2025/2574

23.12.2025

DECISIONE DI ESECUZIONE (UE) 2025/2574 DELLA COMMISSIONE

del 19 dicembre 2025

che modifica la decisione di esecuzione (UE) 2021/1772 della Commissione a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito

[notificata con il numero C(2025) 8771]

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il 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) ([1]), in particolare l'articolo 45, paragrafo 3,

considerando quanto segue:

1. INTRODUZIONE

(1) La decisione di esecuzione (UE) 2021/1772 della Commissione ([2]) conclude che, ai fini dell'articolo 45 del regolamento (UE) 2016/679, il Regno Unito assicura un livello di protezione adeguato dei dati personali trasferiti nell'ambito di applicazione di detto regolamento dall'Unione europea verso il Regno Unito ([3]).

(2) Nell'adottare la decisione di esecuzione (UE) 2021/1772, la Commissione ha tenuto conto del fatto che, alla fine del periodo di transizione previsto dall'accordo sul recesso del Regno Unito di Gran Bretagna e Irlanda del Nord dall'Unione europea e dalla Comunità europea dell'energia atomica ([4]) e non appena la disposizione provvisoria di cui all'articolo 782 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 ([5]) avesse cessato di applicarsi, il Regno Unito avrebbe adottato, applicato e fatto rispettare un nuovo regime di protezione dei dati, diverso da quello in vigore quando era vincolato dal diritto dell'Unione.

(3) Poiché ciò avrebbe potuto comportare modifiche del quadro in materia di protezione dei dati valutato nella decisione di esecuzione (UE) 2021/1772 o altri importanti sviluppi, si è ritenuto opportuno prevedere che tale decisione si applicasse per un periodo di quattro anni a decorrere dalla sua entrata in vigore. Pertanto la decisione di esecuzione (UE) 2021/1772 avrebbe dovuto scadere il 27 giugno 2025, a meno che non fosse prorogata secondo la procedura di cui all'articolo 93, paragrafo 2, del regolamento (UE) 2016/679.

([1]) GU L 119 del 4.5.2016, pag. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) Decisione di esecuzione (UE) 2021/1772 della Commissione, del 28 giugno 2021, a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito (GU L 360 dell'11.10.2021, pag. 1, ELI: http://data.europa.eu/eli/dec_impl/2021/1772/oj).
([3]) Cfr. articolo 1, paragrafo 1, della decisione di esecuzione (UE) 2021/1772. A norma dell'articolo 1, paragrafo 2, di tale decisione, la decisione non riguarda i dati personali che sono trasferiti a fini di controllo dell'immigrazione da parte del Regno Unito o che altrimenti rientrano nell'ambito di applicazione dell'esenzione rispetto a determinati diritti degli interessati a fini di mantenimento dell'effettivo controllo dell'immigrazione a norma dell'allegato 2, paragrafo 4, punto 1, della legge del 2018 del Regno Unito sulla protezione dei dati.
([4]) GU C 384 I del 12.11.2019, pag. 1.
([5]) GU L 149 del 30.4.2021, pag. 10, ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.

(4) Per decidere in merito a un'eventuale proroga della decisione di esecuzione (UE) 2021/1772, la Commissione deve valutare se la conclusione secondo cui il Regno Unito assicura un livello di protezione adeguato rimanga giustificata sotto il profilo fattuale e giuridico alla luce degli sviluppi intervenuti dopo l'adozione della suddetta decisione per quanto riguarda gli elementi di cui all'articolo 45, paragrafo 2, del regolamento (UE) 2016/679.

(5) In particolare, il 23 ottobre 2024 il governo del Regno Unito ha presentato al parlamento del Regno Unito il disegno di legge sull'accesso ai dati e sul loro utilizzo [Data (Use and Access) Bill] ([6]), proponendo modifiche del regolamento generale sulla protezione dei dati del Regno Unito (United Kingdom General Data Protection Regulation, GDPR del Regno Unito) e della legge del 2018 sulla protezione dei dati (Data Protection Act 2018), valutati nella decisione di esecuzione (UE) 2021/1772. Il 24 giugno 2025 la Commissione ha adottato la decisione di esecuzione (UE) 2025/1226 ([7]), che ha prorogato la validità della decisione di esecuzione (UE) 2021/1772 per un periodo di sei mesi fino al 27 dicembre 2025. Questa proroga tecnica limitata nel tempo ha consentito alla Commissione di completare la valutazione dell'adeguato livello di protezione dei dati personali fornito dal Regno Unito sulla base di un quadro giuridico stabile, ossia dopo la conclusione del pertinente processo legislativo ([8]).

(6) Dall'adozione della decisione di esecuzione (UE) 2021/1772 la Commissione ha controllato su base continuativa gli sviluppi della situazione nel Regno Unito ([9]). Conformemente al considerando 281 della decisione di esecuzione (UE) 2021/1772, è stata prestata particolare attenzione all'applicazione pratica delle norme del Regno Unito sul trasferimento di dati personali verso paesi terzi, all'impatto di tale applicazione sul livello di protezione offerto ai dati trasferiti a norma di detta decisione e all'effettività dell'esercizio dei diritti individuali, compresi eventuali sviluppi giuridici e pratici pertinenti riguardanti le eccezioni o le limitazioni relative a tali diritti (in particolare per quanto riguarda il mantenimento dell'effettivo controllo dell'immigrazione), nonché al rispetto delle limitazioni e delle garanzie in materia di accesso da parte delle pubbliche amministrazioni. Assieme ad altri elementi, gli sviluppi giurisprudenziali e la vigilanza da parte dell'ufficio dell'Information Commissioner (ICO) e di altri organismi indipendenti contribuiranno al monitoraggio della Commissione.

(7) Sulla base della valutazione di tali sviluppi, comprese le modifiche del GDPR del Regno Unito e della legge del 2018 sulla protezione dei dati introdotte dalla legge sull'accesso ai dati e sul loro utilizzo [Data (Use and Access) Act], la Commissione conclude che il Regno Unito continua ad assicurare un livello di protezione adeguato dei dati personali trasferiti dall'Unione europea verso il Regno Unito nell'ambito di applicazione del regolamento (UE) 2016/679.

(8) La Commissione conclude inoltre che, alla luce delle modifiche delle pertinenti disposizioni della legge del Regno Unito ([10]), l'esclusione dall'ambito di applicazione della decisione di esecuzione (UE) 2021/1772 dei dati personali trasferiti a fini di controllo dell'immigrazione da parte del Regno Unito o che altrimenti rientrano nell'ambito di applicazione dell'esenzione rispetto a determinati diritti degli interessati ai fini del mantenimento dell'effettivo controllo dell'immigrazione («esenzione per motivi di immigrazione») a norma dell'allegato 2, paragrafo 4, punto 1, della legge del Regno Unito del 2018 sulla protezione dei dati non è più giustificata, come spiegato al considerando 37 della presente decisione.

([6]) Disponibile al seguente indirizzo: https://bills.parliament.uk/bills/3825/news.

([7]) Decisione di esecuzione (UE) 2025/1226 della Commissione, del 24 giugno 2025, che modifica la decisione di esecuzione (UE) 2021/1772 a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito (GU L 2025/1226, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1226/oj).

([8]) La legge sull'accesso ai dati e sul loro utilizzo è stata approvata (Royal Assent) il 19 giugno 2025.

([9]) Articolo 45, paragrafo 4, del regolamento (UE) 2016/679.

([10]) Nel maggio 2021 la Corte d'appello di Inghilterra e Galles aveva ritenuto che l'esenzione per motivi di immigrazione, nella formulazione dell'epoca dell'allegato 2, paragrafo 4, punto 1, della legge del Regno Unito sulla protezione dei dati, fosse incompatibile con il diritto del Regno Unito, in quanto la misura legislativa non conteneva disposizioni specifiche che prevedessero le garanzie elencate all'articolo 23, paragrafo 2, del GDPR del Regno Unito. Per conformarsi alla sentenza, il governo del Regno Unito ha rivisto l'esenzione per motivi di immigrazione approvando i regolamenti 2022 sulla legge del 2018 sulla protezione dei dati (modifica dell'allegato 2, Esenzioni). Tuttavia l'esenzione riveduta è stata nuovamente contestata in quanto non soddisfaceva tutte le disposizioni dell'articolo 23, paragrafo 2, del GDPR del Regno Unito. Con sentenza dell'11 dicembre 2023, la Corte d'appello ha ritenuto nuovamente che l'esenzione per motivi di immigrazione riveduta non fosse compatibile con l'articolo 23, paragrafo 2, del GDPR del Regno Unito. Per conformarsi, il governo del Regno Unito ha successivamente approvato i regolamenti 2024 sulla legge del 2018 sulla protezione dei dati (modifica dell'allegato 2, Esenzioni), entrati in vigore l'8 marzo 2024.

2. IMPORTANTI SVILUPPI RIGUARDANTI LE NORME CHE SI APPLICANO AL TRATTAMENTO DI DATI PERSONALI

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

(9) All'epoca dell'adozione della decisione di esecuzione (UE) 2021/1772 il quadro giuridico in materia di protezione dei dati personali del Regno Unito era costituito dagli atti seguenti:

— il GDPR del Regno Unito ([11]), incorporato nel diritto del Regno Unito ai sensi della legge del 2018 relativa al recesso dall'Unione europea [European Union (Withdrawal) Act 2018] ([12]) e modificato dai regolamenti del 2019 in materia di protezione dei dati, tutela della vita privata e comunicazioni elettroniche (modifiche ecc.) (Uscita dall'UE) [Data Protection, Privacy and Electronic Communications (Amendments ecc.) (EU Exit) Regulations 2019, regolamenti DPPEC] ([13]);

— la legge del 2018 sulla protezione dei dati ([14]), come modificata dai regolamenti DPPEC.

(10) Sebbene le suddette due leggi, che rispecchiavano in larga misura le corrispondenti norme applicabili all'interno dell'Unione europea, continuino a costituire la legislazione del Regno Unito in materia di protezione dei dati, da allora sono state oggetto di alcune modifiche limitate, che riflettono il fatto che il Regno Unito non è più soggetto al diritto dell'Unione europea.

(11) In primo luogo, la legge del 2023 sul diritto dell'Unione mantenuto (revoca e riforma) [Retained EU Law (Revocation and Reform) Act 2023] ([15]) ha chiarito che i principi generali del diritto dell'UE non rientrano più nel diritto interno del Regno Unito dalla fine del 2023 ([16]). Inoltre gli organi giurisdizionali del Regno Unito non sono più tenuti a interpretare il «diritto assimilato» non modificato, precedentemente denominato «diritto dell'Unione mantenuto», in modo conforme ai principi generali del diritto dell'Unione, in quanto tale diritto deve essere invece interpretato in modo compatibile con il diritto interno del Regno Unito ([17]). Tuttavia gli organi giurisdizionali del Regno Unito devono interpretare il diritto assimilato non modificato conformemente alla pertinente giurisprudenza della Corte di giustizia dell'Unione europea emessa prima della fine del periodo di transizione ([18]), come indicato anche nel considerando 13 della decisione di esecuzione (UE) 2021/1772. La legge del 2018 sulla protezione dei dati è stata modificata dalla legge sull'accesso ai dati e sul loro utilizzo per chiarire l'effetto della legge sul diritto dell'Unione mantenuto (revoca e riforma) sulla legislazione del Regno Unito in materia di protezione dei dati. Ad esempio, la sezione 183 A, paragrafo 1, della legge del 2018 sulla protezione dei dati prevede, come regola generale, che qualsiasi nuova normativa (adottata il 20 agosto 2025 o successivamente) che introduce nuovi obblighi o poteri ai fini del trattamento dei dati personali sia considerata soggetta alla legislazione del Regno Unito in materia di protezione dei dati. Ciò significa che il quadro in materia di protezione dei dati del

([11]) General Data Protection Regulation, disponibile all'indirizzo: https://www.legislation.gov.uk/eur/2016/679/contents.

([12]) European Union (Withdrawal) Act 2018, disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2018/16/contents, integrava la legislazione dell'Unione che era direttamente applicabile nel Regno Unito alla fine del periodo di transizione nel diritto del Regno Unito. Il cosiddetto «diritto dell'Unione mantenuto» comprendeva il regolamento (UE) 2016/679 nella sua interezza, inclusi i suoi considerando (cfr. note esplicative della legge del 2018 relativa al recesso dall'Unione europea, paragrafo 83, disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Conformemente a tale atto, il diritto dell'Unione mantenuto senza modifiche doveva essere interpretato dagli organi giurisdizionali del Regno Unito in conformità con la pertinente giurisprudenza della Corte di giustizia dell'Unione europea e con i principi generali del diritto dell'Unione così come efficaci prima della fine del periodo di transizione (denominati rispettivamente «giurisprudenza dell'UE mantenuta» e «principi generali del diritto dell'UE mantenuti»).

([13]) The Data Protection, Privacy and Electronic Communications (Amendments ecc.) (EU Exit) Regulations 2019, disponibili al seguente indirizzo: https://www.legislation.gov.uk/uksi/2019/419/contents/made, come modificati dai regolamenti DPPEC del 2020, disponibili al seguente indirizzo: https://www.legislation.gov.uk/ukdsi/2020/9780348213522. I regolamenti DPPEC modificano il regolamento (UE) 2016/679 come recepito nel diritto del Regno Unito attraverso la legge del 2018 relativa al recesso dall'Unione europea, la legge del 2018 sulla protezione dei dati e altra legislazione in materia di protezione dei dati, al fine di adattarlo al contesto interno.

([14]) Legge del 2018 sulla protezione dei dati, disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2018/12/contents. Prima del recesso del Regno Unito dall'Unione europea e durante il periodo di transizione, la legge del 2018 sulla protezione dei dati ha fissato norme nazionali, ove consentito dal regolamento (UE) 2016/679, specificando e limitando l'applicazione delle norme del regolamento (UE) 2016/679, e ha recepito la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([15]) Disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2023/28.

([16]) Sezione 5 della legge del 2018 relativa al recesso dall'Unione europea, come modificata dalla legge sul diritto dell'Unione mantenuto (revoca e riforma).

([17]) Sezione 5, paragrafo A2, della legge del 2018 relativa al recesso dall'Unione europea, come modificata dalla legge sul diritto dell'Unione mantenuto (revoca e riforma).

([18]) Sezione 6, paragrafi 3 e 7, della legge del 2018 relativa al recesso dall'Unione europea, come modificata dalla legge sul diritto dell'Unione mantenuto (revoca e riforma).

Regno Unito continua a prevalere su altre normative. Ai sensi della sezione 183 A, paragrafo 2, lettera b), della legge del 2018 sulla protezione dei dati, tale presunzione può essere disapplicata se il parlamento del Regno Unito decide deliberatamente di farlo in modo espresso nella legislazione, preservando la sovranità parlamentare. Inoltre la sezione 186, paragrafo 2 A, della legge del 2018 sulla protezione dei dati chiarisce che sulle limitazioni ai diritti degli interessati di cui alla sezione 186, paragrafo 3, della legge del 2018 sulla protezione dei dati non prevale la sezione 186, paragrafo 1, della medesima legge, che prevede che le disposizioni che vietano o limitano la divulgazione di informazioni non prevalgano su determinati diritti in materia di protezione dei dati. Ciò garantisce che, ad esempio, le limitazioni dei diritti degli interessati stabilite nella legge del 2018 sulla protezione dei dati non rientrino di per sé nella «prevalenza della protezione dei dati» di cui alla sezione 186, paragrafo 1, della legge del 2018.

(12) In secondo luogo, dall'adozione della decisione di esecuzione (UE) 2021/1772, la legislazione del Regno Unito in materia di protezione dei dati è stata modificata mediante i regolamenti di modifica del 2023 sulla protezione dei dati (diritti e libertà fondamentali) [Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023] ([19]). Tali regolamenti definiscono i riferimenti ai diritti o alle libertà fondamentali nella legge del 2018 sulla protezione dei dati (precedentemente definiti in modo da includere i diritti e le libertà fondamentali dell'UE ([20])) come riferimenti ai diritti sanciti dalla convenzione europea dei diritti dell'uomo, che sono stati attuati nel diritto interno del Regno Unito ai sensi della legge del 1998 sui diritti umani (Human Rights Act 1998) ([21]). La legge del 1998 sui diritti umani integra nel diritto del Regno Unito i diritti sanciti dalla convenzione europea dei diritti dell'uomo. Tale legge accorda a qualsiasi persona fisica i diritti e le libertà fondamentali di cui agli articoli da 2 a 12 e 14 della convenzione europea dei diritti dell'uomo, agli articoli 1, 2 e 3 del suo primo protocollo e all'articolo 1 del suo tredicesimo protocollo, in combinato disposto con gli articoli 16, 17 e 18 della convenzione medesima. Tra di essi è compreso il diritto al rispetto della vita privata e familiare (così come la protezione dei dati personali rientrante in tale diritto) e il diritto a un equo processo ([22]).

(13) In ultimo luogo, il GDPR del Regno Unito e la legge del 2018 sulla protezione dei dati sono stati oggetto di riforme mirate previste dalle parti 5 e 6 della legge sull'accesso ai dati e sul loro utilizzo. Sebbene il suo ambito di applicazione vada ben oltre la protezione dei dati personali, la legge sull'accesso ai dati e sul loro utilizzo prevede limitate modifiche di diversi aspetti del regime di protezione dei dati, quali, tra l'altro, le norme in materia di trattamento dei dati a scopo di ricerca scientifica, le basi giuridiche del trattamento dei dati, le norme relative al principio di limitazione delle finalità e le condizioni relative al processo decisionale automatizzato. Inoltre la legge sull'accesso ai dati e sul loro utilizzo apporta modifiche alla struttura di governance dell'ICO. Una volta attuate, queste misure sostituiranno l'ICO con una nuova entità, la Information Commission. Il ruolo e le funzioni dell'autorità di regolamentazione in qualità di autorità indipendente di controllo della protezione dei dati nel Regno Unito rimarranno invariati. La legge introduce anche nuovi poteri di esecuzione per l'autorità di regolamentazione.

(14) La presente decisione valuta gli sviluppi legislativi, normativi e di altro tipo attinenti alle conclusioni sul livello di protezione garantita dal Regno Unito, formulate nella decisione di esecuzione (UE) 2021/1772. La valutazione effettuata nella decisione di esecuzione (UE) 2021/1772 rimane valida per quanto riguarda gli aspetti del quadro in materia di protezione dei dati del Regno Unito che non sono stati modificati o influenzati da altri sviluppi successivi all'adozione della decisione di esecuzione (UE) 2021/1772.

(15) Gli sviluppi legislativi, normativi e altri sviluppi importanti sono analizzati in dettaglio nelle sezioni seguenti sulla base del livello di adeguatezza: la Commissione deve determinare se il paese terzo in questione garantisce un livello di protezione «sostanzialmente equivalente» a quello assicurato all'interno dell'Unione europea ([23]). Come chiarito dalla Corte di giustizia dell'Unione europea, non è richiesto un livello di protezione identico ([24]). In particolare, gli strumenti dei quali il paese terzo in questione si avvale per proteggere i dati personali possono essere diversi da quelli attuati all'interno dell'Unione europea, purché si rivelino efficaci, nella prassi, al fine di assicurare un livello adeguato di protezione ([25]). Il livello di adeguatezza non comporta pertanto una duplicazione pedissequa delle norme dell'Unione. La prova consiste, piuttosto, nel determinare se, con la sostanza dei diritti alla protezione dei dati e rendendone l'attuazione, l'azionabilità e il controllo effettivi, il sistema giuridico estero, nel suo insieme, offra il necessario livello di protezione ([26]).

([19]) Disponibili al seguente indirizzo: https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.

([20]) I diritti e le libertà fondamentali dell'UE sono stati mantenuti nel diritto del Regno Unito mediante la sezione 4 della legge del 2018 relativa al recesso dall'Unione europea, abrogata alla fine del 2023 dalla legge sul diritto dell'Unione mantenuto (revoca e riforma).

