il trattamento o esercita il controllo sul trattamento, unitamente al controllo da parte di organismi indipendenti. Le norme in materia di protezione dei dati, tuttavia, sono efficaci solo se sono applicabili 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 applicazione efficienti è di fondamentale importanza per garantire l'efficacia delle norme sulla protezione dei dati[11].

2.3 Osservazioni e preoccupazioni generali

2.3.1. Impegni internazionali assunti dal Regno Unito

21. A norma dell'articolo 36, paragrafo 2, lettera c), della direttiva sulla protezione dei dati, e delle raccomandazioni sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati[12], nel valutare l'adeguatezza del livello di protezione di un paese terzo la Commissione europea tiene in considerazione, tra le altre cose, gli impegni internazionali assunti dal paese terzo, o altri obblighi derivanti dalla sua partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali, nonché l'attuazione di tali obblighi. Inoltre si dovrebbe tenere in considerazione l'adesione del paese terzo alla convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale ("convenzione 108")[13] e al relativo protocollo addizionale[14].

22. **A tal riguardo l'EDPB accoglie favorevolmente il fatto che il Regno Unito abbia aderito alla CEDU e sia soggetto alla giurisdizione della Corte europea dei diritti dell'uomo (CEDH). Inoltre il Regno Unito ha aderito alla convenzione 108 e al suo protocollo addizionale, ha firmato la convenzione 108+[15] nel 2018 e attualmente sta lavorando alla sua ratifica.**

[10] Cfr. causa C-362/14, *Maximillian Schrems/Data Protection Commissioner*, 6 ottobre 2015, ECLI:EU:C:2015:650 (*Schrems I*), punti 73-74.
[11] Cfr. Raccomandazioni 1/2021 dell'EDPB sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, paragrafo 14, pag. 5.
[12] Cfr. Raccomandazioni 1/2021 dell'EDPB sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, punto 24, pag. 7.
[13] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, del 28 gennaio 1981 ("convenzione 108").
[14] Cfr. il protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri, aperto alla firma l'8 novembre 2001.
[15] Cfr. il protocollo, del 18 maggio 2018, che modifica la convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (di seguito "convenzione 108+").

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

23. Come indicato nel considerando 171 del progetto di decisione, la Commissione europea deve tener conto del fatto che, una volta terminato il periodo di transizione previsto dall'accordo di recesso[16], e non appena la disposizione provvisoria[17] di cui all'articolo FINPROV.10A dell'accordo sugli scambi commerciali e la cooperazione UE-Regno Unito[18] cesserà di applicarsi, il Regno Unito gestirà, applicherà e farà rispettare il proprio regime di protezione dei dati. Ciò può comportare, in particolare, modifiche o cambiamenti del quadro normativo in materia di protezione dei dati preso in esame nel progetto di decisione, nonché altri sviluppi pertinenti.

24. La Commissione europea ha pertanto deciso di includere nel suo progetto di decisione una clausola di temporaneità[19], fissando la data di scadenza a quattro anni dalla sua entrata in vigore.

25. È importante notare che la possibilità che i ministri e il segretario di Stato del Regno Unito adottino atti di diritto derivato dopo la fine del periodo di transizione potrebbe determinare in futuro una divergenza significativa tra il quadro normativo in materia di protezione dei dati del Regno Unito e quello dell'UE.

26. Infine, non solo il Regno Unito non è più vincolato alla giurisprudenza della Corte dopo il termine del periodo di transizione, ma la giurisprudenza pregressa della Corte, considerata come giurisprudenza mantenuta nel quadro giuridico del Regno Unito, potrebbe non essere più vincolante per il Regno Unito, in particolare perché quest'ultimo ha la possibilità di modificare il corpus del diritto dell'UE mantenuto dopo la fine del periodo di transizione e la Corte suprema non è vincolata da alcuna giurisprudenza UE mantenuta[20].

