II

(Atti non legislativi)

DECISIONI

REGOLAMENTO 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

[notificata con il numero C(2021) 4800]

(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) Il regolamento (UE) 2016/679 stabilisce le norme per il trasferimento di dati personali da titolari del trattamento o responsabili del trattamento nell'Unione verso paesi terzi e organizzazioni internazionali nella misura in cui tale trasferimento rientri nel suo ambito di applicazione. Le norme sui trasferimenti internazionali di dati sono stabilite nel capo V di detto regolamento, ossia negli articoli da 44 a 50. Sebbene la circolazione di dati personali verso e da paesi al di fuori dell'Unione europea sia essenziale per l'espansione della cooperazione internazionale e degli scambi transfrontalieri, occorre garantire che il livello di protezione offerto ai dati personali nell'Unione europea non sia compromesso da trasferimenti verso paesi terzi ([2]).

(2) Ai sensi dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 la Commissione può decidere, mediante atti di esecuzione, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato. Nel rispetto di tale condizione, i trasferimenti di dati personali verso un paese terzo possono avvenire senza la necessità di ottenere ulteriori autorizzazioni, come previsto dall'articolo 45, paragrafo 1, e dal considerando 103 di tale regolamento.

(3) Come specificato all'articolo 45, paragrafo 2, del regolamento (UE) 2016/679, l'adozione della decisione di adeguatezza deve basarsi su un'analisi completa dell'ordinamento giuridico del paese terzo, per quanto riguarda tanto le norme applicabili agli importatori di dati quanto le limitazioni e le garanzie relative all'accesso ai dati personali da parte delle autorità pubbliche. Nella propria valutazione la Commissione deve stabilire se il paese terzo in questione assicura un livello di protezione «sostanzialmente equivalente» a quello garantito all'interno dell'Unione europea (considerando 104 del regolamento (UE) 2016/679). Il criterio rispetto al quale viene valutata l'«equivalenza sostanziale» è quello stabilito dalla legislazione dell'UE, in particolare il regolamento (UE) 2016/679, nonché dalla giurisprudenza della Corte di giustizia dell'Unione europea ([3]). Anche i criteri di riferimento per l'adeguatezza del comitato europeo per la protezione dei dati (EDPB) sono rilevanti a questo proposito ([4]).

([1]) GU L 119 del 4.5.2016, pag. 1.

([2]) Cfr. considerando 101 del regolamento (UE) 2016/679.

([3]) Cfr., più di recente, la sentenza della Corte di giustizia del 16 luglio 2020, *Facebook Ireland e Schrems* («*Schrems II*»), C-311/18, ECLI:EU:C:2020:559.

([4]) Comitato europeo per la protezione dei dati, Criteri di riferimento per l'adeguatezza, WP 254 rev. 01, disponibile al seguente indirizzo: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Come chiarito dalla Corte di giustizia dell'Unione europea, non è richiesto un livello di protezione identico ([5]). 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 ([6]). 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 estero, nel suo insieme, offre il necessario livello di protezione ([7]).

(5) La Commissione ha analizzato attentamente la normativa e la prassi del Regno Unito. Sulla base delle risultanze illustrate nei considerando da 8 a 270, la Commissione conclude che il Regno Unito assicura un livello di protezione adeguato per i dati personali trasferiti dall'Unione europea verso il Regno Unito nell'ambito di applicazione del regolamento (UE) 2016/679.

(6) Questa conclusione non riguarda i 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 a fini di mantenimento dell'effettivo controllo dell'immigrazione («esenzione per motivi di immigrazione») a norma dell'allegato 2, paragrafo 4, punto 1, della legge del 2018 sulla protezione dei dati. La validità e l'interpretazione dell'esenzione per motivi di immigrazione ai sensi del diritto del Regno Unito non sono stabilite, a seguito di una decisione della Corte d'appello di Inghilterra e Galles del 26 maggio 2021. Pur riconoscendo che i diritti degli interessati possono, in linea di principio, essere limitati a fini di controllo dell'immigrazione quale «aspetto importante dell'interesse pubblico», la Corte d'appello ha ritenuto che l'esenzione per motivi di immigrazione, nella sua forma attuale, è incompatibile con il diritto del Regno Unito, in quanto la misura legislativa non contiene disposizioni specifiche che prevedono le garanzie elencate all'articolo 23, paragrafo 2, del regolamento generale sulla protezione dei dati del Regno Unito (in appresso «GDPR del Regno Unito») ([8]). In tali condizioni, i trasferimenti di dati personali dall'Unione verso il Regno Unito ai quali può applicarsi l'esenzione per motivi di immigrazione dovrebbero essere esclusi dall'ambito di applicazione della presente decisione ([9]). Una volta posto rimedio all'incompatibilità con il diritto del Regno Unito, l'esenzione per motivi di immigrazione dovrebbe essere riesaminata, come pure la necessità di mantenere la limitazione dell'ambito di applicazione della presente decisione.