([21]) Sezione 2, paragrafo 3, dei regolamenti di modifica del 2023 sulla protezione dei dati (diritti e libertà fondamentali).

([22]) Articoli 6, 8, 10 e 13 CEDU (cfr. anche l'allegato 1 della legge del 1998 sui diritti umani).

([23]) Considerando 104 del regolamento (UE) 2016/679.

([24]) Sentenza della Corte di giustizia del 6 ottobre 2015, *Schrems* («*Schrems I*»), C-362/14, ECLI:EU:C:2015:650, punto 73.

([25]) *Schrems I*, punto 74.

([26]) Cfr. comunicazione della Commissione al Parlamento europeo e al Consiglio, Scambio e protezione dei dati personali in un mondo globalizzato, COM(2017) 7 del 10.1.2017, sezione 3.1, pag. 7, disponibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

2.1.1. *Definizioni*

(16) Nel regime di protezione dei dati del Regno Unito continuano ad applicarsi i concetti fondamentali di protezione dei dati che rispecchiano la terminologia del regolamento (UE) 2016/679. Tali concetti sono stati valutati nel considerando 23 della decisione di esecuzione (UE) 2021/1772.

(17) Sebbene abbia lasciato per la maggior parte immutate le definizioni, la legge sull'accesso ai dati e sul loro utilizzo ha introdotto nell'articolo 4, paragrafi 2, 3, 4 e 5, del GDPR del Regno Unito definizioni specifiche relative al trattamento dei dati personali a fini scientifici, storici e statistici. Il paragrafo 2 definisce il «trattamento a fini scientifici» come il trattamento di dati personali effettuato per finalità legate a qualunque ricerca che possa ragionevolmente essere descritta come scientifica. Tale ricerca può essere finanziata con fondi pubblici o privati e può essere svolta come attività commerciale o non commerciale. Rispecchiando il contenuto del considerando 159 del regolamento (UE) 2016/679, il paragrafo 3 fornisce un elenco non esaustivo di esempi di attività di ricerca qualificabili come attività che perseguono finalità scientifiche, tra cui lo sviluppo tecnico, la dimostrazione, la ricerca fondamentale e la ricerca applicata. Il paragrafo 4 chiarisce che la «ricerca storica» comprende la ricerca a fini genealogici, che è riconosciuta come finalità storica anche nel considerando 160 del regolamento (UE) 2016/679. Da ultimo, il paragrafo 5 definisce il trattamento a fini statistici come il trattamento di dati per indagini statistiche o per produrre risultati statistici, dove i dati sono aggregati in misura tale da non costituire più dati personali. I dati trattati o le informazioni risultanti inoltre non devono essere utilizzati per adottare decisioni riguardanti una persona fisica o per intraprendere azioni nei suoi confronti. La definizione è coerente con la nozione di finalità statistiche delineata nel considerando 162 del regolamento (UE) 2016/679.

(18) In conclusione, sebbene le modifiche dell'articolo 4 del GDPR del Regno Unito aggiungano definizioni specifiche di trattamento dei dati a fini scientifici, storici e statistici, tali definizioni sono coerenti con la lettera e lo spirito del regolamento (UE) 2016/679, come risulta dai considerando 159, 160 e 162 succitati.

(19) Aggiungendo il paragrafo 6 all'articolo 4 del GDPR del Regno Unito, la legge sull'accesso ai dati e sul loro utilizzo ha inoltre stabilito un quadro specifico per ottenere il consenso dell'interessato al trattamento dei dati personali per finalità scientifiche. In termini molto simili a quelli del considerando 33 del regolamento (UE) 2016/679, che riconosce che nel settore della ricerca scientifica il consenso non può sempre essere ottenuto per una finalità specifica di trattamento, la nuova disposizione prevede forme più ampie di consenso, permettendo agli interessati di prestare validamente il loro consenso anche quando le finalità esatte della ricerca non possono essere pienamente individuate al momento della raccolta dei dati, a condizione che la richiesta di consenso sia coerente con le norme deontologiche generalmente riconosciute per lo specifico settore della ricerca. In ogni caso, ove possibile, gli interessati devono avere la possibilità di acconsentire al trattamento dei dati personali solo per parti specifiche della ricerca.

(20) Infine, la legge sull'accesso ai dati e sul loro utilizzo ha ulteriormente precisato le garanzie precedentemente contenute nell'articolo 89 del GDPR del Regno Unito e nella sezione 19 della legge del 2018 sulla protezione dei dati per quanto riguarda il trattamento dei dati a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in un nuovo capo 8 A del GDPR del Regno Unito ([27]). Tali garanzie sono simili a quelle imposte all'articolo 89 del regolamento (UE) 2016/679 e comprendono l'obbligo di predisporre misure tecniche e organizzative al fine di garantire il rispetto del principio della minimizzazione dei dati.

2.2. **Garanzie, diritti e obblighi**

2.2.1. *Liceità e correttezza del trattamento*

(21) Il quadro in materia di protezione dei dati del Regno Unito continua ad esigere che i dati siano trattati in modo lecito, corretto e legittimo, come valutato nei considerando da 24 a 26 della decisione di esecuzione (UE) 2021/1772.

([27]) Articoli da 84 A a 84D del GDPR del Regno Unito, introdotti dalla sezione 86 della legge sull'accesso ai dati e sul loro utilizzo.

(22) I principi di liceità e correttezza e le basi per il trattamento lecito continuano ad essere garantiti nel diritto del Regno Unito attraverso l'articolo 5, paragrafo 1, lettera a), e l'articolo 6, paragrafo 1, del GDPR del Regno Unito, come valutato nella decisione di esecuzione (UE) 2021/1772. Sebbene tali disposizioni restino in gran parte identiche ([28]) alle rispettive disposizioni del regolamento (UE) 2016/679, la legge sull'accesso ai dati e sul loro utilizzo modifica innanzitutto l'articolo 6, paragrafo 1, del GDPR del Regno Unito introducendo un ulteriore motivo lecito per il trattamento dei dati personali a norma dell'articolo 6, paragrafo 1, lettera ea) ([29]). Secondo tale disposizione, il trattamento è lecito se e nella misura in cui «è necessario per il perseguimento di un interesse legittimo riconosciuto». A differenza del motivo giuridico di legittimo interesse a norma dell'articolo 6, paragrafo 1, lettera f), del GDPR del Regno Unito, la nuova base giuridica del legittimo interesse riconosciuto non impone un equilibrio, caso per caso, tra legittimo interesse del titolare del trattamento e gli interessi o i diritti e le libertà fondamentali dell'interessato, con l'obiettivo di garantire una maggiore certezza del diritto ai titolari del trattamento diversi dagli organismi pubblici. Il nuovo articolo 6, paragrafo 5, del GDPR del Regno Unito specifica che il trattamento è necessario per il perseguimento di un interesse legittimo riconosciuto solo se soddisfa una condizione di cui all'allegato 1 ([30]), che elenca poi le situazioni in cui il trattamento è considerato necessario per il perseguimento di un interesse legittimo riconosciuto: ad esempio, quando ha luogo in risposta a una richiesta ricevuta da un'autorità pubblica che necessita dei dati per eseguire un compito di interesse pubblico la cui base giuridica è conforme all'articolo 6, paragrafo 3, del GDPR del Regno Unito, qualora il trattamento sia necessario per garantire la sicurezza nazionale, proteggere la sicurezza pubblica o per finalità di difesa, per rispondere a un'emergenza, accertare, indagare o prevenire reati o tutelare le persone vulnerabili ([31]).

(23) Mentre la legge sull'accesso ai dati e sul loro utilizzo amplia l'elenco delle basi giuridiche per il trattamento dei dati personali a disposizione del titolare del trattamento, la nuova base giuridica per il legittimo interesse riconosciuto è sottoposta a diverse importanti limitazioni. In primo luogo, il legittimo interesse riconosciuto è limitato a situazioni specifiche dettagliatamente elencate nella legge. In secondo luogo, tale fondamento giuridico non può essere invocato dalle autorità pubbliche nell'adempimento dei loro compiti ([32]). In terzo luogo, riguarda solo i settori in cui esiste un evidente pubblico interesse dell'attività di trattamento (in base alle condizioni di cui all'allegato 1), ossia quando il trattamento persegue gli obiettivi elencati all'articolo 23 del GDPR del Regno Unito [che corrisponde all'articolo 23 del regolamento (UE) 2016/679] e non può pertanto essere invocato a fini commerciali. In quarto luogo, se da un lato la legge sull'accesso ai dati e sul loro utilizzo conferisce al segretario di Stato la facoltà

([28]) Per chiarezza, la legge sull'accesso ai dati e sul loro utilizzo introduce nell'articolo 6 del GDPR del Regno Unito anche un nuovo paragrafo che fornisce esempi di tipi di trattamento che possono essere considerati necessari per il perseguimento di un interesse legittimo ai sensi dell'articolo 6, paragrafo 1, lettera f), del GDPR del Regno Unito. Questi esempi (marketing diretto, trasmissione all'interno del gruppo imprenditoriale di dati a fini amministrativi, sicurezza delle reti e dei sistemi informativi) sono menzionati anche nei considerando 47 e 48 del regolamento (UE) 2016/679 come situazioni in cui il trattamento sarebbe considerato nel legittimo interesse del titolare del trattamento.

([29]) Sezione 70, paragrafo 2, lettera b), della legge sull'accesso ai dati e sul loro utilizzo. La sezione 70, paragrafo 5, della legge sull'accesso ai dati e sul loro utilizzo ha esteso il diritto di opposizione, di cui all'articolo 21 del GDPR del Regno Unito, al nuovo articolo 6, paragrafo 1, lettera ea), del GDPR del Regno Unito.

([30]) Sezione 70, paragrafo 4, della legge sull'accesso ai dati e sul loro utilizzo.

([31]) Cfr. allegato 4 della legge sull'accesso ai dati e sul loro utilizzo. Secondo le autorità britanniche, tra le situazioni in cui gli organismi non pubblici possono dover trattare dati personali per prevenire o accertare reati figurano, ad esempio, il caso di una società che venga a conoscenza di tentativi di pirateria illecita a danno dei suoi sistemi informatici, o di una banca o un'istituzione finanziaria che riscontri tentativi fraudolenti di aprire un conto. Il trattamento di dati personali da parte di un organismo non pubblico può essere necessario, ad esempio, per salvaguardare la sicurezza nazionale o a fini di difesa qualora un'organizzazione commerciale sospetti che l'attività online di un cliente riveli la partecipazione ad attività terroristiche. L'ICO sta elaborando orientamenti specifici in materia, compresa una definizione dei concetti pertinenti. Ad esempio, il concetto di «sicurezza nazionale» potrebbe riguardare la sicurezza e il benessere del Regno Unito nel suo complesso, della sua popolazione, delle sue istituzioni e del suo sistema di governo. Cfr. il progetto di orientamenti dell'ICO sul legittimo interesse riconosciuto, pubblicato per la consultazione pubblica, disponibile al seguente indirizzo: https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/.

([32]) Articolo 6, paragrafo 1, ultimo comma, come modificato dalla sezione 70, paragrafo 2, lettera c), della legge sull'accesso ai dati e sul loro utilizzo.

di modificare l'elenco di cui all'allegato 1 mediante regolamento ([33]), dall'altro il segretario di Stato può adottare tale regolamento solo dopo aver sentito l'ICO ([34]) e aggiungere all'elenco un legittimo interesse riconosciuto solo se il trattamento è necessario per salvaguardare uno degli obiettivi di pubblico interesse elencati all'articolo 23, paragrafo 1, lettere da c) a j), del GDPR del Regno Unito ([35]). Infine, come confermato anche dagli orientamenti dell'ICO ([36]), i titolari del trattamento che invocano un legittimo interesse riconosciuto come base giuridica sono tenuti a rispettare tutti gli altri obblighi previsti dal GDPR del Regno Unito, compresa la garanzia che il trattamento sia necessario e proporzionato per conseguire il legittimo interesse.

(24) In secondo luogo, la legge sull'accesso ai dati e sul loro utilizzo chiarisce all'articolo 6, paragrafo 3, all'articolo 9, paragrafo 2, lettera g), e all'articolo 10, paragrafo 1, del GDPR del Regno Unito, corrispondenti alle rispettive disposizioni del regolamento (UE) 2016/679, che la base per il trattamento dei dati personali, delle categorie particolari di dati personali e dei dati personali relativi a condanne penali e reati in conformità di un obbligo legale o per l'esecuzione di un compito di interesse pubblico può essere fondata non solo sul diritto interno, ma anche sul pertinente diritto internazionale ([37]). Il diritto internazionale pertinente è poi limitato dal nuovo articolo 9 A del GDPR del Regno Unito, in combinato disposto con l'allegato A1, a un unico accordo, ossia l'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 (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), firmato il 3 ottobre 2019 (accordo UK-USA) ([38]). Le garanzie previste da tale accordo sono state valutate nei considerando da 153 a 155 della decisione di esecuzione (UE) 2021/1772 e la loro applicazione è esaminata ai considerando da 87 a 93 della medesima decisione.

2.2.2. *Trattamento di categorie particolari di dati personali*

(25) Il quadro in materia di protezione dei dati del Regno Unito continua a fornire garanzie specifiche per quanto riguarda categorie particolari di dati, come valutato nei considerando da 27 a 42 della decisione di esecuzione (UE) 2021/1772.

(26) Restano in vigore sia la definizione di categorie particolari di dati personali, sia le norme specifiche applicabili al trattamento di tali categorie di dati di cui al GDPR del Regno Unito e alla legge del 2018 sulla protezione dei dati. Al contempo la legge sull'accesso ai dati e sul loro utilizzo conferisce nuovi poteri normativi al segretario di Stato, il quale, se necessario, può aggiungere categorie particolari di dati, adattare le condizioni applicabili al loro utilizzo e aggiungere nuove definizioni ([39]). È importante sottolineare che tale potere non consente al segretario di Stato di sopprimere o modificare le categorie particolari di dati esistenti, né di modificarne le condizioni di trattamento ([40]). Il nuovo potere normativo consente quindi al governo solo di aggiungere nuove categorie di dati sensibili e di determinare le condizioni per il trattamento di tali categorie, permettendo al governo di rispondere, ove necessario, ai futuri sviluppi tecnologici e sociali.

(27) Tali modifiche pertanto non incidono sul livello di protezione delle categorie particolari di dati personali ritenuto, nella decisione di esecuzione (UE) 2021/1772, sostanzialmente equivalente alla protezione all'interno dell'UE.

([33]) Prima di emanare regolamenti, il segretario di Stato deve tenere conto degli effetti di eventuali modifiche sugli interessi, i diritti e le libertà fondamentali degli interessati, come anche del fatto che i dati personali dei minori (se del caso) godono di una protezione specifica. I regolamenti devono essere stabiliti per legge e sono soggetti all'approvazione espressa (*affirmative resolution procedure*), il che significa che devono essere approvati dal parlamento del Regno Unito. Sezione 70, paragrafo 4, comma 8, della legge sull'accesso ai dati e sul loro utilizzo.

([34]) Sezione 182, paragrafo 2, della legge del 2018 sulla protezione dei dati.

([35]) Sezione 70, paragrafo 4, comma 9, della legge sull'accesso ai dati e sul loro utilizzo.

([36]) Cfr. gli orientamenti dell'ICO sugli interessi legittimi, disponibili al seguente indirizzo: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/?q=appropriate+policy.

([37]) Sezione 72 della legge sull'accesso ai dati e sul loro utilizzo.

([38]) 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, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

([39]) Sezione 74 della legge sull'accesso ai dati e sul loro utilizzo. Tali regolamenti sono soggetti all'approvazione espressa (*affirmative resolution procedure*) del parlamento del Regno Unito.

([40]) Cfr. il nuovo articolo 11 A, paragrafo 1, lettera b), e paragrafo 2, del GDPR del Regno Unito, nonché le note esplicative del disegno di legge sull'accesso ai dati e sul loro utilizzo, paragrafo 571, disponibili al seguente indirizzo: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

2.2.3. *Limitazione delle finalità*

(28) Il regime del Regno Unito in materia di protezione dei dati personali continua ad esigere che i dati siano trattati per una finalità specifica e successivamente utilizzati solo nella misura in cui ciò non sia incompatibile con la finalità originaria del trattamento, come valutato nei considerando da 43 a 48 della decisione di esecuzione (UE) 2021/1772.

(29) In primo luogo, la legge sull'accesso ai dati e sul loro utilizzo apporta alcune modifiche specifiche al principio di limitazione delle finalità di cui all'articolo 5, paragrafo 1, lettera b), del GDPR del Regno Unito. Le modifiche chiariscono l'applicazione di tale principio senza modificarne la sostanza. La sezione 71, paragrafi 1, 2 e 3, della legge sull'accesso ai dati e sul loro utilizzo specifica che il principio di limitazione delle finalità si applica laddove i dati siano raccolti presso l'interessato o in altro modo, che tale principio si applica solo quando i dati personali sono ulteriormente trattati dallo stesso titolare del trattamento o per suo conto (ossia non si applica se il titolare del trattamento cambia) e che la liceità del trattamento non dipende solo dalla compatibilità con le finalità per le quali i dati personali sono stati raccolti.

(30) In secondo luogo, la legge sull'accesso ai dati e sul loro utilizzo chiarisce le norme relative all'ulteriore trattamento dei dati personali raggruppandole nel nuovo articolo 8 A, aggiunto al GDPR del Regno Unito, che stabilisce il regime completo per l'ulteriore trattamento dei dati personali. L'articolo 8 A, paragrafo 2, del GDPR del Regno Unito elenca gli elementi da considerare nel determinare se una nuova finalità di trattamento sia compatibile con la finalità originaria. Tali elementi erano precedentemente elencati all'articolo 6, paragrafo 4, del GDPR del Regno Unito, che corrisponde all'articolo 6, paragrafo 4, del regolamento (UE) 2016/679 ([41]). L'articolo 8 A, paragrafo 3, del GDPR del Regno Unito raggruppa in un'unica disposizione le situazioni in cui il trattamento dei dati personali per una nuova finalità deve essere considerato compatibile con la finalità originaria. L'articolo riguarda le situazioni in cui l'interessato acconsente al trattamento dei dati personali per la nuova finalità o in cui il trattamento è necessario per salvaguardare uno degli obiettivi di cui all'articolo 23, paragrafo 1 ([42]), o in cui il trattamento è effettuato per finalità di ricerca scientifica o storica, archiviazione nel pubblico interesse o a fini statistici ([43]). In ultimo luogo, la legge sull'accesso ai dati e sul loro utilizzo chiarisce che qualsiasi trattamento effettuato per garantire che il trattamento sia conforme ai principi di protezione dei dati di cui all'articolo 5, paragrafo 1, del GDPR del Regno Unito, o che lo dimostri, è considerato compatibile con la finalità originaria. Le situazioni succitate continuano a corrispondere a quanto ritenuto un ulteriore trattamento compatibile dal regolamento (UE) 2016/679.

(31) In terzo luogo, la legge sull'accesso ai dati e sul loro utilizzo introduce, all'articolo 8 A, paragrafo 3, lettera d), del GDPR del Regno Unito, altre nuove situazioni in cui l'ulteriore trattamento dei dati personali per una nuova finalità è considerato compatibile con la finalità originaria. Tali situazioni sono elencate nell'allegato 2 del GDPR del Regno Unito ([44]) e comprendono, ad esempio, il trattamento effettuato in risposta a una richiesta di un'autorità pubblica che necessita dei dati ai fini dell'esecuzione di un compito di interesse pubblico la cui base giuridica è conforme all'articolo 6, paragrafo 3, del GDPR del Regno Unito, il trattamento necessario per tutelare la sicurezza pubblica, rispondere a un'emergenza, accertare, indagare o prevenire reati, tutelare gli interessi vitali dell'interessato e di altri soggetti, tutelare le persone vulnerabili, a fini fiscali o se necessario per adempiere un obbligo legale ([45]).