27. **Considerando i rischi connessi alla possibile deviazione del quadro di protezione dei dati del Regno Unito dall'*acquis* dell'UE dopo la fine del periodo di transizione, l'EDPB accoglie con favore la decisione della Commissione europea di introdurre una clausola di temporaneità di quattro anni per il progetto di decisione. Tuttavia l'EDPB desidera sottolineare l'importanza del ruolo di monitoraggio della Commissione europea[21], che dovrebbe monitorare costantemente e permanentemente tutti gli sviluppi pertinenti nel Regno Unito tali da poter incidere sull'equivalenza sostanziale del livello di protezione dei dati personali trasferiti ai sensi della decisione di adeguatezza del Regno Unito a partire dalla sua entrata in vigore. Inoltre la Commissione europea dovrebbe intervenire in modo appropriato sospendendo, modificando o abrogando la decisione di adeguatezza, in base alle circostanze del caso, qualora, dopo l'adozione di quest'ultima, ricevesse informazioni sul fatto che nel Regno Unito non è più garantito un livello di protezione adeguato.**

[16] 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 29 del 31.1.2020, pag. 7).
[17] La fine del periodo di transizione è fissata al 31 dicembre 2020, data dopo la quale il diritto dell'UE non si applica più nel Regno Unito. La fine del "periodo di grazia" è fissata al più tardi al 30 giugno 2021 e si riferisce al periodo aggiuntivo durante il quale la trasmissione dei dati personali dall'UE al Regno Unito non è considerata un trasferimento.
[18] 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).
[19] Cfr. l'articolo 4 del progetto di decisione. Cfr. anche il considerando 172 del progetto di decisione.
[20] Cfr. articolo 6, paragrafi da 3 a 6, della legge del 2018 relativa al recesso.
[21] Cfr. l'articolo 36, paragrafo 4, della direttiva sulla protezione dei dati.

28. Da parte sua l'EDPB farà quanto in suo potere per informare la Commissione europea di qualsiasi azione pertinente intrapresa dalle autorità di controllo della protezione dei dati degli Stati membri, in particolare con riguardo ai reclami presentati da interessati nell'UE in merito al trasferimento di dati personali dall'UE al Regno Unito.

3 NORME CHE SI APPLICANO AL TRATTAMENTO DEI DATI PERSONALI DA PARTE DELLE AUTORITÀ COMPETENTI PER FINALITÀ DI CONTRASTO IN MATERIA PENALE

3.1 Ambito di applicazione materiale

29. In relazione ai considerando 24 e seguenti del progetto di decisione, l'EDPB prende atto che il progetto di decisione di adeguatezza non contiene molti dettagli sulle attività e sul quadro giuridico applicabile alle agenzie diverse dalla polizia con compiti di contrasto.

30. Ad esempio, il quadro esplicativo del Regno Unito per le discussioni sull'adeguatezza, sezione F: attività di contrasto[22], a pagina 11 indica che **l'agenzia nazionale per la lotta alla criminalità** (National Crime Agency, NCA) potrebbe essere un'autorità di contrasto di particolare interesse che, tra l'altro, ha una più ampia funzione di intelligence criminale. La missione della NCA è quella di raccogliere i dati di intelligence provenienti da una serie di fonti al fine di massimizzare l'analisi, la valutazione e le opportunità tattiche, incluse le intercettazioni tecniche delle comunicazioni, le autorità di contrasto partner nel Regno Unito e all'estero, le agenzie di sicurezza e di intelligence[23]. La NCA è anche uno dei principali interlocutori dei partner internazionali delle forze dell'ordine e svolge un ruolo chiave nello scambio di dati di intelligence criminale[24].

31. L'EDPB prende inoltre atto del fatto che l'agenzia di intelligence britannica "Government Communications Headquarters" ("GCHQ"), le cui attività rientrano tipicamente nell'ambito di applicazione della parte 4 del legge del 2018 sulla protezione dei dati, ovvero la sicurezza nazionale, assume anche un ruolo attivo nel ridurre il danno sociale e finanziario causato al Regno Unito dalle

[22] Cfr. UK Government, 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.

[23] Cfr. il 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.