(7) La presente decisione non dovrebbe incidere sull'applicazione diretta del regolamento (UE) 2016/679 alle organizzazioni stabilite nel Regno Unito qualora siano soddisfatte le condizioni relative all'ambito di applicazione territoriale di tale regolamento, di cui all'articolo 3 dello stesso.

2. NORME CHE SI APPLICANO AL TRATTAMENTO DI DATI PERSONALI

2.1. Il quadro costituzionale

(8) Il Regno Unito è una democrazia parlamentare che ha un sovrano costituzionale come capo di Stato. Dispone di un parlamento sovrano che costituisce l'autorità suprema rispetto a tutte le altre istituzioni pubbliche, di un potere esecutivo designato dal parlamento e responsabile di fronte a quest'ultimo, e di un potere giudiziario indipendente. Il potere esecutivo deriva la propria autorità dalla propria capacità di ottenere la fiducia della *House of Commons* (Camera dei Comuni) eletta, e risponde a entrambe le camere del parlamento competenti per l'esame dell'operato del governo nonché per la discussione e l'emanazione di leggi.

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

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

([7]) 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.

([8]) Corte d'appello (Sezione civile), *Open Rights Group v Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport,* [2021] EWCA Civ 800, punti da 53 a 56. La Corte d'appello ha riformato la decisione della *High Court of Justice* che aveva precedentemente valutato l'esenzione alla luce del regolamento (UE) 2016/679 (in particolare dell'articolo 23) e della Carta dei diritti fondamentali dell'Unione europea e che aveva dichiarato legittima l'esenzione (*Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor* [2019] EWHC 2562).

([9]) Purché siano soddisfatte le condizioni applicabili, i trasferimenti a fini di controllo dell'immigrazione da parte del Regno Unito possono essere effettuati sulla base dei meccanismi di trasferimento di cui agli articoli da 46 a 49 del regolamento (UE) 2016/679.

(9) Il parlamento del Regno Unito ha delegato al parlamento scozzese, al parlamento gallese (*Senedd Cymru*) e all'assemblea dell'Irlanda del Nord il potere di legiferare, rispettivamente in Scozia, Galles e Irlanda del Nord, in materie interne che il parlamento del Regno Unito non ha riservato a sé stesso. Sebbene la protezione dei dati sia una materia di competenza del governo centrale, il che significa che la medesima legislazione si applica in tutto il paese, la regolamentazione di altri settori politici pertinenti per la presente decisione è stata delegata. Ad esempio i sistemi di giustizia penale, comprese le attività di polizia di Scozia e Irlanda del Nord, sono soggetti rispettivamente alla competenza del parlamento scozzese e dell'assemblea dell'Irlanda del Nord. Il Regno Unito non dispone di una costituzione codificata nel senso di un documento costitutivo attestato. I principi costituzionali si sono affermati nel corso del tempo, tratti in particolare dalla giurisprudenza e dalla convenzione. Il valore costituzionale di taluni statuti, quali la Magna Carta, il *Bill of Rights 1689* e la *Human Rights Act 1998* (legge del 1998 sui diritti umani), è stato riconosciuto dagli organi giurisdizionali. I diritti fondamentali delle persone fisiche sono stati sviluppati, come parte della costituzione, attraverso la «*common law*» (diritto giurisprudenziale), gli statuti corrispondenti e i trattati internazionali, in particolare la convenzione europea dei diritti dell'uomo che il Regno Unito ha ratificato nel 1951. Nel 1987 il Regno Unito ha ratificato altresì la convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (convenzione 108) ([10]).

(10) La legge del 1998 sui diritti umani integra nel diritto del Regno Unito i diritti sanciti dalla convenzione europea dei diritti dell'uomo (CEDU). Tale legge accorda a qualsiasi persona fisica i diritti e le libertà fondamentali di cui agli articoli da 2 a 12 e 14 CEDU, 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 CEDU. Tra di essi è compreso il diritto al rispetto della vita privata e familiare (così come il diritto alla protezione dei dati rientrante in tale diritto) e il diritto a un equo processo ([11]). In particolare, conformemente all'articolo 8 di tale convenzione, può esservi ingerenza da parte di un'autorità pubblica in relazione al diritto alla tutela della vita privata conformemente alla legge soltanto laddove ciò costituisca in una società democratica una misura necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

(11) Conformemente alla legge del 1998 sui diritti umani, qualsiasi azione delle autorità pubbliche deve essere compatibile con un diritto sancito da tale convenzione ([12]). Inoltre la legislazione primaria e quella subordinata vanno lette e attuate in maniera compatibile con i diritti sanciti da tale convenzione ([13]).