(32) Sebbene la legge sull'accesso ai dati e sul loro utilizzo ampli l'elenco delle situazioni in cui l'ulteriore trattamento per una finalità diversa è considerato compatibile con la finalità originaria del trattamento, tale ampliamento è sottoposto a importanti limitazioni. In primo luogo, è limitato a situazioni specifiche dettagliatamente elencate nella legge. In secondo luogo, riguarda solo i settori in cui esiste un evidente pubblico interesse dell'attività di trattamento, ossia in cui l'ulteriore trattamento persegue gli obiettivi elencati all'articolo 23 del GDPR del Regno

([41]) Come nel regolamento (UE) 2016/679, tra tali elementi figurano i legami di qualunque natura tra la finalità originaria e quella nuova, il contesto in cui i dati personali sono stati raccolti, compresi il rapporto tra l'interessato e il titolare del trattamento, la natura del trattamento e l'eventuale presenza di categorie particolari di dati, le possibili conseguenze per l'interessato del trattamento previsto e l'esistenza di garanzie adeguate.

([42]) Cfr. l'articolo 6, paragrafo 4, del regolamento (UE) 2016/679.

([43]) Considerando 50 del regolamento (UE) 2016/679.

([44]) L'allegato 2 è introdotto nel GDPR del Regno Unito mediante l'allegato 5 della legge sull'accesso ai dati e sul loro utilizzo, sezione 71, paragrafo 6.

([45]) Cfr. allegato 5 della legge sull'accesso ai dati e sul loro utilizzo.

Unito [che corrisponde all'articolo 23 del regolamento (UE) 2016/679]. Non può quindi essere invocato a fini commerciali. In terzo luogo, se da un lato la legge sull'accesso ai dati e sul loro utilizzo conferisce al segretario di Stato la facoltà di modificare l'elenco di cui all'allegato 2 mediante regolamento ([46]), dall'altro il segretario di Stato può aggiungere all'elenco nuovi tipi di trattamento solo laddove il trattamento sia necessario per salvaguardare uno degli obiettivi di pubblico interesse elencati all'articolo 23, paragrafo 1, lettere da c) a j), del GDPR del Regno Unito ([47]). In quarto luogo, quando la raccolta di dati personali da parte del titolare del trattamento si basa sul consenso dell'interessato, il trattamento per una nuova finalità nelle situazioni elencate nell'allegato 2 è considerato compatibile con la finalità originaria solo qualora non si possa ragionevolmente prevedere che il titolare del trattamento ottenga un nuovo consenso dall'interessato ([48]).

2.2.4. *Diritti delle persone fisiche*

(33) Nel quadro del Regno Unito in materia di protezione dei dati personali, gli interessati continuano a godere degli stessi diritti individuali di cui al regolamento (UE) 2016/679, senza modifiche significative ([49]), azionabili nei confronti del titolare del trattamento o del responsabile del trattamento, in particolare il diritto di accesso ai dati, il diritto di opporsi al trattamento e il diritto di far rettificare e cancellare i dati, come previsto dai considerando da 51 a 54 della decisione di esecuzione (UE) 2021/1772.

(34) In primo luogo, la legge sull'accesso ai dati e sul loro utilizzo chiarisce determinate modalità in base alle quali tali diritti possono essere esercitati. Da un lato, mediante la modifica dell'articolo 12 e l'introduzione nel GDPR del Regno Unito di un nuovo articolo 12 A ([50]), specifica i termini entro i quali i titolari del trattamento devono rispondere alla richiesta dell'interessato. Più specificamente, con la modifica dell'articolo 12 del GDPR del Regno Unito il titolare del trattamento è tenuto a fornire informazioni sull'azione intrapresa (o sui motivi per cui non ha intrapreso un'azione) in risposta a una richiesta dell'interessato a norma degli articoli da 15 a 22 del GDPR del Regno Unito non più «entro un mese dal ricevimento della richiesta», bensì «prima della scadenza del termine applicabile». Il termine applicabile è ulteriormente definito nel nuovo articolo 12 A del GDPR del Regno Unito come il periodo di un mese a decorrere dal momento rilevante, ossia il momento in cui il titolare del trattamento riceve la richiesta o le informazioni in relazione a una richiesta a norma dell'articolo 12, paragrafo 6, del GDPR del Regno Unito, oppure il momento in cui sono stati pagati i diritti addebitati in relazione alla richiesta a norma dell'articolo 12, paragrafo 5, del GDPR del Regno Unito, a seconda di quale sia l'evento più recente ([51]). L'articolo 12 A, paragrafo 3, consente inoltre al titolare del trattamento di prorogare il termine applicabile di altri due mesi qualora ciò sia necessario a causa della complessità delle richieste presentate dall'interessato o del numero di tali richieste. Dall'altro lato, per quanto riguarda solo il diritto di accesso alle informazioni e ai dati personali, la legge sull'accesso ai dati e sul loro utilizzo modifica l'articolo 15 del GDPR del Regno Unito per integrare il chiarimento elaborato nell'ambito della giurisprudenza nazionale esistente (sulla base del principio di proporzionalità previsto dal diritto dell'UE) secondo cui i titolari del trattamento sono tenuti soltanto ad effettuare ricerche ragionevoli e proporzionate riguardo alle informazioni e ai dati personali richiesti ([52]). La nuova disposizione dovrebbe essere interpretata in linea con la giurisprudenza esistente, secondo la quale «[…] ciò che viene ponderato nell'esercizio di proporzionalità è l'oggetto finale della ricerca, vale a dire il potenziale vantaggio che la fornitura delle informazioni potrebbe apportare all'interessato, rispetto ai mezzi con cui tali informazioni sono ottenute. Occorre valutare in ogni singolo caso se saranno necessari sforzi sproporzionati per reperire e fornire le informazioni rispetto ai benefici che questo potrebbe apportare all'interessato» ([53]).

([46]) Articolo 8 A, paragrafo 5, del GDPR del Regno Unito, introdotto dalla sezione 71, paragrafo 1, della legge sull'accesso ai dati e sul loro utilizzo.

([47]) Articolo 8 A, paragrafo 6, del GDPR del Regno Unito, introdotto dalla sezione 71, paragrafo 1, della legge sull'accesso ai dati e sul loro utilizzo.

([48]) Articolo 8 A, paragrafo 4, lettera b), del GDPR del Regno Unito, introdotto dalla sezione 71, paragrafo 1, della legge sull'accesso ai dati e sul loro utilizzo.

([49]) La sezione 31 della legge del 2024 sulle vittime e i detenuti ha aggiunto un ulteriore motivo per il diritto di cancellare i dati di cui all'articolo 17 del GDPR del Regno Unito, riconoscendo agli interessati il diritto di chiedere ai titolari del trattamento di cancellare i loro dati personali quando siano stati trattati a seguito di un'accusa infondata nei loro confronti formulata da una persona in malafede. Una persona è considerata «in malafede» se è stata condannata per un reato di cui alla sezione 31, paragrafo 3, della legge del 2024 sulle vittime e i detenuti (ad esempio per molestie) o è soggetta a un ordine di protezione contro molestie persecutorie. La legge del 2024 sulle vittime e i detenuti è disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2024/21/contents. La sezione 77 della legge sull'accesso ai dati e sul loro utilizzo modifica inoltre il diritto all'informazione di cui all'articolo 13 del GDPR del Regno Unito per cui il titolare del trattamento non è più tenuto a informare l'interessato in merito all'ulteriore trattamento dei suoi dati personali per una nuova finalità se si tratta di ricerca scientifica o storica, archiviazione nel pubblico interesse o a fini statistici, se il trattamento è effettuato conformemente alle garanzie specifiche di cui al nuovo articolo 84B del GDPR del Regno Unito e se l'informazione è impossibile o sproporzionata.

([50]) Sezione 76 della legge sull'accesso ai dati e sul loro utilizzo.

([51]) Articolo 12 A, paragrafi 1 e 2, del GDPR del Regno Unito, introdotto dalla sezione 76 della legge sull'accesso ai dati e sul loro utilizzo.

([52]) Articolo 15, paragrafo 1 A, del GDPR del Regno Unito, introdotto dalla sezione 78 della legge sull'accesso ai dati e sul loro utilizzo.

([53]) *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74.

(35) Pertanto, sebbene i termini per rispondere alle richieste degli interessati e gli obblighi specifici dei titolari del trattamento in relazione al diritto di accesso siano soggetti a norme più dettagliate, il sistema del Regno Unito continua a garantire che le richieste degli interessati siano trattate entro termini ragionevoli definiti sulla base di fattori oggettivi. Inoltre, gli obblighi sostanziali di risposta alle richieste di accesso incombenti al titolare del trattamento sono definiti sulla base di norme giuridiche consolidate che tengono conto anche degli interessi dell'interessato. Infine, gli attuali orientamenti dell'ICO già prevedono che un titolare del trattamento non sia tenuto a effettuare ricerche che sarebbero irragionevoli o sproporzionate rispetto all'importanza di fornire l'accesso alle informazioni ([54]).

(36) Le limitazioni a tali diritti individuali stabilite nella legge del 2018 sulla protezione dei dati e che rientrano nel quadro dell'articolo 23 del GDPR del Regno Unito, come pure le limitazioni e le garanzie che ne disciplinano l'applicazione, continuano a essere in vigore nel quadro del Regno Unito ([55]), come descritto in dettaglio nei considerando da 55 a 67 della decisione di esecuzione (UE) 2021/1772.

(37) Per quanto riguarda specificamente la limitazione dei dati personali trattati a fini di mantenimento dell'effettivo controllo dell'immigrazione, o di indagine o accertamento di attività che comprometterebbero il mantenimento dell'effettivo controllo dell'immigrazione, nella misura in cui l'applicazione di tali disposizioni potrebbe pregiudicare tale mantenimento (esenzione per motivi di immigrazione) ([56]), il governo del Regno Unito ha modificato il paragrafo 4 dell'allegato 2 della legge del 2018 sulla protezione dei dati mediante i regolamenti del 2022 sulla legge del 2018 sulla protezione dei dati (modifica dell'allegato 2 Esenzioni) ([57]), e i regolamenti del 2024 sulla legge del 2018 sulla protezione dei dati (modifica dell'allegato 2 Esenzioni) ([58]) che integra i regolamenti del 2022 ([59]). Le modifiche aggiungono ai paragrafi 4 A e 4B dell'allegato 2 della legge del 2018 sulla protezione dei dati le garanzie per l'esercizio dell'esenzione per motivi di immigrazione imposte dall'articolo 23, paragrafo 2, del GDPR del Regno Unito. In particolare, esigono i) che l'esenzione per motivi di immigrazione possa essere invocata solo caso per caso, separatamente rispetto a ciascuna delle pertinenti disposizioni del GDPR del Regno Unito e, di nuovo, ogniqualvolta il segretario di Stato ritenga di non applicare o limitare l'applicazione di una delle pertinenti disposizioni del GDPR del Regno Unito ([60]), ii) che nell'esercizio dell'esenzione per motivi di immigrazione siano presi in considerazione i diritti, le libertà e le potenziali vulnerabilità dell'interessato ([61]), iii) che il segretario di Stato conservi un registro sull'uso dell'esenzione per motivi di immigrazione e informi l'interessato in merito al suo utilizzo (tranne in specifiche circostanze in cui l'informazione pregiudicherebbe l'obiettivo dell'esenzione) ([62]) e iv) che sia chiaro che l'uso dell'esenzione per motivi di immigrazione è limitato al trattamento dei dati personali da parte del segretario di Stato ([63]) ossia, nella pratica, da parte del ministero degli Interni per le sue funzioni di cui al paragrafo 4, punto 1, dell'allegato 2 della legge del 2018 sulla protezione dei dati. Le modifiche spiegano inoltre che, nel determinare se l'esercizio dei diritti degli interessati possa pregiudicare l'effettivo controllo dell'immigrazione e se sia necessario e proporzionato limitare di conseguenza tali diritti, occorre far prova di equilibrio.

([54]) Disponibili al seguente indirizzo: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/.

([55]) La sezione 88, paragrafo 2, della legge sull'accesso ai dati e sul loro utilizzo apporta una piccola modifica alla sezione 26, paragrafo 2, lettera f), della legge del 2018 sulla protezione dei dati (esenzione per motivi di sicurezza nazionale e difesa), chiarendo che il diritto di presentare un reclamo al Commissioner a norma dell'articolo 77 del GDPR del Regno Unito non rientra nelle disposizioni la cui applicazione può essere limitata a fini di sicurezza nazionale o difesa.

([56]) Al momento dell'adozione della decisione di esecuzione (UE) 2021/1772, la validità e l'interpretazione dell'esenzione per motivi di immigrazione a norma del diritto del Regno Unito erano controverse a causa di una decisione della Corte d'appello dell'Inghilterra e del Galles del 26 maggio 2021 secondo la quale l'esenzione per motivi di immigrazione, quale prevista all'epoca nella legge del 2018 sulla protezione dei dati, era incompatibile con il diritto del Regno Unito, in quanto mancava di disposizioni specifiche che definissero le garanzie di cui all'articolo 23, paragrafo 2, del GDPR del Regno Unito corrispondente all'articolo 23, paragrafo 2, del regolamento (UE) 2016/679. Per tale motivo, i dati personali trasferiti a fini di controllo dell'immigrazione nel Regno Unito o che altrimenti rientrano nell'ambito di applicazione dell'esenzione per motivi di immigrazione erano stati esclusi dall'ambito di applicazione della decisione di esecuzione (UE) 2021/1772.

([57]) I regolamenti sono entrati in vigore il 31 gennaio 2022 e sono disponibili al seguente indirizzo: https://www.legislation.gov.uk/uksi/2022/76/contents/made.

([58]) I regolamenti sono entrati in vigore l'8 marzo 2024 e sono disponibili al seguente indirizzo: https://www.legislation.gov.uk/uksi/2024/342/contents/made.

([59]) L'esenzione per motivi di immigrazione, come riveduta mediante i regolamenti del 2022, è stata nuovamente contestata mediante controllo giurisdizionale, sulla base del fatto che non soddisfaceva ancora tutte le disposizioni dell'articolo 23, paragrafo 2, del GDPR del Regno Unito. Nel dicembre 2023 la Corte d'appello dell'Inghilterra e del Galles l'ha ritenuta incompatibile con le disposizioni dell'articolo 23, paragrafo 2, del GDPR del Regno Unito. I regolamenti del 2024 integrano, come conseguenza della suddetta sentenza, i regolamenti del 2022 e modificano ulteriormente l'esenzione per motivi di immigrazione.

([60]) Paragrafo 4 A, punto 2, dell'allegato 2 della legge del 2018 sulla protezione dei dati.

([61]) Paragrafo 4AB, punti 3 e 4, dell'allegato 2 della legge del 2018 sulla protezione dei dati. L'ICO, consultato in merito al progetto di regolamenti del 2024, ha dichiarato pubblicamente di essere soddisfatto della normativa. La lettera pubblicata in risposta alla consultazione, che conferma il parere dell'ICO, è disponibile al seguente indirizzo: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-responds-to-home-office-s-draft-regulations-to-the-immigration-exemption/.

([62]) Paragrafo 4B, punti 1 e 2, dell'allegato 2 della legge del 2018 sulla protezione dei dati.

([63]) Paragrafo 4, punto 1, dell'allegato 2 della legge del 2018 sulla protezione dei dati.

(38) L'ICO ha inoltre pubblicato orientamenti dettagliati sull'uso di questa limitazione specifica ([64]). Tali orientamenti in particolare affermano che l'esenzione per motivi di immigrazione non dovrebbe essere un'esenzione generalizzata per limitare i diritti relativi a tutti i dati in possesso di un'organizzazione. L'ambito di applicazione dell'esenzione è limitato ai diritti che, se esercitati per i dati detenuti, pregiudicherebbero le finalità specificate in materia di immigrazione. […]. Pertanto il titolare del trattamento dovrebbe di base rispettare, per quanto possibile, le disposizioni del regolamento (UE) 2016/679 e della legge del 2018 sulla protezione dei dati. La verifica del pregiudizio ha una soglia elevata e l'esenzione non dovrebbe essere applicata in modo generalizzato. Occorre valutare se l'applicazione dell'esenzione costituisca una risposta proporzionata alla richiesta di protezione dei dati della persona fisica. È possibile ritenere che l'applicazione dell'esenzione per motivi di immigrazione risponda a un'urgente necessità sociale, ma occorre anche considerare se ciò prevalga sugli obblighi nei confronti delle persone fisiche previsti dal regolamento (UE) 2016/679. Tali persone godono di diritti relativi ai loro dati personali che devono essere presi in considerazione in ogni circostanza, in particolare il diritto di accesso. È quindi importante valutare in ciascun caso se i diritti di protezione dei dati di una persona fisica prevalgono sul rischio di pregiudizio individuato. L'applicazione dell'esenzione deve essere proporzionata alle circostanze e deve essere attentamente esaminata e documentata in ciascun caso.

(39) Nel complesso, la limitazione relativa all'immigrazione di cui al paragrafo 4 dell'allegato 2 della legge del 2018 sulla protezione dei dati, come riveduta dal governo del Regno Unito nel 2022 e nel 2024 e interpretata dalla giurisprudenza ([65]) e dagli orientamenti dell'ICO, è soggetta a una serie di condizioni rigorose che ne disciplinano l'applicazione, molto simili a quelle stabilite dal diritto dell'Unione, in particolare dall'articolo 23 del regolamento (UE) 2016/679, per la limitazione dei diritti e degli obblighi in materia di protezione dei dati per importanti obiettivi di interesse pubblico, come il controllo dell'immigrazione.

2.2.5. *Limitazioni ai trasferimenti successivi*

(40) Il livello di protezione offerto ai dati personali trasferiti dall'Unione europea verso titolari del trattamento o responsabili del trattamento nel Regno Unito continua a non essere compromesso da ulteriori trasferimenti di tali dati a destinatari che si trovano in un paese terzo. Il regime in materia di trasferimenti internazionali di dati personali dal Regno Unito rimane molto simile alle norme di cui al capo V del regolamento (UE) 2016/679, come valutato nei considerando da 74 a 82 della decisione di esecuzione (UE) 2021/1772.

(41) Sebbene la legge sull'accesso ai dati e sul loro utilizzo abbia modificato il capo 5 del GDPR del Regno Unito relativo ai trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali, essa mantiene la disposizione centrale secondo cui i dati personali possono essere trasferiti a un paese terzo o a un'organizzazione internazionale solo se il trasferimento si basa su: i) regolamenti che approvano il trasferimento (nuova terminologia per ciò che in precedenza era indicato come «regolamenti di adeguatezza»), ii) garanzie adeguate o iii) una deroga per situazioni specifiche. Tali principi generali alla base dei trasferimenti di dati sono ripresi all'articolo 44 A che sostituisce l'articolo 44 del GDPR del Regno Unito ([66]), il quale specifica, tra l'altro, che i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale sono consentiti solo se il trasferimento è effettuato in conformità delle altre disposizioni del GDPR del Regno Unito.

(42) Per quanto riguarda specificamente i regolamenti che approvano un trasferimento, l'articolo 45 A, paragrafo 2, del GDPR del Regno Unito precisa che il segretario di Stato può adottare tali regolamenti solo se ritiene che la verifica della protezione dei dati sia soddisfatta. Ciò significa che la possibilità per il segretario di Stato, introdotta nell'articolo 45 A, paragrafo 3, del GDPR del Regno Unito, di tenere conto dell'opportunità di agevolare i flussi di dati nell'elaborazione di tali regolamenti è sempre subordinata al soddisfacimento della verifica della protezione dei dati. Il criterio giuridico per la verifica della protezione dei dati da soddisfare è enunciato nel nuovo articolo 45B, paragrafo 1, del GDPR del Regno Unito, che impone che il livello di protezione degli interessati nei paesi o nelle organizzazioni internazionali destinatari non sia sostanzialmente inferiore a quello previsto dalla pertinente legislazione del Regno Unito in materia di protezione dei dati. L'articolo 45B, paragrafo 2, del GDPR del Regno Unito fornisce un elenco non esaustivo di elementi da considerare nel valutare se tale verifica è soddisfatta, quali il rispetto dello Stato di diritto e dei diritti umani, la presenza di un'autorità di protezione dei dati e le sue competenze, le modalità di ricorso giurisdizionale o extragiudiziale, le norme sul trasferimento di dati personali dal

([64]) Disponibili al seguente indirizzo: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/immigration-exemption-a-guide/.