[24] Anche se non tutte le informazioni trattate dalla NCA sono dati personali, una parte sostanziale potrebbe essere costituita da informazioni personali e le attività qui descritte differiscono da quelle della polizia classica; di conseguenza, una valutazione dell'accesso ai dati personali da parte delle autorità di contrasto nel Regno Unito sarebbe incompleta senza una valutazione approfondita delle attività della NCA. Sembra ragionevole assicurarsi che i principi di protezione dei dati abbiano lo stesso significato per tutte le autorità di contrasto competenti, facendo così luce su un'agenzia che si occupa particolarmente di dati come la NCA. La spiegazione continua nel paragrafo "Looking to the future": "cerchiamo continuamente nuove opportunità per raccogliere, sviluppare e migliorare le capacità tradizionali per aumentare la quantità e la qualità di intelligence disponibile da sfruttare sia nel Regno Unito che all'estero. Per questo stiamo sviluppando la nuova capacità nazionale di utilizzo dei dati (National Data Exploitation Capability), che usa i poteri conferiti all'agenzia dal Crime and Courts Act di collegare, accedere e sfruttare i dati detenuti dal governo. [...] Tutto questo aumenterà la nostra agilità e flessibilità per rispondere alle nuove minacce e operare in modo proattivo, per raccogliere e analizzare informazioni e intelligence sulle minacce emergenti, in modo da poter agire prima che tali minacce si realizzino".

forme gravi di criminalità organizzata, lavorando a stretto contatto con il Ministero degli Interni, la NCA, l'HM Revenue and Customs ("HMRC") e altri dipartimenti del governo[25]. Le sue attività riguardano la lotta contro gli abusi sessuali sui minori, la frode, altri tipi di reati economici, compreso il riciclaggio di denaro, l'uso criminale della tecnologia, la criminalità informatica, la criminalità organizzata dell'immigrazione, compresa la tratta di esseri umani, il contrabbando di droga e armi da fuoco e altre attività di contrabbando.

32. **L'EDPB invita la Commissione europea a completare la sua analisi con un esame delle agenzie che operano nell'ambito delle attività di contrasto e che sembrano aver fatto della raccolta e dell'analisi dei dati, inclusi quelli personali, il fulcro delle loro operazioni quotidiane, in particolare la NCA. Inoltre l'EDPB invita la Commissione a esaminare in modo più dettagliato le agenzie come la GCHQ, le cui attività rientrano nell'ambito sia delle attività di contrasto che della sicurezza nazionale, e il quadro giuridico ad esse applicabile per quanto riguarda il trattamento dei dati personali.**

3.2 Garanzie, diritti e obblighi

3.2.1. Trattamento sulla base del "consenso" dell'interessato

33. L'EDPB prende atto che nei considerando 37 e 38 del progetto di decisione la Commissione europea afferma che **il ricorso al consenso** non è considerato pertinente in uno scenario di adeguatezza, poiché, nelle situazioni di trasferimento, i dati non sono raccolti direttamente presso l'interessato da un'autorità di contrasto del Regno Unito sulla base del consenso.

34. A questo proposito, l'EDPB ricorda che l'articolo 36, paragrafo 2, lettera a), della direttiva sulla protezione dei dati prevede la valutazione di un'ampia serie di elementi che non si limitano alla 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)*".

35. Il consenso nel contesto delle attività di contrasto può essere pertinente quale base giuridica per il trattamento dei dati, quale garanzia aggiuntiva, o più in generale quale fondamento per l'esercizio di poteri investigativi che portano all'acquisizione di dati personali, ad esempio il consenso di una terza parte a perquisire i suoi locali o a confiscare gli archivi di dati.

36. L'EDPB osserva, anche sulla base delle informazioni fornite dalla Commissione europea nel considerando 38 del progetto di decisione, che il ricorso al consenso, così come concepito nel sistema giuridico del Regno Unito, richiederebbe comunque una base giuridica su cui fare affidamento. Ciò significa che, anche se la polizia ha legalmente il potere di trattare i dati a scopo investigativo, in alcune circostanze specifiche (ad esempio la raccolta di un campione di DNA) la polizia potrebbe ritenere opportuno chiedere il consenso dell'interessato.