2.2. **Il quadro del Regno Unito in materia di protezione dei dati**

(12) Il Regno Unito ha receduto dall'Unione europea il 31 gennaio 2020. In base all'accordo sul recesso del Regno Unito di Gran Bretagna e Irlanda del Nord dall'Unione europea e dalla Comunità europea dell'energia atomica ([14]), il diritto dell'Unione ha continuato ad applicarsi nel Regno Unito durante il periodo di transizione, fino al 31 dicembre 2020. Prima del recesso e durante il periodo di transizione, il quadro normativo in materia di protezione dei dati personali nel Regno Unito era costituito dalla legislazione UE pertinente (in particolare il regolamento (UE) 2016/679 e la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio ([15])) e dalla legislazione nazionale, in particolare la *Data Protection Act 2018* ([16]) (legge del 2018 sulla protezione dei dati) che ha fissato norme nazionali, ove consentito dal regolamento (UE) 2016/679, specificando e limitando l'applicazione delle norme del regolamento (UE) 2016/679, e recepito la direttiva (UE) 2016/680.

([10]) I principi della convenzione 108 sono stati originariamente attuati nel diritto del Regno Unito attraverso la legge del 1984 sulla protezione dei dati, sostituita dalla legge del 1998 sulla protezione dei dati, la quale è stata successivamente a sua volta sostituita dalla legge del 2018 sulla protezione dei dati (letta in combinato disposto con il GDPR del Regno Unito). Nel 2018 il Regno Unito ha inoltre firmato il protocollo che modifica la convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (nota come convenzione 108+) e sta attualmente lavorando alla ratifica della convenzione.

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

([12]) Sezione 6 della legge del 1998 sui diritti umani.

([13]) Sezione 3 della legge del 1998 sui diritti umani.

([14]) Accordo sul recesso del Regno Unito di Gran Bretagna e Irlanda del Nord dall'Unione europea e dalla Comunità europea dell'energia atomica, 2019/C 384 I/01, XT/21054/2019/INIT (GU C 384I del 12.11.2019, pag. 1), disponibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/ITN/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=IT.

([15]) 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), disponibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L0680&from=IT.

([16]) Legge del 2018 sulla protezione dei dati, disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(13) In preparazione al recesso dall'Unione europea, il governo del Regno Unito ha emanato la *European Union (Withdrawal) Act 2018* ([17]) (legge del 2018 relativa al recesso dall'Unione europea), che incorpora la legislazione dell'Unione direttamente applicabile nel diritto del Regno Unito ([18]). Tale cosiddetto «diritto dell'Unione mantenuto» comprende il regolamento (UE) 2016/679 nella sua interezza (compresi i suoi considerando) ([19]). Conformemente a tale atto, il diritto dell'Unione mantenuto senza modifiche deve essere interpretato dagli organi giurisdizionali del Regno Unito in conformità con la relativa 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») ([20]).

(14) Ai sensi della legge del 2018 relativa al recesso dall'Unione europea, i ministri del Regno Unito hanno il potere di introdurre diritto derivato, tramite strumenti legislativi, al fine di apportare le modifiche necessarie al diritto dell'Unione mantenuto in conseguenza del recesso del Regno Unito dall'Unione europea. Essi hanno esercitato tale potere adottando i *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019* (regolamenti DPPEC) ([21]). 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 ([22]).

(15) Di conseguenza il quadro giuridico in materia di protezione dei dati personali del Regno Unito dopo la fine del periodo di transizione è costituito:

— dal GDPR del Regno Unito, incorporato nel diritto del Regno Unito ai sensi della legge del 2018 relativa al recesso dall'Unione europea e modificato dai regolamenti DPPEC ([23]); e

— dalla legge del 2018 sulla protezione dei dati ([24]), come modificata dai regolamenti DPPEC.

(16) Dato che il GDPR del Regno Unito si basa sulla legislazione dell'UE, le norme in materia di protezione dei dati nel Regno Unito in molti aspetti rispecchiano da vicino le norme corrispondenti applicabili all'interno dell'Unione europea.

(17) Oltre ai poteri conferiti al segretario di Stato dalla legge del 2018 relativa al recesso dall'Unione europea, diverse disposizioni della legge del 2018 sulla protezione dei dati conferiscono al segretario di Stato poteri per adottare diritto derivato per modificare talune disposizioni di detta legge o prevedere norme supplementari e aggiuntive ([25]).

([17]) *European Union (Withdrawal) Act 2018* (legge del 2018 relativa al recesso dall'Unione europea), disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2018/16/contents.