([65]) *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor* [2019] EWHC (England and Wales High Court, Alta Corte di Inghilterra e Galles) 2562 (Admin), punti 40 e 41.

([66]) Sezione 85 e allegato 7 della legge sull'accesso ai dati e sul loro utilizzo.

paese o dall'organizzazione ad altri paesi o organizzazioni internazionali, i pertinenti obblighi internazionali del paese o dell'organizzazione e la costituzione, le tradizioni e la cultura del paese o dell'organizzazione. Nel riformulare l'elenco degli elementi pertinenti di cui al previgente articolo 45 del GDPR del Regno Unito, il nuovo articolo 45B, paragrafo 2, mantiene gli elementi centrali di tale elenco e rimane pertanto simile alle disposizioni del capo V del regolamento (UE) 2016/679. Le autorità del Regno Unito hanno inoltre confermato che il segretario di Stato terrà conto di elementi non previsti all'articolo 45B, paragrafo 2, quali le leggi e le prassi di un paese terzo relative al modo in cui le autorità pubbliche accedono ai dati personali per finalità quali la sicurezza nazionale o l'applicazione della legge, nella misura in cui queste incidono sul livello generale di protezione. Inoltre le autorità del Regno Unito ritengono che la giurisprudenza pertinente del paese terzo sarà una componente essenziale in sede di considerazione delle questioni elencate in modo non esaustivo all'articolo 45B, paragrafo 2, del GDPR del Regno Unito.

(43) I regolamenti che approvano un trasferimento continuano a essere soggetti ai requisiti procedurali «generali» previsti dalla sezione 182 della legge del 2018 sulla protezione dei dati, come indicato al considerando 77 della decisione di esecuzione (UE) 2021/1772. Secondo tale procedura, quando propone futuri regolamenti di adeguatezza del Regno Unito il segretario di Stato deve consultare l'Information Commissioner ([67]). Una volta adottati dal segretario di Stato, tali regolamenti sono presentati al parlamento e sottoposti alla procedura di «risoluzione negativa» nel contesto della quale entrambe le camere del parlamento possono esaminare i regolamenti e hanno la facoltà di presentare una mozione di annullamento dei regolamenti stessi entro un termine di 40 giorni ([68]).

(44) Per quanto riguarda le garanzie adeguate, il nuovo articolo 46, paragrafo 1 A, del GDPR del Regno Unito stabilisce che tali trasferimenti possono essere effettuati solo se negli strumenti disponibili a norma dell'articolo 46, paragrafi 2 e 3, del GDPR del Regno Unito ([69]) sono previste garanzie pertinenti e se il titolare del trattamento, il responsabile del trattamento o gli organismi pubblici competenti ritengono, agendo in modo ragionevole e proporzionato, che la verifica della protezione dei dati sia soddisfatta. I nuovi paragrafi 6 e 7 chiariscono che la verifica della protezione dei dati è soddisfatta se, grazie alle garanzie imposte, il previsto livello di protezione degli interessati non è sostanzialmente inferiore a quello previsto dalla pertinente legislazione del Regno Unito in materia di protezione dei dati, vale a dire, come nel caso del regolamento (UE) 2016/679, si applicano gli stessi criteri giuridici sia ai regolamenti che approvano il trasferimento sia alle garanzie adeguate. A norma del medesimo paragrafo, ciò che è ragionevole e proporzionato deve essere determinato con riferimento a tutte le circostanze, o alle circostanze probabili, del trasferimento o del tipo di trasferimento, compresi la natura e il volume dei dati personali trasferiti.

(45) Per quanto riguarda le deroghe in situazioni specifiche, nell'articolo 49 del GDPR del Regno Unito relativo alle condizioni in base alle quali, in situazioni specifiche, è possibile applicare una deroga, sono state introdotte diverse modifiche tecniche che adeguano la disposizione alle modifiche di altre disposizioni, ma non incidono sul livello di protezione dei dati personali nel Regno Unito. È stato inserito inoltre un nuovo paragrafo 4 A per riprodurre gli effetti della sezione 18, paragrafo 1, della legge del 2018 sulla protezione dei dati, che conferisce al segretario di Stato la facoltà di specificare, mediante regolamenti, le circostanze in cui i trasferimenti di dati sono ritenuti necessari per motivi di pubblico interesse. In ultimo luogo, il nuovo articolo 49 A riproduce gli effetti della sezione 18, paragrafo 2, della legge del 2018 sulla protezione dei dati, che consente al segretario di Stato di limitare, mediante regolamenti, i trasferimenti di dati che non siano approvati a norma dell'articolo 45 A (trasferimenti approvati mediante regolamenti) e se necessario per importanti motivi di pubblico interesse.

(46) In termini di attuazione delle norme del Regno Unito in materia di trasferimenti internazionali, dall'adozione della decisione di esecuzione (UE) 2021/1772 sono intervenuti numerosi sviluppi.

([67]) Cfr. il protocollo d'intesa tra il segretario di Stato del dipartimento per il Digitale, la cultura, i media e lo sport e l'ICO sul ruolo dell'ICO in relazione alla nuova valutazione dell'adeguatezza del Regno Unito, disponibile al seguente indirizzo: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([68]) Laddove tale votazione abbia esito positivo, i regolamenti cesseranno in definitiva di avere ulteriore effetto giuridico.

([69]) Gli strumenti in materia di trasferimento disponibili a norma dell'articolo 46, paragrafi 2 e 3, del GDPR del Regno Unito sono strumenti giuridicamente vincolanti ed esecutivi applicabili tra autorità o organismi pubblici, norme vincolanti d'impresa conformi all'articolo 47 del GDPR del Regno Unito, clausole tipo di protezione dei dati specificate nei regolamenti adottati dal segretario di Stato o specificati in un documento diffuso dall'Information Commission, un codice di condotta approvato e un meccanismo di certificazione approvato.

(47) Per quanto riguarda i regolamenti di approvazione dei trasferimenti, finora sono stati adottati due nuovi regolamenti che rispecchiano le decisioni di adeguatezza in vigore anche nell'Unione, ossia i regolamenti relativi ai trasferimenti verso la Repubblica di Corea e quelli relativi ai trasferimenti a entità commerciali che hanno aderito all'estensione al Regno Unito del quadro UE-USA per la protezione dei dati personali. I regolamenti di adeguatezza riguardanti la Repubblica di Corea ([70]) sono entrati in vigore il 19 dicembre 2022 e consentono il trasferimento di dati personali dal Regno Unito alla Repubblica di Corea. L'estensione al Regno Unito del quadro UE-USA per la protezione dei dati personali, per la quale i regolamenti ([71]) pertinenti sono entrati in vigore il 12 ottobre 2023, consente la libera circolazione dei dati personali verso organizzazioni statunitensi certificate.

(48) Per quanto riguarda le garanzie adeguate, il Regno Unito ha pubblicato le proprie clausole contrattuali tipo per la protezione dei dati, denominate accordo internazionale sul trasferimento dei dati ([72]), oltre a un addendum alle clausole contrattuali tipo dell'UE, entrambi entrati in vigore nel marzo 2022. L'accordo internazionale sul trasferimento dei dati, che prevede un meccanismo specifico per il Regno Unito volto ad assicurare garanzie adeguate per il trasferimento di dati personali, presenta varie analogie con le clausole contrattuali tipo dell'UE. L'addendum, emesso dall'ICO, consente ai titolari del trattamento e ai responsabili del trattamento nel Regno Unito di avvalersi, per i trasferimenti internazionali, delle clausole contrattuali tipo dell'UE di cui al GDPR del Regno Unito. L'ICO ha inoltre pubblicato uno strumento di valutazione dei rischi connessi ai trasferimenti per aiutare le organizzazioni del Regno Unito a valutare i rischi associati ai trasferimenti internazionali.

(49) Il Regno Unito ha inoltre razionalizzato il processo di approvazione delle norme vincolanti d'impresa (Binding Corporate Rules) mediante nuovi orientamenti e nuove opzioni per tale approvazione. Nel luglio 2022 l'ICO ha pubblicato orientamenti e tabelle di riferimento per spiegare l'approccio del Regno Unito alle norme vincolanti d'impresa post-Brexit e, nel dicembre 2023, è stato pubblicato un addendum per garantire che le norme vincolanti d'impresa approvate secondo il quadro dell'Unione fossero applicabili nel Regno Unito ([73]).

(50) Infine, nel luglio 2023, il Regno Unito è diventato membro associato del Global Cross-Border Privacy Rules Forum (CBPR) ([74]). È importante sottolineare che tale adesione non comporta alcuna agevolazione dei trasferimenti di dati dal Regno Unito ad altri membri del forum CBPR. Il Regno Unito ha chiarito che qualsiasi trasferimento di dati personali dal Regno Unito verso paesi terzi o organizzazioni internazionali deve soddisfare le condizioni stabilite dalla legislazione del Regno Unito, come descritto in precedenza, in particolare la verifica della protezione dei dati, che richiede che i livelli di protezione non siano «sostanzialmente inferiori» a quelli previsti dal GDPR del Regno Unito.

(51) Come la Commissione ha già spiegato, il forum CBPR non garantisce un livello sufficiente di protezione dei dati personali provenienti dall'UE. In particolare, non prevede diritti delle persone fisiche azionabili ([75]). È quindi particolarmente importante che, sebbene il Regno Unito sia membro associato del Global CBPR Forum, quest'ultimo non possa costituire un meccanismo di trasferimento valido a norma del diritto del Regno Unito in materia di protezione dei dati. Se così non fosse, il livello di protezione attualmente garantito ai dati personali trasferiti dall'UE al Regno Unito sarebbe compromesso. La Commissione continuerà pertanto a seguire da vicino gli ulteriori sviluppi al riguardo.

([70]) Disponibili al seguente indirizzo: https://www.legislation.gov.uk/uksi/2022/1213/made.

([71]) Disponibili al seguente indirizzo: https://www.legislation.gov.uk/uksi/2023/1028/made.

([72]) Disponibile al seguente indirizzo: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/.

([73]) Dopo la Brexit, l'ICO ha ricevuto un notevole numero di domande relative alle norme vincolanti d'impresa del Regno Unito. Molte norme vincolanti d'impresa approvate non potevano più essere utilizzate, perché solo quelle in cui l'ICO era stato coinvolto nel processo di approvazione potevano continuare a esserlo dopo la Brexit, ma occorreva presentare all'ICO una documentazione aggiornata sulle suddette norme conforme al GDPR del Regno Unito.

([74]) Al forum CBPR aderiscono gli Stati Uniti d'America, il Canada, il Giappone, la Repubblica di Corea, le Filippine, Singapore, Taiwan e Australia, mentre Maurizio, il Dubai International Financial Centre e le Bermuda sono membri associati come il Regno Unito.

([75]) Cfr. ad esempio l'analisi comparativa condotta dalle autorità di protezione dei dati del G7 sugli elementi fondamentali del sistema di certificazione del GDPR e del sistema CBPR, che ha evidenziato «notevoli differenze» tra gli stessi, anche per quanto riguarda l'applicabilità e i mezzi di ricorso legali, le norme in materia di vigilanza indipendente e di accesso da parte delle pubbliche amministrazioni. Disponibile al seguente indirizzo: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165.
Cfr. considerando 79 della decisione di esecuzione (UE) 2021/419 della Commissione, del 23 gennaio 2019, a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio per quanto riguarda la protezione adeguata dei dati personali da parte del Giappone a norma della legge sulla protezione delle informazioni personali (GU L 76 del 19.3.2019, pag. 1, ELI: http://data.europa.eu/eli/dec_impl/2019/419/oj).
Cfr. gruppo di lavoro articolo 29, parere 02/2014 relativo a un repertorio dei requisiti relativi alle norme vincolanti di impresa presentate alle autorità nazionali di protezione dei dati dell'Unione europea e alle norme transfrontaliere in materia di privacy presentate agli agenti responsabili delle CBPR dei paesi dell'APEC, del 6 marzo 2014.

2.2.6. *Processo decisionale automatizzato*

(52) Pur mantenendo diversi elementi delle norme sul processo decisionale automatizzato valutati nel considerando 54 della decisione di esecuzione (UE) 2021/1772, la legge sull'accesso ai dati e sul loro utilizzo ne ha modificato alcuni aspetti.

(53) In primo luogo, il nuovo articolo 22B del GDPR del Regno Unito stabilisce un divieto generale di trattamento di categorie particolari di dati personali (definite all'articolo 9, paragrafo 1, del GDPR del Regno Unito) per decisioni basate unicamente su un trattamento automatizzato che producono effetti giuridici o che, in modo analogo, incidono significativamente sull'interessato. Sono tuttavia previste tre eccezioni a tale divieto: l'interessato ha manifestato il proprio consenso esplicito a tale trattamento, oppure la decisione è necessaria per la conclusione o l'esecuzione di un contratto tra il titolare dei dati e l'interessato, oppure il trattamento è imposto o autorizzato per legge. Per queste due ultime eccezioni, il trattamento automatizzato deve essere necessario per motivi di interesse pubblico rilevante ([76]). Il divieto generale non si applica alle decisioni significative basate su un trattamento automatizzato di categorie non particolari di dati.

(54) Inoltre la nuova sezione 22 A del GDPR del Regno Unito chiarisce la definizione di decisione «basata unicamente su un trattamento automatizzato» stabilendo che si tratta di una decisione in cui non vi è alcun coinvolgimento umano significativo nel processo decisionale. È importante sottolineare che i titolari del trattamento, per determinare se il coinvolgimento umano è stato significativo, sono tenuti a valutare in che misura la profilazione contribuisca a una decisione. L'articolo 22 A del GDPR del Regno Unito chiarisce inoltre che per «decisione significativa» si intende una decisione che produce effetti giuridici o che, in modo analogo, incide significativamente su un interessato ([77]).

(55) In secondo luogo, il nuovo articolo 22C del GDPR del Regno Unito impone ai titolari del trattamento di attuare misure che prevedano garanzie pertinenti per qualsiasi decisione significativa basata, interamente o parzialmente, su dati personali, e basata unicamente su un trattamento automatizzato (anche di categorie non particolari di dati personali). Tali garanzie devono includere l'informazione dell'interessato in merito al processo decisionale, consentendogli di contestare la decisione e presentare osservazioni, nonché di ottenere l'intervento umano nel processo decisionale ([78]).

(56) Infine, il nuovo articolo 22D del GDPR del Regno Unito conferisce al segretario di Stato il potere di adottare atti di diritto derivato per definire cosa costituisca un coinvolgimento umano significativo, e quale decisione debba essere considerata come avente effetti altrettanto significativi sugli interessati. Tale nuovo articolo consente inoltre al segretario di Stato di adottare atti di diritto derivato per i) aggiungere nuove garanzie; ii) imporre prescrizioni che integrino le garanzie esistenti; e iii) definire le misure che non soddisfano le garanzie ([79]). È importante sottolineare che, prima di adottare regolamenti conformemente all'articolo 22D del GDPR del Regno Unito, il segretario di Stato deve consultare l'ICO ([80]); inoltre i regolamenti non possono modificare l'articolo 22C del GDPR del Regno Unito ([81]) e sono soggetti all'approvazione espressa ([82]), il che significa che devono essere approvati da entrambe le camere del parlamento del Regno Unito prima di poter essere adottati.

(57) Sebbene la legge sull'accesso ai dati e sul loro utilizzo abbia così modificato il quadro del processo decisionale automatizzato, è importante osservare che, nell'ambito del quadro giuridico del Regno Unito, il processo decisionale automatizzato continua ad essere soggetto alle garanzie fondamentali che proteggono il diritto di ottenere l'intervento umano in tutti i casi di decisioni significative basate unicamente su un trattamento automatizzato, ossia sulla base del trattamento di dati personali sensibili e non sensibili ([83]). Inoltre, come rilevato

([76]) Articolo 22B del GDPR del Regno Unito, introdotto dalla sezione 80, paragrafo 1, della legge sull'accesso ai dati e sul loro utilizzo.
([77]) Articolo 22 A del GDPR del Regno Unito, introdotto dalla sezione 80, paragrafo 1, della legge sull'accesso ai dati e sul loro utilizzo.
([78]) Articolo 22C del GDPR del Regno Unito, introdotto dalla sezione 80, paragrafo 1, della legge sull'accesso ai dati e sul loro utilizzo.
([79]) Articolo 22D del GDPR del Regno Unito, introdotto dalla sezione 80, paragrafo 1, della legge sull'accesso ai dati e sul loro utilizzo. Qualsiasi norma adottata nell'ambito di tali poteri è soggetta all'approvazione espressa (*affirmative resolution procedure*), che garantisce il controllo parlamentare. I regolamenti non possono modificare le disposizioni dell'articolo 22C.
([80]) Sezione 182, paragrafo 2, della legge del 2018 sulla protezione dei dati.
([81]) Articolo 22D, paragrafo 4, del GDPR del Regno Unito.
([82]) Articolo 22D, paragrafo 5, del GDPR del Regno Unito.
([83]) Articolo 22C, paragrafo 2, del GDPR del Regno Unito, introdotto dalla sezione 80, paragrafo 1, della legge sull'accesso ai dati e sul loro utilizzo.

dalla Commissione in precedenti decisioni di adeguatezza ([84]), è improbabile che le norme specifiche relative al processo decisionale automatizzato di cui al GDPR del Regno Unito incidano sul livello di protezione dei dati personali trasferiti dall'Unione al Regno Unito. Per quanto riguarda i dati personali raccolti nell'Unione, qualsiasi decisione basata su un trattamento automatizzato sarà generalmente presa dal titolare del trattamento nell'Unione (che ha un rapporto diretto con l'interessato) ed è, di conseguenza, soggetta al regolamento (UE) 2016/679.

2.3. **Vigilanza e applicazione**

2.3.1. *Vigilanza indipendente*

(58) Nel Regno Unito continua a spettare a un'autorità indipendente di controllo della protezione dei dati il compito di controllare e fare applicare il quadro in materia di protezione dei dati, come analizzato nei considerando da 85 a 91 della decisione di esecuzione (UE) 2021/1772. La legge sull'accesso ai dati e sul loro utilizzo riforma la struttura di governance di tale autorità istituendo un'entità giuridica, l'Information Commission, che sostituirà l'ICO, strutturata come «corporation sole».

(59) Più specificamente, le misure di governance previste dalla legge sull'accesso ai dati e sul loro utilizzo, una volta attuate, aboliranno l'ufficio dell'Information Commissioner e trasferiranno le funzioni, il personale e i beni dall'ICO alla nuova entità, l'Information Commission. L'Information Commission è composta da membri con e senza incarichi esecutivi ([85]). La legge affida all'Information Commissioner, uno dei membri senza incarichi esecutivi, il ruolo di presidente dell'Information Commission ([86]). La legge sui dati (utilizzo e accesso) prevede inoltre che, nella misura in cui ciò sia opportuno in conseguenza del trasferimento di funzioni, i riferimenti all'Information Commissioner in tutti gli atti normativi o in altri documenti (ogniqualvolta siano stati approvati o redatti) siano considerati come riferimenti all'Information Commission. Per l'esercizio delle sue funzioni, l'Information Commission può istituire comitati e delegare funzioni a un membro, a un dipendente o a un comitato dell'Information Commission ([87]) e può adottare disposizioni per disciplinare la sua procedura e quella dei comitati, anche per quanto riguarda il quorum e l'adozione di decisioni a maggioranza. Tali procedure devono essere rese pubbliche ([88]).