37. **L'EDPB invita la Commissione europea ad analizzare, in via generale, l'eventuale ricorso al consenso nel contesto di attività di contrasto quale elemento della valutazione dell'adeguatezza di un paese terzo ai sensi della direttiva sulla protezione dei dati.**

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

3.2.2. Diritti delle persone

3.2.2.1 Certificati di sicurezza nazionale

38. Ai sensi dell'articolo 79 del legge del 2018 sulla protezione dei dati, i titolari del trattamento possono richiedere certificati di sicurezza nazionale rilasciati da un ministro, da un membro del gabinetto, dal procuratore generale o dall'avvocato generale per la Scozia, che attestino che le limitazioni degli obblighi e dei diritti sanciti nei capitoli 3 e 4 della parte 3 della legge del 2018 sulla protezione dei dati sono una misura necessaria e proporzionata per la protezione della sicurezza nazionale.

39. Questi certificati hanno lo scopo di fornire ai titolari del trattamento una maggiore certezza del diritto e saranno la prova conclusiva del fatto che la sicurezza nazionale è il contesto nel quale ha luogo il trattamento dei dati personali. Tuttavia è opportuno ricordare che tali certificati non sono un prerequisito per l'applicazione delle restrizioni legate alla sicurezza nazionale, ma costituiscono piuttosto una misura di trasparenza[26].

40. L'EDPB interpreta l'allegato 20 della legge del 2018 sulla protezione dei dati, articoli 17 e 18, nel senso che un certificato di sicurezza nazionale rilasciato ai sensi della legge del 1998 sulla protezione dei dati (di seguito "vecchio certificato") aveva una validità estesa fino al 25 maggio 2019 con riguardo al trattamento dei dati personali ai sensi della legge del 2018 sulla protezione dei dati. Fino a tale data i vecchi certificati, se non sostituiti o revocati, erano trattati come se fossero stati rilasciati ai sensi della legge del 2018 sulla protezione dei dati. Tuttavia, in mancanza di una data di scadenza esplicita su un certificato di sicurezza nazionale rilasciato ai sensi della legge del 2018 sulla protezione dei dati, l'EDPB interpreta le norme nel senso che tale certificato continuerà ad avere effetto in relazione al trattamento ai sensi della legge del 1998 sulla protezione dei dati, a meno che il certificato stesso non sia revocato o annullato.[27] Anche se la protezione fornita dai vecchi certificati è limitata al trattamento dei dati personali ai sensi della legge del 1998 sulla protezione dei dati, l'EDPB prende atto del fatto che in virtù di tale legge possono essere rilasciati nuovi certificati di sicurezza nazionale per i dati personali trattati ai sensi di tale legge.[28]

41. **Per motivi di completezza, l'EDPB invita la Commissione europea a chiarire nel progetto di decisione di adeguatezza che i certificati di sicurezza nazionale possono ancora essere rilasciati ai sensi della legge del 1998 sulla protezione dei dati. Inoltre l'EDPB invita la Commissione europea a descrivere nel progetto di decisione di adeguatezza i meccanismi di ricorso e supervisione per quanto riguarda i certificati rilasciati ai sensi della legge del 1998 sulla protezione dei dati. Infine l'EDPB invita la Commissione europea a includere nel suo progetto di decisione di adeguatezza il numero dei certificati esistenti rilasciati ai sensi della legge del 1998 sulla protezione dei dati e a monitorare attentamente questo aspetto.**

3.2.2.2 Processo decisionale automatizzato ai sensi della direttiva sulla protezione dei dati

42. L'EPDB sottolinea che l'articolo 11, paragrafo 3, della direttiva sulla protezione dei dati vieta la profilazione che porta alla discriminazione delle persone fisiche sulla base di categorie particolari di

[26] Cfr. UK Home Office, The Data Protection Act 2018, National Security Certificates Guidance, agosto 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf, pag. 4.
[27] Cfr. UK Home Office, The Data Protection Act 2018, National Security Certificates Guidance, agosto 2020, pag.5.
[28] Cfr. UK Home Office, The Data Protection Act 2018, National Security Certificates Guidance, agosto 2020, pag. 5.

dati personali. Tuttavia l'EDPB osserva che l'articolo 50 della legge del 2018 sulla protezione dei dati, che stabilisce le norme specifiche per il processo decisionale automatizzato, non prevede tale divieto.

43. **L'EDPB invita pertanto la Commissione europea a verificare questo aspetto e a indicare esplicitamente le sue conclusioni nella decisione di adeguatezza. Inoltre l'EDPB invita la Commissione europea a monitorare attentamente i casi connessi a processi decisionali automatizzati e alla profilazione.**

44. Secondo le raccomandazioni sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati, "*[i]l diritto del paese terzo dovrebbe, in ogni caso, prevedere le garanzie necessarie per i diritti e le libertà dell'interessato. A tale riguardo dovrebbe essere presa in considerazione l'esistenza di un meccanismo per informare le autorità competenti dello Stato membro pertinente in merito a qualsiasi ulteriore trattamento, come l'uso dei dati trasferiti per la profilazione su larga scala*"[29].

45. **L'EDPB invita la Commissione a valutare questo elemento alla luce delle indicazioni fornite dall'EDPB nelle sue raccomandazioni sui criteri di riferimento.**

3.2.3. Trasferimenti successivi

46. Secondo le raccomandazioni sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati, i trasferimenti successivi di dati personali da parte del destinatario iniziale verso un altro paese terzo o un'altra organizzazione internazionale non devono compromettere il livello di protezione, previsto nell'Unione, delle persone fisiche i cui dati vengono trasferiti. Di conseguenza tali trasferimenti successivi di dati dovrebbero essere consentiti soltanto laddove sia garantita la continuità del livello di protezione offerto dal diritto dell'Unione. L'EDPB ritiene che, come sottolineato dalla Commissione europea nella sua valutazione, le disposizioni di cui alla parte 3, capo 5, della legge del 2018 sulla protezione dei dati, e in particolare l'articolo 73, prevedano, in linea di principio, un livello di protezione sostanzialmente equivalente a quello garantito dal diritto dell'UE, per quando riguarda il trasferimento di dati personali da un'autorità di contrasto del Regno Unito a un paese terzo.

47. In primo luogo l'articolo 73, paragrafo 1, lettera b), della legge del 2018 sulla protezione dei dati prevede che un titolare del trattamento non possa trasferire dati personali a un paese terzo o a un'organizzazione internazionale a meno che, "*nel caso in cui i dati personali siano stati originariamente trasmessi o altrimenti resi disponibili al titolare del trattamento o a un'altra autorità competente da uno Stato membro diverso dal Regno Unito, tale Stato membro, o qualsiasi persona con sede in tale Stato membro che sia un'autorità competente ai fini della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, abbia autorizzato il trasferimento conformemente alla legislazione dello Stato membro*". Tali disposizioni sembrano essere in linea con le raccomandazioni sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati, che prevedono che si debba anche tenere conto dell'esistenza di un meccanismo che consenta alle autorità competenti dello Stato membro interessato di essere informate e di autorizzare tale trasferimento successivo dei dati. Il destinatario iniziale dei dati trasferiti dall'UE dovrebbe essere responsabile e in grado di dimostrare che l'autorità competente dello Stato membro ha autorizzato il trasferimento successivo e che sono previste garanzie adeguate per i trasferimenti successivi in assenza di una decisione di adeguatezza relativa al paese terzo verso il quale i dati verrebbero successivamente trasferiti. "*In tale contesto è*

[29] Cfr. Raccomandazioni 1/2021 dell'EDPB sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, punti 59-61.

opportuno prendere in considerazione l'esistenza di un obbligo o un impegno ad attuare meccanismi codificati di gestione definiti dalle autorità dello Stato membro che effettua il trasferimento"[30].

48. **L'EDPB invita la Commissione a valutare questo elemento alla luce delle indicazioni fornite dall'EDPB nelle sue raccomandazioni sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati.**