(60) È importante sottolineare che l'indipendenza dell'Information Commission è soggetta, anche per quanto riguarda le norme relative alla nomina e alla revoca del suo presidente, alle stesse garanzie che sono state citate nei considerando da 87 a 90 della decisione di esecuzione (UE) 2021/1772 ([89]). Analoghe tutele si applicano agli altri membri senza incarichi esecutivi dell'Information Commission. In particolare, il presidente dell'Information Commission è nominato dal Re su raccomandazione del segretario di Stato. È selezionato sulla base del merito nell'ambito di un concorso equo e aperto ([90]). Gli altri membri senza incarichi esecutivi sono nominati dal segretario di Stato previa consultazione del presidente. I candidati possono essere raccomandati per la nomina o nominati solo se selezionati sulla base del merito nell'ambito di un concorso equo e aperto e se il segretario di Stato ha accertato che non si trovano in una situazione di conflitto di interessi ([91]). I membri con incarichi esecutivi sono assunti dall'Information Commission alle condizioni stabilite dai membri senza incarichi esecutivi ([92]). Il direttore esecutivo è nominato dal presidente e da altri membri senza incarichi esecutivi, previa consultazione del segretario di Stato. Anche le nomine dei membri con incarichi esecutivi sono soggette a una selezione sulla base del merito nell'ambito di un concorso equo e aperto ([93]).

(61) Il presidente può essere revocato solo dal Re su indirizzo di entrambe le camere del parlamento e solo se il segretario di Stato ha presentato una relazione alla camera in questione in cui dichiara di aver accertato che il presidente si è reso colpevole di gravi negligenze, si trova in situazione di conflitto di interessi, non ha assolto obblighi specifici di

([84]) Cfr. ad esempio il considerando 94 della decisione di esecuzione (UE) 2019/419 e il considerando 81 della decisione di esecuzione (UE) 2022/254 della Commissione, del 17 dicembre 2021, a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte della Repubblica di Corea nel quadro della legge sulla protezione delle informazioni personali (GU L 44, 24.2.2022, p. 1, ELI: http://data.europa.eu/eli/dec_impl/2022/254/oj).
([85]) Paragrafo 3, punto 1, dell'allegato 12 A della legge del 2018 sulla protezione dei dati.
([86]) Sezioni 117, 118, 119 e 120 in combinato disposto con l'allegato 14 della legge sull'accesso ai dati e sul loro utilizzo.
([87]) Paragrafi 13 e 14 dell'allegato 12 A della legge del 2018 sulla protezione dei dati.
([88]) Paragrafo 16 dell'allegato 12 A della legge del 2018 sulla protezione dei dati.
([89]) Articolo 52 del GDPR del Regno Unito e allegato 12 A della legge del 2018 sulla protezione dei dati, introdotto dalla sezione 114 A del disegno di legge sull'accesso ai dati e sul loro utilizzo.
([90]) Paragrafo 5, punto 1, e paragrafo 3, punto 2, dell'allegato 12 A della legge del 2018 sulla protezione dei dati.
([91]) Paragrafo 3, punto 2, e paragrafi 5 e 6, dell'allegato 12 A della legge del 2018 sulla protezione dei dati.
([92]) Paragrafo 11 dell'allegato 12 A della legge del 2018 sulla protezione dei dati.
([93]) Paragrafo 5, punto 2, dell'allegato 12 A della legge del 2018 sulla protezione dei dati.

informazione in merito a potenziali conflitti di interessi o non è in grado, non è idoneo o non è disposto a svolgere le funzioni di presidente ([94]). I membri senza incarichi esecutivi possono essere rimossi dall'incarico dal segretario di Stato solo se sono soddisfatte le condizioni specifiche stabilite dalla legislazione. Tra queste figurano una situazione di conflitto di interessi, gravi negligenze o incapacità, indisponibilità o inidoneità a svolgere le proprie funzioni. In termini di garanzie supplementari, il segretario di Stato è tenuto a rendere pubblica la decisione di procedere in tal senso e a fornire al membro in questione una dichiarazione attestante i motivi della rimozione dall'incarico ([95]).

(62) Il ruolo principale dell'Information Commission continuerà a essere il monitoraggio e l'applicazione del quadro in materia di protezione dei dati nel Regno Unito al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche ([96]). Per quanto riguarda la funzione dell'Information Commission di garantire un livello adeguato di protezione dei dati personali, la legge sull'accesso ai dati e sul loro utilizzo esige specificamente che l'Information Commission tenga conto degli interessi degli interessati, dei titolari del trattamento e di altri soggetti, consideri l'interesse pubblico generale e promuova tra il pubblico un clima di fiducia nel trattamento dei dati personali ([97]). Tali obiettivi sono menzionati anche nel considerando 7 del regolamento (UE) 2016/679.

(63) Inoltre la legge sull'accesso ai dati e sul loro utilizzo specifica che l'Information Commission, nello svolgimento delle sue funzioni a norma della legislazione in materia di protezione dei dati, deve prendere in considerazione la promozione dell'innovazione e della concorrenza, l'importanza della prevenzione, dell'indagine, dell'accertamento e del perseguimento dei reati, la necessità di salvaguardare la pubblica sicurezza e la sicurezza nazionale e le esigenze specifiche connesse alla protezione dei minori ([98]). Il diritto dell'UE in materia di protezione dei dati riconosce inoltre la necessità di trovare un equilibrio tra la protezione dei dati personali e diversi altri diritti e obiettivi fondamentali, quali il progresso economico e sociale, la sicurezza e la giustizia, e la libertà d'impresa ([99]).

2.3.2. *Applicazione, comprese le sanzioni*

(64) I poteri e i compiti dell'Information Commission continuano a corrispondere a quelli delle autorità di controllo della protezione dei dati degli Stati membri a norma dei pertinenti articoli del regolamento (UE) 2016/679 ([100]), come valutato nei considerando da 91 a 95 della decisione di esecuzione (UE) 2021/1772.

(65) La legge sull'accesso ai dati e sul loro utilizzo ha introdotto alcuni chiarimenti in merito all'esercizio di alcuni di tali poteri.

(66) Da un lato, la legge sull'accesso ai dati e sul loro utilizzo chiarisce che l'Information Commission può chiedere documenti e informazioni specifici quando ricorre al potere relativo all'avviso di informazione ([101]). Dall'altro, la legge sull'accesso ai dati e sul loro utilizzo introduce due nuovi poteri di indagine in capo all'Information Commission: un nuovo potere di richiedere una relazione ([102]) e la facoltà di emettere avvisi formali di comparizione (*interview notices*) indirizzati ai titolari del trattamento in caso di presunta violazione del GDPR del Regno Unito o della legge del 2018 sulla protezione dei dati ([103]).

([94]) Paragrafo 7, punti 6 e 7, dell'allegato 12 A della legge del 2018 sulla protezione dei dati.
([95]) Paragrafo 9, punti 6, 7, 8 e 9, dell'allegato 12 A della legge del 2018 sulla protezione dei dati.
([96]) Articolo 51 del GDPR del Regno Unito.
([97]) Sezione 91 della legge sull'accesso ai dati e sul loro utilizzo, che introduce la sezione 120 A della legge del 2018 sulla protezione dei dati.
([98]) Sezione 91 della legge sull'accesso ai dati e sul loro utilizzo, che introduce la sezione 120B della legge del 2018 sulla protezione dei dati. La legge sull'accesso ai dati e sul loro utilizzo introduce inoltre una nuova sezione 120C nella legge del 2018 sulla protezione dei dati, che impone all'Information Commission di preparare e pubblicare una strategia che, tra l'altro, rifletta il modo in cui considererà i temi summenzionati e la promozione della crescita economica nell'esercizio delle sue funzioni normative.
([99]) Cfr. in particolare i considerando 2 e 4 e l'articolo 23 del regolamento (UE) 2016/679.
([100]) Articoli 57 e 58 del GDPR del Regno Unito.
([101]) Sezione 97 della legge sull'accesso ai dati e sul loro utilizzo, che modifica la sezione 142 della legge del 2018 sulla protezione dei dati. L'esame degli effetti della tecnologia e del ruolo della protezione dei dati nella creazione di un clima di fiducia nell'economia digitale rientra tra le attività delle autorità di regolamentazione della protezione dei dati sia nel Regno Unito che nell'UE. Nella relazione annuale 2024 del comitato europeo per la protezione dei dati, pag. 12, il vicepresidente dichiara che l'EDPB è un organismo dinamico e collaborativo che svolge un ruolo centrale nel garantire l'applicazione coerente delle norme in materia di protezione dei dati in tutta Europa, e che, in qualità di vicepresidente, lo considera un custode dei diritti alla vita privata delle persone fisiche in grado di equilibrare pienamente le esigenze dell'innovazione e della crescita economica.
([102]) Sezione 98 della legge sull'accesso ai dati e sul loro utilizzo, che modifica la sezione 146 della legge del 2018 sulla protezione dei dati.
([103]) Sezione 100 della legge sull'accesso ai dati e sul loro utilizzo, che introduce la sezione 148 A della legge del 2018 sulla protezione dei dati.

(67) Per quanto riguarda l'esercizio di tali poteri da parte dell'Information Commission, dall'entrata in vigore della decisione di esecuzione (UE) 2021/1772, l'organismo ha trattato circa 40 000 reclami di interessati all'anno, un numero simile a quelli trattati quando il Regno Unito faceva ancora parte dell'Unione e applicava il regolamento (UE) 2016/679 ([104]). L'ICO ha inoltre condotto indagini d'ufficio su un'ampia gamma di questioni settoriali e di conformità, compresi i diritti degli interessati ([105]).

(68) In termini di misure di contrasto, dall'entrata in vigore della decisione di esecuzione (UE) 2021/1772 l'Information Commissioner ha emesso 120 ammonimenti, 32 avvisi di informazione, 3 avvisi di valutazione, 12 avvisi di esecuzione, 2 avvertimenti e 12 sanzioni pecuniarie ([106]). Queste misure comprendono diverse sanzioni pecuniarie significative imposte a norma del GDPR del Regno Unito e della legge del 2018 sulla protezione dei dati. Ad esempio, nell'aprile 2023 l'Information Commissioner ha comminato a una piattaforma di media sociali una sanzione pecuniaria di 12,7 milioni di GBP per uso improprio di dati di minori ([107]). Nel marzo 2025 a una società di software è stata comminata una sanzione pecuniaria di 3,07 milioni di GBP per carenze in materia di sicurezza che mettevano a rischio le informazioni personali di oltre 70 000 persone ([108]). Recentemente, nel giugno 2025, a seguito di un attacco informatico ([109]) su vasta scala avvenuto nel 2023, l'Information Commissioner ha comminato una sanzione pecuniaria di 2,31 milioni di GBP a una società che conduceva test genetici perché non aveva attuato misure di sicurezza adeguate a proteggere le informazioni personali degli utenti del Regno Unito.

(69) Dall'adozione della decisione di esecuzione (UE) 2021/1772, l'ufficio dell'Information Commissioner ha inoltre elaborato e pubblicato un considerevole numero di orientamenti, pareri e altri documenti di orientamento, che chiariscono l'applicazione delle norme in materia di protezione dei dati in settori importanti, quali il riconoscimento facciale, l'equità nell'intelligenza artificiale, i dati dei minori, il marketing diretto, la videosorveglianza, il diritto di accesso, la trasparenza nell'assistenza sanitaria e sociale ecc., rivolti a vari destinatari, tra cui piccole e medie imprese, soggetti specifici quali scuole, asili nido o amministrazioni pubbliche di piccole dimensioni, come pure alle imprese e al pubblico in generale o agli interessati ([110]).

3. IMPORTANTI SVILUPPI RIGUARDANTI L'ACCESSO E L'USO DEI DATI PERSONALI TRASFERITI DALL'UNIONE EUROPEA DA PARTE DI AUTORITÀ PUBBLICHE NEL REGNO UNITO

3.1. Quadro giuridico generale

(70) Il Regno Unito continua a essere membro del Consiglio d'Europa, ad aderire alla convenzione europea dei diritti dell'uomo e ad essere sottoposto alla giurisdizione della Corte europea dei diritti dell'uomo. Continua pertanto ad essere soggetto agli obblighi sanciti dal diritto internazionale come descritto ai considerando da 116 a 119 della decisione di esecuzione (UE) 2021/1772, che disciplinano il sistema di accesso delle amministrazioni pubbliche del Regno Unito ai dati personali sulla base di principi, garanzie e diritti individuali identici a quelli che si applicano ai 27 Stati membri in quanto firmatari della CEDU e che si riflettono, in larga misura, nella pertinente giurisprudenza della Corte di giustizia dell'Unione europea.

(71) Nel Regno Unito le garanzie e i diritti specifici in materia di protezione dei dati nell'ambito del trattamento dei dati da parte di autorità pubbliche, comprese le autorità di contrasto e gli organismi preposti alla sicurezza nazionale, continuano ad essere garantiti dalla legge del 2018 sulla protezione dei dati, come analizzato nei considerando da 121 a 132 della decisione di esecuzione (UE) 2021/1772. La legge sull'accesso ai dati e sul loro utilizzo ha modificato solo in modo limitato e mirato le parti della legge del 2018 sulla protezione dei dati che stabiliscono le norme per il trattamento dei dati personali nel contesto delle attività di contrasto penale (parte 3 della legge del 2018 sulla protezione dei dati) e della sicurezza nazionale (parte 4 della legge del 2018 sulla protezione dei dati).

([104]) Relazioni annuali dell'Information Commissioner 2021-2022, 2022-2023 e 2023-2024. Cfr. anche decisione di esecuzione (UE) 2021/1772, considerando 96.
([105]) Relazione annuale dell'Information Commissioner 2023-2024, pag. 41.
([106]) Relazioni annuali dell'Information Commissioner 2021-2022, 2022-2023 e 2023-2024.
([107]) Per ulteriori informazioni su queste e altre misure di contrasto cfr. il sito web dell'ICO al seguente indirizzo: https://ico.org.uk/action-weve-taken/enforcement/.
([108]) Ulteriori informazioni sono disponibili al seguente indirizzo: https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/.
([109]) Ulteriori informazioni sono disponibili al seguente indirizzo: https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/.
([110]) Disponibili al seguente indirizzo: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

(72) Per quanto riguarda il trattamento dei dati personali da parte di autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, compresa la salvaguardia e la prevenzione di minacce alla sicurezza pubblica, la parte 3 della legge del 2018 sulla protezione dei dati continua a prevedere principi, diritti e obblighi simili a quelli stabiliti dalla direttiva (UE) 2016/680 ([111]).

(73) In particolare, alla stessa data della presente decisione, la Commissione ha adottato una decisione a norma dell'articolo 36, paragrafo 3, della direttiva (UE) 2016/680, in cui constata che il regime di protezione dei dati applicabile al trattamento da parte delle autorità di contrasto penale del Regno Unito a fini di contrasto penale continua ad assicurare un livello di protezione sostanzialmente equivalente a quello garantito dalla direttiva (UE) 2016/680.

(74) La legge sull'accesso ai dati e sul loro utilizzo ha modificato e consolidato le esenzioni previste nella parte 3 della legge del 2018 sulla protezione dei dati, messe a disposizione delle autorità competenti a fini di sicurezza nazionale. L'esenzione per motivi di sicurezza nazionale consente alle autorità competenti di disapplicare talune disposizioni della parte 3 della legge del 2018 sulla protezione dei dati se l'esenzione da tale disposizione è necessaria al fine di salvaguardare la sicurezza nazionale ([112]). L'esenzione rispecchia le esenzioni per motivi di sicurezza nazionale previste per il trattamento dei dati personali ai sensi del GDPR del Regno Unito (di cui alla sezione 26 della legge del 2018 sulla protezione dei dati) e della parte 4 della legge del 2018 sulla protezione dei dati (di cui alla sezione 110 della legge del 2018).

(75) L'esenzione per motivi di sicurezza nazionale è soggetta alle stesse limitazioni e garanzie previste per le esenzioni ai sensi del GDPR del Regno Unito e della parte 4 della legge del 2018 sulla protezione dei dati, analizzate nei considerando da 64 a 67 e 126 della decisione di esecuzione (UE) 2021/1772. In particolare, l'esenzione può essere applicata soltanto se necessaria per salvaguardare la sicurezza nazionale. Non si tratta di un'esenzione generalizzata e deve essere presa in considerazione e invocata dal titolare del trattamento caso per caso ([113]). Inoltre qualsiasi applicazione dell'esenzione deve essere conforme alle norme in materia di diritti umani (sostenute dalla legge del 1998 sui diritti umani e dalla convenzione europea dei diritti dell'uomo), secondo le quali qualsiasi ingerenza rispetto ai diritti in materia di tutela della vita privata dovrebbe essere necessaria e proporzionata in una società democratica ([114]). Ciò è confermato anche dagli orientamenti dell'ICO sull'applicazione delle esenzioni per motivi di sicurezza nazionale ([115]).

(76) Inoltre, sulla base delle modifiche introdotte dalla legge sull'accesso ai dati e sul loro utilizzo ([116]), una specifica attività di trattamento da parte delle autorità di contrasto penale può essere disciplinata anche dalle disposizioni della parte 4 della legge del 2018 sulla protezione dei dati, che di norma si applica solo al trattamento dei dati da parte delle autorità di sicurezza nazionale.

([111]) La sezione 69 della legge sull'accesso ai dati e sul loro utilizzo inserisce nella legge del 2018 sulla protezione dei dati due nuove sezioni relative alla definizione di consenso e alle condizioni per avvalersi del consenso come previsto all'articolo 4, paragrafo 11, e all'articolo 7 del GDPR del Regno Unito [che rispecchiano le corrispondenti disposizioni del regolamento (UE) 2016/679], ossia la sezione 33, paragrafo 1 A e la sezione 40 A, e in tal modo chiarisce il concetto di consenso e le condizioni per avvalersi del consenso, da utilizzarsi come base giuridica per il trattamento dei dati personali da parte delle autorità competenti a fini di contrasto penale. Inoltre la sezione 71, paragrafi 7 e 8, della legge sull'accesso ai dati e sul loro utilizzo modifica leggermente, chiarendola, la formulazione della sezione 36, paragrafo 1, della legge del 2018 sulla protezione dei dati. Infine, nei casi pertinenti, le modifiche del GDPR del Regno Unito introdotte dalla legge sull'accesso ai dati e sul loro utilizzo descritte nella sezione 2 si riflettono anche nella parte 3 della legge del 2018 sulla protezione dei dati: si veda ad esempio la sezione 74, paragrafi da 2 a 5, sul trattamento dei dati sensibili, la sezione 76, paragrafi da 4 a 6, sui termini per rispondere alle richieste dell'interessato, la sezione 78, paragrafi 2 e 3, sulle ricerche in risposta alle richieste degli interessati e la sezione 80, paragrafi da 3 a 5, sul processo decisionale automatizzato.

([112]) Sezione 78 A, paragrafo 1, della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 88 della legge sull'accesso ai dati e sul loro utilizzo. Ai sensi della sezione 78 A, paragrafi da 2 a 4, della legge del 2018 sulla protezione dei dati, l'esenzione consente di disapplicare i principi in materia di protezione dei dati (fatta eccezione per il principio di liceità e le condizioni e garanzie per il trattamento dei dati sensibili), i diritti individuali, gli obblighi dei titolari del trattamento e dei responsabili del trattamento in relazione alle violazioni dei dati, alcune parti delle norme sui trasferimenti internazionali di dati e alcuni dei poteri di accesso dell'Information Commissioner per lo svolgimento di ispezioni e l'adozione di azioni esecutive.

([113]) Cfr. *Baker v Secretary of State for the Home Department* [2001] UKIT NSA2 («*Baker v Secretary of State*»).

([114]) Cfr. anche *Guriev v Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), punto 45; *Lin v Commissioner of the Police for the Metropolis* [2015] EWHC 2484 (QB), punto 80.

([115]) Cfr. gli orientamenti dell'ICO sull'eccezione per motivi di sicurezza nazionale e difesa, disponibili al seguente indirizzo: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/national-security-and-defence-exemption-a-guide.

([116]) Sezioni 89 e 90 della legge sull'accesso ai dati e sul loro utilizzo.