49. In secondo luogo, come spiegato al considerando 81 del progetto di decisione, il segretario di Stato del Regno Unito ha il potere di riconoscere che un paese terzo (o un territorio o un settore all'interno del paese terzo), un'organizzazione internazionale, o una descrizione di tale paese, territorio, settore od organizzazione garantiscono un adeguato livello di protezione dei dati personali, previa consultazione dell'ICO[31]. 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 36, paragrafo 2, lettere da a) a c), della direttiva sulla protezione dei dati, in combinato disposto con il considerando 67 della direttiva sulla protezione dei dati e la giurisprudenza dell'UE mantenuta. Ciò significa che, nel valutare il livello di protezione adeguato di un paese terzo, si applica la norma pertinente secondo cui occorre determinare se il paese terzo in questione assicuri un livello di protezione "sostanzialmente equivalente" a quello garantito nel Regno Unito. Pur prendendo atto della capacità del Regno Unito, ai sensi della legge del 2018 sulla protezione dei dati, di riconoscere che determinati territori sono in grado di garantire un adeguato livello di protezione alla luce del quadro normativo in materia di protezione dei dati del Regno Unito, l'EDPB desidera evidenziare che tali territori potrebbero non beneficiare, ad oggi, di una decisione di adeguatezza emessa dalla Commissione europea che riconosca un livello di protezione "sostanzialmente equivalente" a quello garantito nell'UE. Ciò potrebbe comportare rischi rispetto alla protezione fornita ai dati personali trasferiti dall'UE, soprattutto se il quadro normativo in materia di protezione dei dati del Regno Unito dovesse discostarsi dall'*acquis* dell'UE in futuro. Si noti che, a luglio 2020, il caso emblematico *Schrems II* della Corte[32] ha portato all'invalidazione della decisione "scudo per la privacy" relativa all'adeguatezza degli USA in quanto, secondo la Corte, il quadro giuridico statunitense non poteva essere considerato in grado di fornire un livello di protezione sostanzialmente equivalente a quello dell'UE. Tuttavia le sentenze già adottate dalla Corte, considerate come giurisprudenza mantenuta nel quadro giuridico del Regno Unito, potrebbero non vincolare più il Regno Unito in quanto, in particolare, quest'ultimo ha la possibilità di modificare il diritto dell'UE mantenuto dopo la fine del periodo di transizione e la sua Corte suprema non è vincolata da alcuna giurisprudenza UE mantenuta[33].

50. **L'EDPB invita quindi la Commissione europea a monitorare attentamente il processo e i criteri di valutazione dell'adeguatezza utilizzati dalle autorità del Regno Unito nei confronti di altri paesi terzi, in particolare per quanto riguarda i paesi terzi non riconosciuti come adeguati dall'UE a norma della direttiva sulla protezione dei dati.**

51. Qualora la Commissione europea riscontrasse che un paese terzo ritenuto adeguato dal Regno Unito non assicura un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE a norma dell'articolo 36 della direttiva sulla protezione dei dati, **l'EDPB invita la Commissione ad**

[30] Cfr. Raccomandazioni 1/2021 dell'EDPB sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, punti 55 e 56.
[31] Cfr. sezione 182, paragrafo 2, della legge del 2018 sulla protezione dei dati. Cfr. anche il "Memorandum of Understanding" sul ruolo dell'ICO relativo alle nuove valutazioni di adeguatezza nel 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/.
[32] Cfr. causa C-311/18, *Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems*, 16 luglio 2020, ECLI:EU:C:2020:559 (*Schrems II*).
[33] Cfr. sezione 6, paragrafi da 3 a 6, della legge EU (Withdrawal) Act 2018.

adottare tutte le misure necessarie quali, ad esempio, modificare la decisione di adeguatezza del Regno Unito per introdurre garanzie specifiche per i dati personali provenienti dall'UE, e/o a considerare la possibilità di sospendere la decisione di adeguatezza del Regno Unito, laddove i dati personali trasferiti dall'UE al Regno Unito siano soggetti a trasferimenti successivi verso il paese terzo in questione sulla base di uno strumento di adeguatezza del Regno Unito.

52. **Infine, in relazione agli accordi internazionali conclusi o che verranno conclusi in futuro dal Regno Unito e al possibile accesso ai dati personali provenienti dall'UE da parte delle autorità di paesi terzi che sono parte di tali accordi, l'EDPB raccomanda che la Commissione europea esamini l'interazione tra il quadro normativo in materia di protezione dei dati del Regno Unito e i suoi impegni internazionali, in particolare per garantire la continuità del livello di protezione in caso di trasferimenti successivi verso altri paesi terzi di dati personali trasferiti dall'UE al Regno Unito sulla base di una decisione di adeguatezza del Regno Unito, e che monitori costantemente e intervenga, ove necessario, in merito alla conclusione di accordi internazionali tra il Regno Unito e paesi terzi che rischiano di compromettere il livello di protezione dei dati personali previsto dall'UE.** Ad esempio, se la Commissione europea ha fatto riferimento alla possibilità che l'accordo tra Regno Unito e Stati Uniti sul CLOUD Act[34] incida sui trasferimenti successivi verso gli USA da parte dei prestatori di servizi del Regno Unito, **l'EDPB evidenzia che l'entrata in vigore di detto accordo può incidere anche sui trasferimenti successivi da parte delle autorità di contrasto nel Regno Unito, in particolare per quanto riguarda l'emissione e la trasmissione di ordini conformemente all'articolo 5 dell'accordo stesso.**

53. L'EDPB ritiene inoltre che la conclusione di futuri accordi con paesi terzi ai fini della cooperazione in materia di attività di contrasto, che costituiscano la base giuridica per il trasferimento di dati personali a tali paesi, possa incidere in modo significativo anche sulle condizioni relative alla condivisione successiva delle informazioni raccolte, in quanto tali accordi possono influenzare il quadro giuridico del Regno Unito sulla protezione dei dati oggetto dell'attuale valutazione.

54. **L'EPDB pertanto raccomanda che la Commissione europea monitori costantemente se la conclusione di accordi futuri tra il Regno Unito e paesi terzi possa incidere sull'applicazione della normativa del Regno Unito in materia di protezione dei dati e preveda ulteriori limitazioni o esenzioni in relazione alla condivisione successiva e all'ulteriore utilizzo e comunicazione all'estero di informazioni raccolte per finalità di contrasto. L'EDPB ritiene che tali informazioni e valutazioni siano fondamentali per consentire un esame completo del livello di protezione offerto dalla legislazione e dalle prassi vigenti nel Regno Unito in relazione alle comunicazioni verso paesi esteri.**

55. Infine l'EDPB prende atto che ai sensi dell'articolo 76, paragrafo 4, lettera b), della legge del 2018 sulla protezione dei dati (Trasferimenti sulla base di circostanze particolari), le autorità di contrasto nel Regno Unito possono trasferire i dati personali verso un paese terzo o a un'organizzazione internazionale qualora il trasferimento "*sia necessario per ottenere consulenza legale in relazione a una qualsiasi delle finalità di contrasto*". **L'EPDB sottolinea che l'articolo 38 della direttiva sulla protezione dei dati non contiene una disposizione corrispondente; pertanto invita la Commissione europea a chiarire la nozione di "consulenza legale" e quali tipologie di dati personali vengano scambiati in tali casi.**

[34] Cfr. Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington DC, Stati Uniti, 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.

3.2.4. Ulteriore trattamento, inclusa l'ulteriore condivisione per scopi di sicurezza nazionale

56. Nelle raccomandazioni sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati, l'EDPB aveva sottolineato che per quanto riguarda l'ulteriore trattamento o comunicazione di dati trasferiti dall'UE per finalità diverse da quelle di contrasto, quali quelle relative alla sicurezza nazionale, dovrebbe essere previsto per legge che anch'esse siano necessarie e proporzionate. Come valutato dalla Commissione europea nel suo progetto di decisione, l'articolo 36, paragrafo 3, della legge del 2018 sulla protezione dei dati, il "Digital Economy Act 2017", il "Crime and Courts Act 2013" e il "Serious Crime Act 2017" forniscono effettivamente un chiaro quadro giuridico che disciplina la condivisione successiva, prevedendo che essa sia conforme alle norme stabilite nella legge del 2018 sulla protezione dei dati.

57. L'EDPB osserva che, nel contesto dell'ulteriore trattamento per altre finalità dei dati personali trasferiti dall'UE, la Commissione europea non ha valutato se esistano meccanismi che consentano alle autorità di contrasto del Regno Unito di informare le autorità competenti degli Stati membri interessati di un possibile ulteriore trattamento dei dati. Si tratta tuttavia di un elemento di cui tenere conto, secondo le raccomandazioni sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati[35]. Inoltre l'esistenza di un meccanismo per informare le autorità competenti degli Stati membri interessati rispetto a un ulteriore trattamento dei dati per finalità di contrasto è considerata anch'essa un aspetto di cui tener conto nel quadro delle raccomandazioni sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati[36].