(77) Sebbene il regime di protezione dei dati relativo al trattamento a fini di sicurezza nazionale sia quindi esteso, in determinate situazioni, anche al trattamento dei dati da parte delle autorità di contrasto penale, ciò vale solo in circostanze specifiche e subordinatamente a condizioni e garanzie rigorose, vale a dire qualora i) un'autorità competente sia designata come autorità competente qualificata nei regolamenti adottati dal segretario di Stato che richiedono l'approvazione parlamentare ([117]) e ii) il segretario di Stato designi mediante notifica una specifica attività di trattamento svolta dall'autorità competente qualificata. È importante sottolineare che tale designazione può avvenire solo se il segretario di Stato la ritiene necessaria ai fini della salvaguardia della sicurezza nazionale, ossia qualora un'autorità di contrasto penale agisca per finalità di sicurezza nazionale e l'attività di trattamento sia svolta dall'autorità competente qualificata come contitolare del trattamento con almeno un servizio di intelligence ([118]). Come ulteriori garanzie, il segretario di Stato deve consultare l'Information Commissioner prima di emettere un avviso di designazione ([119]), il testo dell'avviso deve, in linea di principio, essere pubblicato ([120]) e una persona direttamente interessata da un avviso di designazione può chiedere un controllo giurisdizionale ([121]). La modifica mira pertanto essenzialmente a chiarire che, quando le autorità del Regno Unito sono competenti sia in materia di contrasto che in materia di sicurezza nazionale e trattano i dati nell'ambito di quest'ultima competenza, può applicarsi il regime di protezione dei dati relativo ai servizi di sicurezza nazionale.

(78) La parte 4 della legge del 2018 sulla protezione dei dati disciplina il trattamento dei dati da parte dei servizi di intelligence del Regno Unito. Essa continua a stabilire i principali principi in materia di protezione dei dati, a imporre le condizioni relative al trattamento di categorie particolari di dati, a fissare i diritti degli interessati, a richiedere la protezione dei dati fin dalla progettazione e a disciplinare i trasferimenti di dati personali, come descritto nei considerando da 125 a 132 della decisione di esecuzione (UE) 2021/1772.

(79) Le modifiche introdotte in tale regime dalla legge sull'accesso ai dati e sul loro utilizzo sono limitate. Per quanto riguarda il diritto di accesso degli interessati di cui alla sezione 94 della legge del 2018 sulla protezione dei dati, la legge sull'accesso ai dati e sul loro utilizzo introduce una nuova sottosezione (2 A) in cui chiarisce che l'interessato ha diritto alle informazioni pertinenti solo nella misura in cui il titolare del trattamento è in grado di fornirle sulla base di una ricerca ragionevole e proporzionata ([122]). Come spiegato al considerando 35, tale modifica disciplina il diritto di accesso sulla base di norme giuridiche consolidate che tengono conto anche degli interessi dell'interessato. In materia di processo decisionale automatizzato, ai titolari del trattamento continua ad essere vietato adottare una decisione che incida in modo significativo sull'interessato e che si basi unicamente sul trattamento automatizzato di dati personali che lo riguardano, a meno che tale decisione non sia richiesta o autorizzata dalla legge, l'interessato abbia dato il consenso a che la decisione sia presa su tale base, o la decisione sia adottata nel contesto di un contratto ([123]); la legge sull'accesso ai dati e sul loro utilizzo introduce nella parte 4 della legge del 2018 sulla protezione dei dati ([124]) la stessa definizione della nozione di «decisione basata unicamente su un trattamento automatizzato» di cui all'articolo 22 A del GDPR del Regno Unito e analizzata al considerando 53 della presente decisione.

3.2. **Importanti sviluppi riguardanti l'accesso e l'uso di dati personali da parte delle autorità pubbliche del Regno Unito per motivi di contrasto penale**

(80) Il diritto del Regno Unito continua a imporre importanti limitazioni all'accesso e all'uso di dati personali per fini di contrasto penale e prevede, in tale ambito, meccanismi di vigilanza e ricorso, come analizzato nei considerando da 134 a 174 della decisione di esecuzione (UE) 2021/1772.

([117]) Sezione 82, paragrafi A1, 2 A e 4, della legge del 2018 sulla protezione dei dati, introdotta dalla sezione 89, paragrafo 2, della legge sull'accesso ai dati e sul loro utilizzo.

([118]) Sezione 82 A, paragrafi 1 e 2, introdotta della sezione 89, paragrafo 3, della legge sull'accesso ai dati e sul loro utilizzo. Come ulteriori garanzie, il segretario di Stato deve consultare l'Information Commissioner prima di emettere un avviso di designazione (cfr. la nuova sezione 82 A, paragrafo 8, della legge del 2018 sulla protezione dei dati), il testo dell'avviso deve, in linea di principio, essere pubblicato (cfr. la nuova sezione 82D, paragrafo 1, fatte salve le esenzioni di cui alla nuova sezione 82D, paragrafo 3, della legge del 2018 sulla protezione dei dati) e una persona direttamente interessata da un avviso di designazione può chiedere un controllo giurisdizionale (cfr. la nuova sezione 82E della legge del 2018 sulla protezione dei dati).

([119]) Sezione 82 A, paragrafo 8, della legge del 2018 sulla protezione dei dati.

([120]) Sezione 82D, paragrafo 1, fatte salve le esenzioni di cui alla nuova sezione 82D, paragrafo 3, della legge del 2018 sulla protezione dei dati.

([121]) Sezione 82E della legge del 2018 sulla protezione dei dati.

([122]) Sezione 78, paragrafo 4, della legge sull'accesso ai dati e sul loro utilizzo.

([123]) Sezione 96 della legge del 2018 sulla protezione dei dati.

([124]) Conformemente alla nuova sezione 96, paragrafo 4, della legge del 2018 sulla protezione dei dati, una decisione si basa su un trattamento unicamente automatizzato se il processo decisionale non prevede la possibilità per un essere umano di accettarla, respingerla o influenzarla. Cfr. sezione 80, paragrafo 4, lettera c), della legge sull'accesso ai dati e sul loro utilizzo.

3.2.1. *Basi giuridiche e limitazioni/garanzie applicabili*

(81) Nell'ordinamento giuridico del Regno Unito, la raccolta di dati personali da operatori economici per fini di contrasto penale continua ad essere consentita sulla base di mandati di perquisizione e ordini di produzione, subordinatamente alle condizioni e alle garanzie di cui ai considerando da 135 a 138 della decisione di esecuzione (UE) 2021/1772.

(82) Inoltre la legge del 2023 sulla sicurezza nazionale ([125]), che mira a contrastare le minacce alla sicurezza nazionale derivanti da attività di spionaggio e sabotaggio e da attività svolte da persone che agiscono per conto di potenze straniere, ha conferito nuovi poteri di accesso, perquisizione e sequestro alla polizia del Regno Unito, compresa la possibilità di ottenere dati personali, qualora vi siano fondati motivi per ritenere che il materiale possa costituire la prova della commissione, attuale o imminente, di uno dei più gravi reati o di minacce da parte di una potenza straniera previsti dalla legge del 2023 sulla sicurezza nazionale ([126]). Tali poteri sono subordinati a condizioni e a garanzie analoghe a quelle analizzate nella decisione di esecuzione (UE) 2021/1772 relative ai poteri esistenti all'epoca. In particolare, il loro esercizio deve essere autorizzato mediante un mandato, un ordine di produzione o un ordine di giustificazione emesso da un organo giurisdizionale indipendente, su domanda presentata dall'agente di polizia/dal funzionario incaricato delle indagini ([127]). Esistono tutele specifiche per il materiale riservato, come il materiale giornalistico e informazioni coperte da segreto professionale ([128]). Analogamente, l'emissione di ordini di divulgazione ([129]), di ordini di comunicare informazioni relative ai clienti ([130]) e di ordini di monitoraggio dei conti ([131]), anch'essa disciplinata dalla legge del 2023 sulla sicurezza nazionale, deve essere autorizzata da un giudice su domanda presentata da un funzionario competente ed è soggetta a condizioni e garanzie specifiche, tra cui il fatto che l'ordine sia richiesto in relazione a una persona specifica ai fini di un'indagine su una minaccia da parte di una potenza straniera, che l'ordine rafforzi l'efficacia dell'indagine e che non sia utilizzato per ottenere informazioni coperte da segreto professionale o altrimenti escluse, quali materiale giornalistico e determinate informazioni sanitarie ([132]).

(83) Come descritto nei considerando da 139 a 141 della decisione di esecuzione (UE) 2021/1772, nel quadro giuridico del Regno Unito specifiche autorità di contrasto, ad esempio la National Crime Agency o il servizio di polizia metropolitano, possono avvalersi di poteri di indagine mirati ai sensi della legge del 2016 sui poteri di indagine ([133]) al fine di prevenire o accertare reati gravi. Gli specifici poteri di indagine di cui tali autorità di contrasto possono fare uso sono l'intercettazione mirata (parte 2 della legge del 2016 sui poteri di indagine), l'acquisizione dei dati relativi alle comunicazioni (parte 3 della medesima legge) e l'ingerenza mirata in apparecchiature (parte 5 della medesima legge). Qualora gli avvisi di conservazione siano emessi dal segretario di Stato ai sensi della parte 4 della legge del 2016 sui poteri di indagine, anche le autorità di contrasto possono trarre vantaggio dall'accesso ai dati conservati relativi alle comunicazioni attraverso i poteri di acquisizione di tali dati di cui alla parte 3 della legge del 2016 sui poteri di indagine.

([125]) Disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted.

([126]) Allegato 2 della legge del 2023 sulla sicurezza nazionale. I reati disciplinati dalla legge del 2023 sulla sicurezza nazionale sono, ad esempio, l'acquisizione o la divulgazione di informazioni protette (sezione 1), l'acquisizione o la divulgazione di segreti commerciali (sezione 3), l'assistenza a un servizio di intelligence estero (sezione 4), lo svolgimento di attività di sabotaggio (sezione 12) o l'adozione di una specifica condotta vietata per conto di una potenza straniera allo scopo di determinare un'ingerenza (sezione 13).

([127]) Cfr. il paragrafo 2, punto 1, il paragrafo 3, punto 1, il paragrafo 4, punto 1, e il paragrafo 10, punto 1, dell'allegato 2 della legge del 2023 sulla sicurezza nazionale.

([128]) Cfr. il paragrafo 2, punto 4, lettera b), il paragrafo 3, punto 4), lettere b) e c), il paragrafo 4, punto 4, lettere b) e c), e il paragrafo 10, punto 1, dell'allegato 2 della legge del 2023 sulla sicurezza nazionale.

([129]) In forza di un ordine di divulgazione a norma dell'allegato 3 della legge del 2023 sulla sicurezza nazionale, un funzionario può notificare a una persona l'obbligo di fornire informazioni, produrre documenti e/o rispondere a domande pertinenti a un'indagine per individuare beni connessi ad attività di minaccia di una potenza straniera, compresi i movimenti o l'uso di tali beni.

([130]) In forza di un ordine di comunicare informazioni relative ai clienti a norma dell'allegato 4 della legge del 2023 sulla sicurezza nazionale, un funzionario può notificare a un istituto finanziario l'obbligo di fornire qualunque informazione relativa a una determinata persona.

([131]) In forza di un ordine di monitoraggio dei conti a norma dell'allegato 5, un istituto finanziario può essere obbligato a fornire a un funzionario le informazioni specificate nell'ordine per il periodo, che non può superare i 90 giorni, e secondo le modalità specificati nell'ordine.

([132]) Allegato 3, paragrafo 2, punto 1, allegato 4, paragrafo 1 e allegato 5, paragrafo 1, della legge del 2023 sulla sicurezza nazionale.

([133]) La legge del 2016 sui poteri di indagine (cfr.: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) ha sostituito una normativa diversa relativa all'intercettazione di comunicazioni, all'ingerenza in apparecchiature e all'acquisizione dei dati di comunicazione, in particolare la parte I della RIPA 2000 che definiva il precedente quadro normativo generale per l'utilizzo di poteri di indagine da parte delle autorità di contrasto e di sicurezza nazionale.

(84) Dall'adozione della decisione di esecuzione (UE) 2021/1772, la legge del 2016 sui poteri di indagine, unitamente alla legge del 2000 sul regolamento sui poteri di indagine (Regulation of Investigatory Powers Act 2000) per l'Inghilterra, il Galles e l'Irlanda del Nord e alla legge del 2000 sul regolamento sui poteri di indagine - Scozia [Regulation of Investigatory Powers (Scotland) Act 2000] per la Scozia, continuano a prevedere la base giuridica e a definire le limitazioni e le garanzie applicabili all'esercizio di tali poteri, come descritto nella decisione di esecuzione (UE) 2021/1772. È importante sottolineare che il quadro giuridico continua ad esigere che, al fine di esercitare tali poteri, le autorità ottengano un mandato ([134]) rilasciato da un'autorità competente ([135]) e approvato da un commissario giudiziario ([136]) indipendente (cosiddetta procedura «a doppia verifica»). L'ottenimento di tale mandato continua ad essere soggetto a una verifica della necessità e della proporzionalità ([137]).

(85) Allo stesso tempo, dall'adozione della decisione di esecuzione (UE) 2021/1772, la legge del 2024 sui poteri di indagine (modifica), che ha ricevuto la regia sanzione (Royal Assent) nell'aprile 2024, ha modificato alcuni elementi specifici della legge del 2016 sui poteri di indagine ([138]). Nei paragrafi seguenti sono esaminati le modifiche e altri importanti sviluppi nella misura in cui riguardano le condizioni, le limitazioni e le garanzie relative all'uso dei summenzionati poteri di indagine specifici da parte delle autorità pubbliche del Regno Unito a fini di contrasto penale, come valutato nei considerando da 177 a 215 della decisione di esecuzione (UE) 2021/1772. Per quanto riguarda gli elementi del quadro del Regno Unito che non sono stati modificati dalla suddetta legge né sono interessati da altri importanti sviluppi, l'analisi effettuata nella decisione di esecuzione (UE) 2021/1772 continua a essere valida.

(86) Per quanto riguarda l'acquisizione e la conservazione mirate dei dati relativi alle comunicazioni ([139]), restano in vigore le condizioni e le garanzie che disciplinano tali poteri, come valutate nella decisione di esecuzione (UE) 2021/1772. La legge del 2024 sui poteri di indagine (modifica) ha chiarito le garanzie esistenti introducendo nella sezione 11 della legge del 2016 sui poteri di indagine (che configura il reato di acquisizione illecita di dati relativi alle comunicazioni da un operatore di telecomunicazioni) un elenco di esempi riconducibili alla nozione di «'autorità legittima» in tale disposizione ([140]). Inoltre la legge del 2024 sui poteri di indagine (modifica) ha ulteriormente chiarito la definizione di «dati relativi alle comunicazioni» di cui alla sezione 261 della legge del 2016 sui poteri di indagine, specificando esplicitamente che i dati relativi agli abbonati si qualificano come dati relativi alle comunicazioni ([141]).

([134]) La parte 2, capitolo 2, della legge del 2016 sui poteri di indagine prevede un numero limitato di casi nei quali si possono effettuare intercettazioni in assenza di un mandato. Rientrano in tale contesto: l'intercettazione con il consenso del mittente o del destinatario, l'intercettazione per finalità amministrative o di contrasto, l'intercettazione che si svolge presso determinate istituzioni (prigioni, ospedali psichiatrici e strutture di detenzione per l'immigrazione), nonché l'intercettazione effettuata conformemente a un accordo internazionale pertinente.

([135]) Nella maggior parte dei casi, il segretario di Stato è l'autorità che emette i mandati ai sensi della legge del 2016 sui poteri di indagine, mentre i ministri scozzesi hanno il potere di emettere i mandati di intercettazione mirata, i mandati di assistenza reciproca e i mandati di ingerenza mirata in apparecchiature quando le persone o i locali che devono essere oggetto di intercettazione o le apparecchiature da sottoporre a ingerenza si trovano in Scozia (cfr. articoli 22 e 103 della legge del 2016 sui poteri di indagine). In caso di ingerenza mirata in apparecchiature, un capo delle autorità di contrasto (di cui alla parte 1 e alla parte 2 dell'allegato 6 della legge del 2016 sui poteri di indagine) può emettere il mandato nel rispetto delle condizioni di cui alla sezione 106 della legge del 2016 sui poteri di indagine.

([136]) I commissari giudiziari forniscono assistenza all'Investigatory Powers Commissioner (IPC), un organismo indipendente che esercita funzioni di vigilanza sull'esercizio dei poteri di indagine da parte delle agenzie di intelligence.

([137]) Cfr., in particolare, sezioni 19 e 23 della legge del 2016 sui poteri di indagine.

([138]) Disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2024/9/contents/2025-04-25.

([139]) L'espressione «dati relativi alle comunicazioni» indica il «chi», il «quando», il «dove» e il «come» di una comunicazione, ma non il contenuto, ossia ciò che è stato detto o scritto. I dati relativi alle comunicazioni potrebbero includere l'ora e la durata della comunicazione, il numero o l'indirizzo di posta elettronica del mittente e del destinatario e talvolta l'ubicazione dei dispositivi dai quali è stata effettuata la telecomunicazione (cfr. sezione 261, paragrafo 5, della legge del 2016 sulla protezione dei dati). Tale legge consente al segretario di Stato di imporre agli operatori di telecomunicazioni di conservare i dati relativi alle comunicazioni ai fini dell'accesso mirato da parte di varie autorità pubbliche, tra cui le autorità di contrasto e le agenzie di intelligence. La parte 4 della legge del 2016 sui poteri di indagine prevede la conservazione dei dati relativi alle comunicazioni, mentre la parte 3 prevede l'acquisizione mirata di dati relativi alle comunicazioni. La parte 3 e la parte 4 della legge del 2016 sui poteri di indagine stabiliscono altresì limitazioni specifiche sull'utilizzo di tali poteri e prevedono garanzie specifiche.

([140]) Ad esempio, se i dati relativi alle comunicazioni sono acquisiti nell'esercizio di un potere legittimo di un'autorità pubblica competente o in conformità di un provvedimento di un organo giurisdizionale o altra autorizzazione giudiziaria. Sezione 11, paragrafo 3 A, della legge del 2016 sui poteri di indagine, introdotta dalla sezione 12, paragrafo 3, della legge del 2024 sui poteri di indagine (modifica).

([141]) Sezione 261, paragrafi 5 A e 5B, introdotta dalla sezione 13, paragrafo 3, della legge del 2024 sui poteri di indagine (modifica).

(87) L'emissione di avvisi che impongono la conservazione dei dati relativi alle comunicazioni ([142]) continua a essere soggetta a limitazioni e garanzie, come descritto nei considerando 208 e 209 della decisione di esecuzione (UE) 2021/1772, in particolare ai requisiti di necessità e proporzionalità e all'approvazione di un commissario giudiziario indipendente. La legge del 2024 sui poteri di indagine (modifica) ha introdotto la possibilità di rinnovare tali avvisi; tuttavia tali rinnovi sono soggetti alle stesse condizioni di necessità e proporzionalità e all'approvazione del commissario giudiziario ([143]).

(88) Per quanto riguarda i dati relativi alle comunicazioni, la legge del 2024 sui poteri di indagine (modifica) ha modificato anche la definizione di operatore di telecomunicazioni, ossia i possibili destinatari di un avviso di conservazione. Tale definizione comprende ora qualsiasi persona che controlla o fornisce un sistema di telecomunicazioni che i) non è (interamente o parzialmente) ubicato nel Regno Unito o controllato dal Regno Unito e ii) è utilizzato da un'altra persona per offrire o fornire un servizio di telecomunicazioni a persone nel Regno Unito ([144]). È importante sottolineare che la definizione modificata continua a richiedere sempre uno stretto collegamento con il mercato del Regno Unito. La modifica chiarisce pertanto che le grandi imprese con strutture societarie complesse rientrano nella loro totalità nell'ambito di applicazione della legge del 2016 sui poteri di indagine, senza estendere l'ambito di applicazione della definizione ai fornitori di servizi di telecomunicazioni non destinati a persone nel Regno Unito. Ciò è confermato anche dalle note esplicative relative alla legge del 2024 sui poteri di indagine (modifica), secondo cui la modifica non è intesa a far rientrare altre società nell'ambito di applicazione dei poteri pertinenti di cui alla legge del 2016 sui poteri di indagine ([145]), ma ha essenzialmente una funzione chiarificatrice.