58. **L'EDPB invita pertanto la Commissione europea a integrare la sua analisi con informazioni sull'esistenza di meccanismi che consentano alle autorità di contrasto del Regno Unito di notificare alle autorità competenti degli Stati membri interessati un eventuale ulteriore trattamento dei dati trasferiti dall'UE.**

59. Per quanto riguarda la condivisione con un'agenzia di intelligence dei dati raccolti da un'autorità di contrasto penale a fini di sicurezza nazionale, la base giuridica che autorizza tale condivisione successiva è la "Counter-terrorism Act 2008" (legge antiterrorismo 2008). A questo proposito l'EDPB osserva che l'ambito di applicazione e le disposizioni dell'articolo 19 della legge antiterrorismo 2008 non sono oggetto di un esame dettagliato nella valutazione della Commissione europea e possono implicare un ulteriore utilizzo di natura più ampia, in particolare per quanto riguarda l'articolo 19, paragrafo 2, della legge antiterrorismo 2008, in base al quale "*le informazioni ottenute da uno dei servizi di intelligence in relazione all'esercizio di una delle sue funzioni possono essere utilizzate da tale servizio in relazione all'esercizio di qualsiasi altra funzione*". A questo proposito l'EDPB sottolinea che, quando sono oggetto di ulteriori trattamenti o comunicazioni, i dati dovrebbero beneficiare del medesimo livello di protezione di cui godevano nel momento in cui sono stati trattati inizialmente dall'autorità competente che ne era destinataria.

3.3 Supervisione e controllo dell'attuazione

60. L'EDPB rileva che la supervisione delle agenzie di contrasto della criminalità è assicurata da una combinazione di commissari diversi, oltre che dall'ICO. Le conclusioni del progetto di decisione di adeguatezza menzionano il commissario per le indagini (Investigatory Powers Commissioner, IPC), il commissario per la conservazione e l'uso di materiale biometrico (Commissioner for the Retention and Use of Biometric Material) e il commissario responsabile della videosorveglianza (Surveillance Camera

[35] Cfr. Raccomandazioni 1/2021 dell'EDPB sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, punto 41 e nota 39.
[36] Cfr. Raccomandazioni 1/2021 dell'EDPB sui criteri di riferimento per l'adeguatezza ai sensi della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, punto 40.

Commissioner). In questo contesto è da notare che la Corte ha ripetutamente sottolineato la necessità di una supervisione indipendente. Per quanto riguarda le questioni relative all'accesso ai dati personali trasferiti al Regno Unito, risulta di particolare importanza il ruolo svolto dall'IPC. Secondo l'interpretazione dell'EDPB, l'IPC può essere considerato un "commissario giudiziario", al pari di altri commissari con analoghe funzioni, cui fare riferimento nelle materie connesse alla sicurezza nazionale; tali commissari giudiziari godono della stessa indipendenza dei giudici, anche quando ricoprono il ruolo di commissari. Per quanto riguarda le funzioni dell'IPC, nel considerando 245 del progetto di decisione la Commissione europea chiarisce che esso opera in modo indipendente ("arm's length body"), pur essendo finanziato dal Ministero degli Interni.

61. Compete inoltre all'IPC la supervisione ex-post delle misure di sorveglianza. Sembra tuttavia che in questa funzione il ruolo dell'IPC sia quello di formulare raccomandazioni nei casi di non conformità e di informare la persona interessata, se l'errore è grave e se è nell'interesse pubblico che la persona ne sia informata.

62. Nel progetto di decisione, l'EDPB non ha trovato ulteriori indicazioni utili a valutare l'indipendenza del commissario per la conservazione e l'uso di materiale biometrico, oltre che del commissario responsabile della videosorveglianza.

63. **La Commissione europea è invitata a valutare ulteriormente l'indipendenza dei commissari giudiziari, anche nei casi in cui il commissario non operi (più) come giudice, nonché a valutare l'indipendenza del commissario per la conservazione e l'uso di materiale biometrico e del commissario responsabile della videosorveglianza.**