(89) Infine la legge del 2024 sui poteri di indagine (modifica) ha introdotto alcune modifiche mirate alla procedura di emissione di mandati, anche per quanto riguarda le intercettazioni mirate e le ingerenze mirate in apparecchiature, ossia poteri che possono essere esercitati anche da specifiche autorità di contrasto nel Regno Unito al fine di prevenire o accertare reati gravi. Le modifiche riguardano solo la situazione specifica in cui tali poteri sono esercitati per ottenere comunicazioni o informazioni private in merito a una persona appartenente a un organo legislativo pertinente ([146]). Se da un lato i mandati relativi a intercettazioni mirate e a ingerenze in apparecchiature possono di norma essere emessi dal segretario di Stato e sono approvati da un commissario giudiziario [cfr. considerando da 186 a 196 e da 210 a 215 della decisione di esecuzione (UE) 2021/1772], le sezioni 26 e 111 della legge sui poteri di indagine esigono inoltre l'approvazione del primo ministro quando il mandato riguarda un membro del parlamento o un altro organo legislativo pertinente (la cosiddetta procedura «a tripla verifica»). La legge del 2024 sui poteri di indagine (modifica) prevede ora che il primo ministro possa nominare cinque segretari di Stato autorizzati a esercitare il potere di autorizzazione di tali mandati spettante al primo ministro, a condizione che l'autorizzazione sia urgente e che il primo ministro non sia in grado di provvedervi per motivi di salute o per mancanza di accesso a comunicazioni sicure. È importante sottolineare che restano in vigore le limitazioni e le garanzie riguardanti l'emissione di tali mandati, come descritte nei succitati considerando della decisione di esecuzione (UE) 2021/1772.

3.2.2. *Ulteriore utilizzo delle informazioni raccolte*

(90) La condivisione di dati da parte di un'autorità di contrasto con altre autorità per finalità diverse da quelle per le quali sono stati inizialmente raccolti (cosiddetta «condivisione successiva») è soggetta al rispetto delle condizioni esaminate nei considerando da 142 a 156 della decisione di esecuzione (UE) 2021/1772.

([142]) L'emissione di tali avvisi di conservazione a norma delle sezioni da 87 a 89 della legge del 2016 sui poteri di indagine mira a garantire che gli operatori di telecomunicazioni conservino, per un periodo massimo di 12 mesi, i dati relativi alle comunicazioni pertinenti che verrebbero altrimenti cancellati una volta non più necessari per finalità commerciali. I dati conservati devono rimanere disponibili per il periodo richiesto, qualora fosse successivamente necessario per un'autorità pubblica acquisirli ai sensi di un'autorizzazione per un'acquisizione mirata dei dati relativi alle comunicazioni di cui alla parte 3 della legge del 2016 sui poteri di indagine.

([143]) Sezione 94 A della legge del 2016 sui poteri di indagine, introdotta dalla sezione 20, paragrafo 4, della legge del 2024 sui poteri di indagine (modifica).

([144]) Sezione 261, paragrafo 10, lettera c), della legge del 2016 sui poteri di indagine, introdotta dalla sezione 19 della legge del 2024 sui poteri di indagine (modifica).

([145]) Note esplicative relative alla legge del 2024 sui poteri di indagine (modifica), paragrafo 359, disponibili al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2024/9/pdfs/ukpgaen_20240009_en.pdf.

([146]) Cfr. sezioni 26 e 111 della legge del 2016 sui poteri di indagine.

(91) Per quanto riguarda la situazione specifica dei trasferimenti successivi dal Regno Unito agli Stati Uniti, l'accordo UK-USA ([147]), concluso nell'ottobre 2019, è entrato in vigore ed è stato attuato dall'ottobre 2022. In conformità dell'accordo UK-USA, i dati trasferiti dall'UE a prestatori di servizi nel Regno Unito potrebbero essere soggetti a ordini di produzione di prove emessi dalle competenti autorità di contrasto statunitensi e resi applicabili nel Regno Unito.

(92) È importante sottolineare che continuano ad applicarsi le condizioni e le garanzie in base alle quali tali ordinanze possono essere emesse ed eseguite, come riconosciuto al considerando 154 della decisione di esecuzione (UE) 2021/1772. In particolare, i dati ottenuti ai sensi dell'accordo beneficiano di protezioni equivalenti alle garanzie specifiche previste dal cosiddetto «accordo quadro UE-USA» ([148]), che sono tutte integrate nell'accordo UK-USA mediante riferimento mutatis mutandis ([149]).

(93) Dopo l'adozione della decisione di esecuzione (UE) 2021/1772, il Regno Unito ha spiegato di aver chiarito, anche attraverso il dialogo con le parti pertinenti nel contesto dell'attuazione dell'accordo UK-USA, in quale modo le garanzie specifiche dell'accordo quadro concepite per un contesto di cooperazione tra autorità di contrasto sono adattate e applicate ai trasferimenti specifici contemplati dall'accordo UK-USA. In particolare, il Regno Unito ha spiegato che le disposizioni dell'accordo quadro che prevedono un ruolo per l'autorità competente pertinente (che non esiste in una situazione di cooperazione diretta tra un prestatore di servizi del Regno Unito e un'autorità di contrasto negli Stati Uniti) sono interpretate mutatis mutandis per fare riferimento all'autorità designata (quale definita nell'accordo UK-USA) ([150]) della parte interessata.

(94) Ad esempio, per quanto riguarda la notifica di un incidente relativo alla sicurezza delle informazioni a norma dell'articolo 10 dell'accordo quadro UE-USA, che esige una notifica all'autorità competente che trasferisce i dati, il Regno Unito ha spiegato che tale disposizione si applica mutatis mutandis, nel senso che la notifica dovrebbe essere effettuata all'autorità designata della parte da cui i dati sono stati trasferiti.

(95) Relativamente all'autorizzazione dell'autorità competente che trasferisce i dati prima di qualsiasi trasferimento successivo di informazioni personali a norma dell'articolo 7 dell'accordo quadro, il Regno Unito ha chiarito che applicherà tale disposizione mutatis mutandis, nel senso che l'autorità designata della parte che trasferisce i dati dovrà autorizzare qualsiasi trasferimento successivo.

(96) Per quanto riguarda gli obblighi di cui all'articolo 8 dell'accordo quadro sul mantenimento della qualità e dell'integrità delle informazioni, un'interpretazione mutatis mutandis della disposizione, in caso di problemi relativi alla qualità e all'integrità dei dati, attribuirebbe la responsabilità di mantenere i contatti con il fornitore che ha trasferito i dati all'autorità designata della parte destinataria.

([147]) 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, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

([148]) 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 (GU L 336 del 10.12.2016, pag. 3, ELI: http://data.europa.eu/eli/agree_internation/2016/2220/oj).

([149]) Articolo 9, paragrafo 1, dell'accordo.

([150]) A norma dell'articolo 1, paragrafo 8, dell'accordo UK-USA, per «autorità designata» si intende l'organismo governativo designato, per il Regno Unito, dal Secretary of State for the Home Department e, per gli Stati Uniti, dall'Attorney General.

(97) Per quanto riguarda il ricorso giurisdizionale, il Regno Unito ha sottolineato che i trasferimenti a norma dell'accordo UK-USA coinvolgeranno sempre l'autorità designata di ciascuna parte. Se gli Stati Uniti sono la parte destinataria dei dati trasferiti da fornitori di servizi del Regno Unito, il dipartimento della Giustizia degli Stati Uniti agirà in qualità di autorità designata. Pertanto, secondo l'interpretazione del Regno Unito, in ciascuna richiesta emessa sulla base dell'accordo UK-USA sarà coinvolto il dipartimento della Giustizia in qualità di autorità federale designata a norma della legge statunitense sul ricorso giurisdizionale e quindi il ricorso giurisdizionale può essere proposto nei confronti del dipartimento della Giustizia a norma dell'articolo 19 dell'accordo quadro. Inoltre il Regno Unito ha confermato ai servizi della Commissione che la legge sul ricorso giurisdizionale non è l'unico meccanismo di ricorso. A seconda delle circostanze e del contesto del caso specifico sono applicabili altre leggi statunitensi che prevedono modalità alternative di ricorso giurisdizionale.

3.2.3. *Vigilanza e mezzi di ricorso*

(98) A seconda dei poteri utilizzati dalle autorità competenti nel trattamento di dati personali per una finalità di contrasto (ai sensi della legge del 2018 sulla protezione dei dati o della legge del 2016 sui poteri di indagine), la vigilanza sul ricorso a tali poteri continua a essere esercitata da organismi diversi, come osservato nei considerando da 158 a 174 della decisione di esecuzione (UE) 2021/1772, e i meccanismi di ricorso continuano a essere disponibili a norma della parte 3 della legge del 2018 sulla protezione dei dati, della legge del 2016 sui poteri di indagine e della legge del 1998 sui diritti umani, come osservato nei considerando da 250 a 269 della decisione di esecuzione (UE) 2021/1772.

(99) Per quanto riguarda la vigilanza sulla parte 3 della legge del 2018 sulla protezione dei dati, le funzioni e i poteri dell'Information Commission sono analizzati nei considerando da 158 a 160 e 162 della decisione di esecuzione (UE) 2021/1772, fatte salve le modifiche introdotte dalla legge sull'accesso ai dati e sul loro utilizzo di cui alle sezioni 2.3.1 e 2.3.2 della presente decisione.

(100) Per quanto riguarda l'attuazione di tali poteri, dopo l'adozione della decisione di esecuzione (UE) 2021/1772 l'Information Commissioner ha trattato numerosi reclami ([151]), ha condotto diverse indagini e ha adottato misure di esecuzione in relazione al trattamento dei dati da parte delle autorità di contrasto. Tra il 2021 e il 2025 l'Information Commissioner ha condotto indagini e ha ammonito vari organi di polizia per diverse violazioni degli obblighi in materia di protezione dei dati commesse, ad esempio, nel rispondere a richieste di accesso ai dati, nel predisporre misure di sicurezza per i dati di videosorveglianza, nel trattare informazioni giudiziali penali sensibili, nel riunire dati di persone diverse o nel divulgare dati personali a terzi ([152]). L'Information Commissioner ha inoltre pubblicato orientamenti, pareri e documenti di orientamento, ad esempio sul diritto di accesso o su come trattare le richieste manifestamente infondate o eccessive a norma della parte 3 della legge del 2018 sulla protezione dei dati ([153]).

(101) Per quanto riguarda l'uso dei poteri di indagine ai sensi della legge del 2016 sui poteri di indagine, la vigilanza indipendente e giudiziaria continua ad essere assicurata dall'Investigatory Powers Commissioner (IPC), assistito da altri commissari giudiziari, che sono collettivamente denominati commissari giudiziari ([154]). In tale materia, la legge del 2024 sui poteri di indagine (modifiche) ha apportato solo modifiche limitate e mirate, che non incidono sull'indipendenza, sui compiti e sui poteri dei commissari giudiziari, ma sono volte a rafforzare il funzionamento pratico del regime di vigilanza vigente, in particolare introducendo i sostituti dell'Investigatory Powers Commissioner, ai quali quest'ultimo può delegare poteri specifici in caso di sua impossibilità o indisponibilità a svolgere le proprie funzioni. I sostituti dell'Investigatory Powers Commissioner devono essere commissari giudiziari e sono nominati dall'Investigatory Powers Commissioner stesso ([155]).

([151]) Ad esempio, nel periodo 2023-2024 l'Information Commission ha ricevuto 1 890 reclami sulla base del GDPR e/o della legge del 2018 sulla protezione dei dati, riguardanti organizzazioni rientranti nei sottosettori «autorità di polizia», «forze di polizia» e «Commissari di polizia». Cfr. anche *Information Commissioner's Annual Report and Financial Statements 2023/24*, disponibile al seguente indirizzo: https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf.

([152]) Ulteriori informazioni sono disponibili al seguente indirizzo: https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice.

([153]) Disponibili al seguente indirizzo: https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/ e https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

([154]) Cfr. considerando 250 della decisione di esecuzione (UE) 2021/1772.

([155]) Sezione 227 della legge del 2016 sui poteri di indagine, introdotta dalla sezione 7 della legge sui poteri di indagine (modifica).

3.3. **Importanti sviluppi riguardanti l'accesso e l'uso dei dati personali da parte delle autorità pubbliche del Regno Unito per motivi di sicurezza nazionale**

(102) Il quadro giuridico per l'esercizio dei poteri di indagine nel contesto della sicurezza nazionale continua ad essere costituito dalla legge del 2016 sui poteri di indagine. Oltre alle modifiche relative a poteri di indagine mirati che, a certe condizioni, possono essere esercitati anche da determinate autorità di contrasto, come descritto nei considerando da 77 a 85 della presente decisione, la legge del 2024 sui poteri di indagine (modifica) ha modificato anche uno dei poteri previsti dalla legge del 2016 sui poteri di indagine che possono essere esercitati in maniera massiva.

(103) Più specificamente, la legge del 2024 sui poteri di indagine (modifica) ha introdotto nella nuova parte 7 A della legge del 2016 sui poteri di indagine un regime specifico per la conservazione e l'esame di un sottogruppo specifico di serie massive di dati personali ([156]), vale a dire le serie di dati rispetto alle quali gli interessati non possono ragionevolmente attendersi la riservatezza se non, al massimo, in misura ridotta ([157]). Il fatto che una serie massiva di dati personali sia o meno parte di tale sottogruppo specifico di serie di dati è determinato dal capo di un servizio di intelligence sulla base di tutte le circostanze della fattispecie, in particolare i) la natura dei dati, ii) la misura in cui i dati sono stati resi pubblici dalle persone fisiche o le persone hanno acconsentito alla loro pubblicazione, iii) se i dati sono stati pubblicati, la misura in cui sono stati pubblicati sotto controllo editoriale o da una persona che agisce conformemente a norme professionali, iv) se i dati sono stati pubblicati o sono comunque di dominio pubblico, la misura in cui i dati sono ampiamente noti e v) la misura in cui i dati sono già stati impiegati in ambito pubblico ([158]).

(104) È importante sottolineare che per la conservazione e l'esame di serie massive di dati personali che non rientrano in questa categoria, ossia quelle che sono più sensibili e rispetto alle quali gli interessati possono ragionevolmente attendersi la riservatezza, rimane in vigore il regime valutato ai considerando 239 e 240 della decisione di esecuzione (UE) 2021/1772, in particolare la necessità di un mandato che sia approvato prima dal segretario di Stato e successivamente dal commissario giudiziario, fatti salvi i requisiti di necessità e proporzionalità della misura, come previsto dalla parte 7 della legge del 2016 sui poteri di indagine ([159]).

(105) La parte 7 A della legge del 2016 sui poteri di indagine prevede due tipi di autorizzazione: l'autorizzazione individuale e l'autorizzazione per categoria. La conservazione, o la conservazione e l'esame, di ogni serie massiva di dati personali detenuta a norma della parte 7 A devono essere autorizzati nell'ambito di una di tali autorizzazioni. Entrambe le autorizzazioni richiedono, in linea di principio ([160]), un'autorizzazione del capo del servizio di intelligence (o di una persona che agisce per suo conto) e l'approvazione di un commissario giudiziario indipendente ([161]). Un'autorizzazione individuale è concessa dal capo di un servizio di intelligence alle condizioni di cui alla sezione 226B, paragrafo 4, della legge del 2016 sui poteri di indagine e previa approvazione dei commissari giudiziari. Il commissario giudiziario deve esaminare le conclusioni della persona che ha concesso l'autorizzazione in relazione all'applicazione o meno della sezione 226 A, vale a dire l'assenza di un'aspettativa ragionevole di un obbligo di riservatezza se non, al massimo, in misura ridotta, alla serie massiva di dati descritta nell'autorizzazione ([162]).

([156]) I mandati relativi a serie massive di dati personali emessi a norma della sezione 200 della legge del 2016 sui poteri di indagine autorizzano le agenzie di intelligence a conservare ed esaminare serie di dati che contengono dati personali relativi a varie persone fisiche, la cui natura è tale per cui la maggior parte delle persone fisiche non presenta alcun interesse, né è probabile che lo presenti in futuro, per il servizio di intelligence nell'esercizio delle sue funzioni e che sono conservate elettronicamente da un servizio di intelligence ai fini di analisi nell'esercizio delle funzioni statutarie di tale servizio, cfr. anche la sezione 199 della legge del 2016 sui poteri di indagine.

([157]) Sezione 226 A, paragrafo 1, della legge del 2016 sui poteri di indagine, introdotta dalla sezione 2 della legge del 2024 sui poteri di indagine (modifica).

([158]) Sezione 226 A, paragrafo 3, della legge del 2016 sui poteri di indagine, introdotta dalla sezione 2 della legge del 2024 sui poteri di indagine (modifica).

([159]) La legge del 2024 sui poteri di indagine (modifica) ha modificato la sezione 213 della legge del 2016 sui poteri di indagine affinché i mandati relativi a serie massive di dati personali cessino di avere effetto 12 mesi dopo la loro emissione. In precedenza, tali mandati dovevano essere rinnovati ogni 6 mesi. Cfr. la sezione 3 della legge del 2024 sui poteri di indagine (modifica).

([160]) Un'autorizzazione individuale può essere concessa senza previa approvazione giudiziaria solo i) se la persona che concede l'autorizzazione individuale ritiene che la serie massiva di dati personali in questione rientri in un'autorizzazione per categoria esistente, o ii) per motivi d'urgenza (cfr. sezione 226B, paragrafo 6, della legge del 2016 sui poteri di indagine). In quest'ultimo caso, la decisione di concedere un'autorizzazione individuale urgente deve essere riesaminata da un commissario giudiziario entro tre giorni lavorativi dalla data di emissione (cfr. sezione 226BC della legge del 2016 sui poteri di indagine).

([161]) Sezione 226B, paragrafo 1, della legge del 2016 sui poteri di indagine, introdotta dalla sezione 2 della legge sui poteri di indagine (modifica).

([162]) Sezione 226BB, paragrafo 1, lettera a), della legge del 2016 sui poteri di indagine, introdotta dalla sezione 2 della legge del 2024 sui poteri di indagine (modifica).

(106) Un'autorizzazione per categoria autorizza la conservazione, o la conservazione e l'esame, di una categoria di serie massive di dati personali descritta nell'autorizzazione.

(107) La decisione di concedere l'autorizzazione per categoria è adottata dal capo del servizio di intelligence se ritiene che la sezione 226 A si applichi a qualsiasi serie di dati rientrante nella categoria e se la decisione di concedere l'autorizzazione è approvata da un commissario giudiziario indipendente ([163]). Quest'ultimo deve verificare se la sezione 226 A, ossia l'assenza di un'aspettativa ragionevole di un obbligo di riservatezza se non, al massimo, in misura ridotta, si applica a qualsiasi serie di dati rientrante nella categoria di serie di dati descritta nell'autorizzazione ([164]).

(108) È importante sottolineare che, in sede di approvazione di una decisione di concedere un'autorizzazione individuale o per categoria, il commissario giudiziario deve applicare i medesimi principi che sarebbero stati applicati da un organo giurisdizionale in relazione a una domanda di controllo giurisdizionale ([165]) e deve considerare tali questioni con un grado di diligenza sufficiente a garantire il rispetto degli obblighi imposti dalla sezione 2 della legge del 2016 sui poteri di indagine (obblighi generali in relazione alla tutela della vita privata) ([166]). Inoltre il rilascio di autorizzazioni è soggetto a una rigorosa vigilanza ex post, in particolare mediante le relazioni annuali al segretario di Stato e all'Intelligence and Security Committee (commissione per l'intelligence e la sicurezza) del parlamento ([167]) e mediante ispezioni periodiche dell'Ufficio dell'Investigatory Powers Commissioner ([168]).

(109) In termini di importanti sviluppi nell'ambito della vigilanza, l'Ufficio dell'Investigatory Powers Commissioner ha pubblicato le relazioni annuali per gli anni 2021, 2022 e 2023, che forniscono statistiche e informazioni dettagliate sull'utilizzo dei poteri di indagine da parte delle agenzie di intelligence e delle autorità di contrasto del Regno Unito ([169]). Le relazioni descrivono inoltre gli audit e le indagini dell'Ufficio e le relative risultanze, il che conferma che l'Investigatory Powers Commissioner continua a garantire la sua importantissima funzione di vigilanza nell'ambito del regime dei poteri di indagine del Regno Unito. Ad esempio, nel 2023 ha esaminato le giustificazioni relative alla necessità e alla proporzionalità dell'uso dei poteri di intercettazione massiva [come valutato nei considerando da 218 a 225 della decisione di esecuzione (UE) 2021/1772] da parte del Government Communications Headquarters, concludendo che una maggioranza significativa di dichiarazioni aveva una solida motivazione, mentre in alcuni casi la proporzionalità non era ben espressa. Tali risultanze sono state discusse con il Government Communications Headquarters Compliance Team, che si è impegnato a impartire un'ulteriore formazione di sensibilizzazione interna per risolvere la questione ([170]).

(110) Inoltre l'Investigatory Powers Tribunal ha pubblicato una relazione sulle sue attività e sulla sua giurisprudenza per il periodo dal 2021 al 2023 ([171]). Dalla relazione emerge che il numero di cause ricevute da tale organo è più che raddoppiato dal 2017, con oltre 400 cause ricevute nel 2023 ([172]). Le autorità di contrasto sono le principali

([163]) Sezione 226BA della legge del 2016 sui poteri di indagine, introdotta dalla sezione 2 della legge sui poteri di indagine (modifica).

([164]) Sezione 226BB, paragrafo 1, lettera b), della legge del 2016 sui poteri di indagine, introdotta dalla sezione 2 della legge sui poteri di indagine (modifica).

([165]) Sezione 226BB, paragrafo 2, lettera a), della legge del 2016 sui poteri di indagine, introdotta dalla sezione 2 della legge del 2024 sui poteri di indagine (modifica).

([166]) Sezione 226BB, paragrafo 2, lettera b), della legge del 2016 sui poteri di indagine, introdotta dalla sezione 2 della legge del 2024 sui poteri di indagine (modifica). In conformità ai doveri generali in relazione alla tutela della vita privata sanciti dalla sezione 2 della legge del 2016 sui poteri di indagine, un'autorità pubblica deve considerare a) se ciò che si intende conseguire tramite il mandato, l'autorizzazione o l'avviso potrebbe essere ragionevolmente conseguito con altri mezzi meno invasivi, b) se il livello di protezione da applicare in relazione a qualsiasi ottenimento di informazioni in virtù del mandato, dell'autorizzazione o dell'avviso sia più elevato in ragione della sensibilità particolare di tali informazioni, c) l'interesse pubblico per l'integrità e la sicurezza dei sistemi di telecomunicazione e dei servizi postali, nonché d) qualsiasi altro aspetto di interesse pubblico legato alla tutela della vita privata.

([167]) Sezioni 226DA e 226DB della legge del 2016 sui poteri di indagine, introdotte dalla sezione 2 della legge del 2024 sui poteri di indagine (modifica).

([168]) Cfr. la relazione annuale del 2023 dell'Investigatory Powers Commissioner, disponibile al seguente indirizzo: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf, pag. 3.

([169]) Le relazioni annuali sono disponibili al seguente indirizzo: https://www.ipco.org.uk/publications/annual-reports/.

([170]) Cfr. paragrafi da 6.39 a 6.43 della relazione annuale del 2023, disponibile al seguente indirizzo: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf.

([171]) Relazione dell'Investigatory Powers Tribunal 2021-2023, disponibile al seguente indirizzo: https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf.

([172]) Relazione dell'Investigatory Powers Tribunal 2021-2023, pag. 5.

destinatarie dei reclami, seguite da vicino dalle autorità di sicurezza e di intelligence ([173]). È importante sottolineare che, nel 2022 e nel 2023, l'Investigatory Powers Tribunal ha emesso sentenze nell'ambito di cause ricevute prima del 2021 in cui ha constatato che le autorità pubbliche del Regno Unito (rispettivamente il servizio di polizia della Scozia ([174]), il servizio di polizia del Greater Manchester ([175]), il servizio di polizia del Surrey ([176]), l'MI5 e il segretario di Stato per gli Affari interni ([177])) avevano agito illecitamente. In termini di mezzi di ricorso, l'Investigatory Powers Tribunal ha, tra l'altro, ordinato la distruzione di qualsiasi materiale ottenuto illecitamente e, in un caso, anche il pagamento di 12 000 GBP a titolo di equa soddisfazione per le violazioni individuate. La relazione annuale conferma pertanto che l'Investigatory Powers Tribunal svolge efficacemente il suo importante ruolo nel garantire la vigilanza e il ricorso nell'ambito dell'applicazione del diritto penale e dell'accesso ai dati personali ai fini della sicurezza nazionale.

(111) La relazione evidenza anche importanti sviluppi, tra cui una sentenza della Corte europea dei diritti dell'uomo in cui è stato stabilito che i singoli, in qualsiasi parte del mondo, possono presentare ricorso dinanzi all'Investigatory Powers Tribunal in merito al funzionamento del regime per l'intercettazione massiva del Regno Unito se l'atto in questione è stato posto in essere da un ente pubblico del Regno Unito e ha avuto luogo nel Regno Unito ([178]).

4. **CONCLUSIONI**

(112) La Commissione ritiene che il GDPR del Regno Unito e la legge del 2018 sulla protezione dei dati, come modificata dalla legge sull'accesso ai dati e sul loro utilizzo, continuino ad assicurare un livello di protezione dei dati personali trasferiti dall'Unione europea che è essenzialmente equivalente a quello garantito dal regolamento (UE) 2016/679.

(113) Inoltre la Commissione ritiene che, nel complesso, i meccanismi di vigilanza e i mezzi di ricorso previsti dal diritto del Regno Unito continuino a consentire di individuare e sanzionare nella pratica le violazioni e offrano all'interessato mezzi di ricorso che gli permettono di accedere ai dati personali che lo riguardano e, se del caso, di ottenerne la rettifica o la cancellazione.

(114) Infine, sulla base delle informazioni disponibili sull'ordinamento giuridico del Regno Unito, la Commissione ritiene che qualsiasi ingerenza nei diritti fondamentali delle persone fisiche i cui dati personali sono trasferiti dall'Unione europea verso il Regno Unito da parte di autorità pubbliche del Regno Unito per fini di interesse pubblico, in particolare per finalità di contrasto e di sicurezza nazionale, continui ad essere limitata a quanto strettamente necessario per conseguire l'obiettivo legittimo in questione; la Commissione ritiene inoltre che esista una protezione giuridica efficace contro tali ingerenze.

(115) Di conseguenza, in considerazione delle risultanze di cui alla presente decisione, è opportuno decidere che il Regno Unito continua ad assicurare un livello di protezione adeguato ai sensi dell'articolo 45 del regolamento (UE) 2016/679, interpretato alla luce della Carta dei diritti fondamentali dell'Unione europea.

(116) Questa conclusione si basa tanto sul regime interno pertinente del Regno Unito, quale sviluppatosi dopo l'adozione della decisione di esecuzione (UE) 2021/1772, quanto sugli impegni assunti dal Regno Unito a livello internazionale, in particolare la sua permanente adesione alla convenzione europea dei diritti dell'uomo e il permanente assoggettamento alla competenza giurisdizionale della Corte europea dei diritti dell'uomo. Il costante rispetto di tali obblighi internazionali costituisce pertanto un aspetto particolare importante della valutazione sulla quale si basa la presente decisione.

([173]) Relazione dell'Investigatory Powers Tribunal 2021-2023, pag. 12.
([174]) *Wilson v Police Scotland* [2022] UKIPTrib 5.
([175]) *Pendlebury v Greater Manchester Police* [2023] UKIPTrib 2.
([176]) *Hill v Metropolitan Police Service & Independent Office for Police Conduct* [2022] UKIPTrib 6.
([177]) *Liberty & Privacy International v Security Service and Secretary of State for the Home Department* [2023] UKIPTrib 1.
([178]) *Wieder and Guarnieri v UK*, [2023] CEDU 668, cfr. anche relazione dell'Investigatory Powers Tribunal 2021-2023, pag. 6.

5. **EFFETTI DELLA PRESENTE DECISIONE E AZIONE DELLE AUTORITÀ DI PROTEZIONE DEI DATI**

(117) Gli Stati membri e i loro organi sono tenuti ad adottare le misure necessarie per conformarsi agli atti delle istituzioni dell'Unione, poiché questi ultimi si presumono legittimi e producono pertanto effetti giuridici finché non scadano, non siano stati revocati o annullati nel contesto di un ricorso per annullamento ovvero dichiarati invalidi a seguito di un rinvio pregiudiziale o di un'eccezione di illegittimità.

(118) Di conseguenza, una decisione di adeguatezza adottata dalla Commissione a norma dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 è vincolante per tutti gli organi degli Stati membri che ne sono destinatari, comprese le autorità di controllo indipendenti. In particolare, durante il periodo di applicazione della decisione di esecuzione (UE) 2021/1772, quale modificata dalla presente decisione, i trasferimenti da un titolare del trattamento o un responsabile del trattamento nell'Unione europea verso titolari del trattamento o responsabili del trattamento nel Regno Unito possono avvenire senza la necessità di ottenere ulteriori autorizzazioni.

(119) È opportuno ricordare che, ai sensi dell'articolo 58, paragrafo 5, del regolamento (UE) 2016/679, e come spiegato dalla Corte di giustizia nella sentenza *Schrems I* ([179]), quando un'autorità nazionale di protezione dei dati mette in dubbio, anche in seguito a un reclamo, la compatibilità di una decisione di adeguatezza della Commissione con i diritti fondamentali della persona fisica concernenti la tutela della vita privata e la protezione dei dati, il diritto nazionale deve prevedere mezzi di ricorso che consentano di far valere tali obiezioni dinanzi a un organo giurisdizionale nazionale, che può essere tenuto a effettuare un rinvio pregiudiziale alla Corte di giustizia ([180]).

6. **MONITORAGGIO**

(120) Ai sensi dell'articolo 45, paragrafo 4, del regolamento (UE) 2016/679, la Commissione è tenuta a monitorare, su base continuativa, gli sviluppi pertinenti nel Regno Unito al fine di valutare se sia sempre assicurato un livello essenzialmente equivalente di protezione. Tale monitoraggio è particolarmente importante perché il Regno Unito applicherà e farà rispettare un regime modificato di protezione dei dati. Inoltre il quadro modificato del Regno Unito in materia di protezione dei dati conferisce al segretario di Stato il potere di specificare ulteriormente tale quadro mediante atti di diritto derivato. Occorre prestare particolare attenzione a tali specifiche supplementari nonché all'applicazione pratica delle norme modificate del Regno Unito sui trasferimenti di dati personali verso paesi terzi, all'efficacia dell'esercizio dei diritti individuali, compresi eventuali sviluppi pertinenti del diritto e delle prassi riguardanti le nuove eccezioni o limitazioni a tali diritti, al funzionamento dell'ICO ristrutturato, anche per quanto riguarda la gestione dei reclami e l'applicazione dei poteri correttivi, nonché al rispetto delle limitazioni e delle garanzie per quanto riguarda l'accesso da parte delle pubbliche amministrazioni, in particolare per quanto riguarda la nuova parte 7 A della legge del 2016 sui poteri di indagine. Assieme ad altri elementi, gli sviluppi giurisprudenziali e la vigilanza da parte dell'ICO e di altri organismi indipendenti dovrebbero contribuire al monitoraggio della Commissione.

(121) Per agevolare tale monitoraggio, le autorità del Regno Unito dovrebbero informare tempestivamente la Commissione di qualsiasi modifica sostanziale dell'ordinamento giuridico del Regno Unito che abbia un impatto sul quadro giuridico oggetto della decisione di esecuzione (UE) 2021/1772, come modificata dalla presente decisione, nonché di qualsiasi evoluzione delle pratiche relative al trattamento dei dati personali oggetto della decisione di esecuzione (UE) 2021/1772, come modificata dalla presente decisione, per quanto riguarda sia il trattamento dei dati personali da parte dei titolari del trattamento e dei responsabili del trattamento ai sensi del GDPR del Regno Unito, sia le limitazioni e le garanzie applicabili all'accesso ai dati personali da parte delle autorità pubbliche. Ciò dovrebbe includere gli sviluppi relativi agli elementi di cui al considerando (120).

(122) Inoltre, al fine di consentire alla Commissione di svolgere in modo efficace la propria funzione di monitoraggio, gli Stati membri dovrebbero informarla delle eventuali azioni intraprese dalle autorità nazionali di protezione dei dati, in particolare per quanto riguarda eventuali domande o reclami presentati da interessati dell'UE relativamente al trasferimento di dati personali dall'Unione europea verso titolari del trattamento o responsabili del trattamento nel Regno Unito. La Commissione dovrebbe inoltre essere informata di eventuali indicazioni del fatto che le azioni delle autorità pubbliche del Regno Unito responsabili della prevenzione, dell'indagine, dell'accertamento o del perseguimento dei reati ovvero della sicurezza nazionale, compresi gli organismi di vigilanza, non garantiscono il necessario livello di protezione.

([179]) *Schrems I*, punto 65.

([180]) *Schrems I*, punto 65: «A tal riguardo, incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione».

(123) Se dalle informazioni disponibili, in particolare da quelle risultanti dal monitoraggio della decisione di esecuzione (UE) 2021/1772, come modificata dalla presente decisione, o fornite dalle autorità del Regno Unito o degli Stati membri, risulta che il livello di protezione offerto dal Regno Unito potrebbe non essere più adeguato, la Commissione dovrebbe informare prontamente le autorità competenti del Regno Unito e richiedere che adottino misure adeguate entro un periodo di tempo specificato, che non può essere superiore a tre mesi. Se necessario, tale periodo può essere prorogato per un periodo di tempo determinato, tenuto conto della natura della questione in esame e/o delle misure da adottare. Ad esempio, tale procedura sarebbe avviata nei casi in cui i trasferimenti successivi, anche sulla base di nuovi regolamenti di adeguatezza adottati dal segretario di Stato o di accordi internazionali conclusi dal Regno Unito, non sarebbero più effettuati nel quadro di garanzie che assicurino la continuità della protezione ai sensi dell'articolo 44 del regolamento (UE) 2016/679.

(124) Laddove alla scadenza di tale periodo di tempo specificato le autorità competenti del Regno Unito non abbiano adottato tali misure o non dimostrino altrimenti in modo soddisfacente che la presente decisione continua ad essere basata su un livello di protezione adeguato, la Commissione avvierà la procedura di cui all'articolo 93, paragrafo 2, del regolamento (UE) 2016/679 al fine di sospendere o abrogare parzialmente o completamente la presente decisione.

(125) In alternativa, la Commissione avvierà tale procedura al fine di modificare la presente decisione, in particolare imponendo ulteriori condizioni per i trasferimenti di dati o limitando il riconoscimento dell'adeguatezza soltanto ai trasferimenti di dati per cui continua ad essere garantito un livello di protezione adeguato.

(126) In ragione di motivi imperativi d'urgenza debitamente giustificati, la Commissione farà ricorso alla possibilità di adottare, conformemente alla procedura di cui all'articolo 93, paragrafo 3, del regolamento (UE) 2016/679, atti di esecuzione immediatamente applicabili destinati a sospendere, abrogare o modificare la presente decisione.

7. **RIESAME, DURATA E RINNOVO DELLA PRESENTE DECISIONE**

(127) In applicazione dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 e alla luce del fatto che il livello di protezione assicurato dal quadro giuridico del Regno Unito può evolversi, la Commissione, successivamente all'adozione della presente decisione, dovrebbe riesaminare periodicamente se le constatazioni relative al livello di protezione assicurato dal Regno Unito continuino ad essere giustificate in fatto e in diritto, tenendo conto degli elementi di cui all'articolo 45, paragrafo 2, del regolamento (UE) 2016/679. Tali valutazioni dovrebbero aver luogo almeno ogni quattro anni e dovrebbero riguardare tutti gli aspetti del funzionamento della presente decisione, compreso il funzionamento dei pertinenti meccanismi di controllo e applicazione.

(128) Per effettuare il riesame, la Commissione dovrebbe incontrare i rappresentanti pertinenti delle autorità britanniche, compresa l'Information Commission. A tale riunione dovrebbero poter partecipare i rappresentanti dei membri del comitato europeo per la protezione dei dati. Nel quadro del riesame la Commissione dovrebbe chiedere al Regno Unito di fornire informazioni complete su tutti gli aspetti pertinenti alla constatazione di adeguatezza. La Commissione dovrebbe inoltre chiedere delucidazioni in merito a qualsiasi informazione ricevuta risultata pertinente ai fini della presente decisione, compreso dall'EDPB, dalle singole autorità di protezione dei dati e dai gruppi della società civile, da relazioni pubbliche o dalle notizie diffuse dai mezzi di comunicazione o da qualsiasi altra fonte di informazioni disponibile.

(129) La Commissione dovrebbe elaborare, sulla base del riesame, una relazione pubblica da presentare al Parlamento europeo e al Consiglio.

(130) La Commissione deve anche tenere conto del fatto che il quadro in materia di protezione dei dati valutato nella presente decisione e nella decisione di esecuzione (UE) 2021/1772 può evolvere ulteriormente.

(131) Di conseguenza è opportuno prevedere che la presente decisione si applichi per un periodo di sei anni a decorrere dalla sua entrata in vigore.

(132) Laddove in particolare le informazioni risultanti dal monitoraggio della presente decisione rivelino che le conclusioni sull'adeguatezza del livello di protezione assicurato nel Regno Unito continuano ad essere giustificate in fatto e in diritto, la Commissione dovrebbe, al più tardi sei mesi prima della data in cui la presente decisione cesserà di applicarsi, avviare la procedura per modificare la presente decisione prorogandone l'applicazione temporale, in linea di principio, per un ulteriore periodo di quattro anni. Qualsiasi atto di esecuzione di tale sorta destinato a modificare la presente decisione deve essere adottato conformemente alla procedura di cui all'articolo 93, paragrafo 2, del regolamento (UE) 2016/679.

8. **CONSIDERAZIONI FINALI**

(133) Il comitato europeo per la protezione dei dati ha pubblicato un parere ([181]), del quale si è tenuto conto nell'elaborazione della presente decisione.

(134) La misura di cui alla presente decisione è conforme al parere del comitato istituito a norma dell'articolo 93 del regolamento (UE) 2016/679.

(135) È pertanto opportuno modificare di conseguenza la decisione di esecuzione (UE) 2021/1772,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

L'articolo 1, paragrafo 2, della decisione di esecuzione (UE) 2021/1772 è abrogato.

Articolo 2

L'articolo 4 della decisione di esecuzione (UE) 2021/1772 è sostituito dal seguente:

«*Articolo 4*

La presente decisione scade il 27 dicembre 2031, a meno che non sia prorogata secondo la procedura di cui all'articolo 93, paragrafo 2, del regolamento (UE) 2016/679.».

Articolo 3

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 19 dicembre 2025

Per la Commissione
Michael MCGRATH
Membro della Commissione

([181]) Parere 26/2025 relativo al progetto di decisione di esecuzione della Commissione europea ai sensi del regolamento (UE) 2016/679 sull'adeguata protezione dei dati personali da parte del Regno Unito, disponibile al seguente indirizzo: https://www.edpb.europa.eu/system/files/2025-10/edpb_opinion_202526_united_kingdom_adequacy_gdpr_en.pdf.