([18]) L'intenzione e l'effetto della legge del 2018 relativa al recesso dall'Unione europea prevedono che tutta la legislazione diretta dell'Unione che è stata incorporata nel diritto del Regno Unito alla fine del periodo di transizione sia incorporata nel diritto del Regno Unito come ha effetto nel diritto dell'UE immediatamente prima della fine del periodo di transizione, cfr. sezione 3 della legge del 2018 relativa al recesso dall'Unione europea.

([19]) Le note esplicative sulla legge del 2018 relativa al recesso dall'Unione europea specificano che: «Qualora la legislazione sia convertita ai sensi della presente sezione, il testo stesso della legislazione farà parte integrante della legislazione interna. Rientrerà in tale contesto il testo completo di qualsiasi strumento dell'UE (compresi i suoi considerando)». Note esplicative sulla legge del 2018 relativa al recesso dall'Unione europea, punto 83, disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Secondo le informazioni fornite dalle autorità del Regno Unito, dato che i considerando non godono dello status di norme giuridiche vincolanti, non è stato necessario modificarli nello stesso modo in cui gli articoli del regolamento (UE) 2016/679 sono stati modificati dai regolamenti DPPEC.

([20]) Sezione 6 della legge del 2018 relativa al recesso dall'Unione europea.

([21]) *The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019* (regolamenti del 2019 in materia di protezione dei dati, tutela della vita privata e comunicazioni elettroniche (modifiche, ecc.) (uscita dall'UE)), disponibili al seguente indirizzo: https://www.legislation.gov.uk/uksi/2019/419/contents/made, come modificati dai regolamenti DPPEC 2020, disponibili al seguente indirizzo: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([22]) Tali modifiche del GDPR del Regno Unito e alla legge del 2018 sulla protezione dei dati hanno per lo più di natura tecnica, come nel caso dell'eliminazione dei riferimenti a «Stati membri» o di adeguamenti della terminologia, ad esempio sostituendo i riferimenti al regolamento (UE) 2016/679 con riferimenti al GDPR del Regno Unito. In alcuni casi le modifiche si sono rese necessarie per rispecchiare il contesto puramente interno delle disposizioni, ad esempio, in relazione al «soggetto» che adotta i «regolamenti di adeguatezza» ai fini del quadro normativo del Regno Unito in materia di protezione dei dati (cfr. sezione 17A della legge del 2018 sulla protezione dei dati), ossia il segretario di Stato anziché la Commissione europea.

([23]) *General Data Protection Regulation, Keeling Schedule*, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([24]) *Data Protection Act 2018, Keeling Schedule*, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([25]) Tali poteri sono sanciti ad esempio dalla sezione 16 (potere di concedere, in situazioni specifiche e rigorosamente circoscritte, ulteriori esenzioni rispetto a disposizioni specifiche del GDPR del Regno Unito), dalla sezione 17A (potere di adottare regolamenti di adeguatezza), dagli articoli 212 e 213 (poteri di avviare il processo legislativo ed adottare disposizioni transitorie) e dalla sezione 211 (potere di apportare modifiche minori e consequenziali) della legge del 2018 sulla protezione dei dati.

Finora il segretario di Stato ha esercitato il potere conferitogli dalla sezione 137 della legge del 2018 sulla protezione dei dati soltanto per adottare i *Data Protection (Charges and Information) (Amendment) Regulations 2019* (regolamenti del 2019 in materia di protezione dei dati (contributi spese e informazioni) (modifica)), che stabiliscono le circostanze nelle quali i titolari del trattamento sono tenuti a versare un contributo spese annuo all'autorità di protezione dei dati indipendente del Regno Unito, ossia l'*Information Commissioner*.

(18) Infine ulteriori orientamenti sulla legislazione in materia di protezione dei dati del Regno Unito sono forniti nei codici di pratica e in altri orientamenti adottati dall'*Information Commissioner*. Sebbene non siano formalmente giuridicamente vincolanti, tali orientamenti hanno valenza interpretativa e dimostrano come l'*Information Commissioner* applica e fa rispettare la legislazione in materia di protezione dei dati nella pratica. In particolare, gli articoli da 121 a 125 della legge del 2018 sulla protezione dei dati impongono all'*Information Commissioner* di preparare i codici di pratica in materia di condivisione di dati, marketing diretto, progettazione adeguata all'età, protezione dei dati e giornalismo.

(19) In termini di struttura e componenti principali, il quadro giuridico del Regno Unito che si applica ai dati trasferiti nell'ambito della presente decisione è quindi molto simile a quello che si applica nell'Unione europea. Tale quadro non si basa soltanto sugli obblighi stabiliti dal diritto interno che sono stati modellati dal diritto dell'Unione, ma anche sugli obblighi sanciti dal diritto internazionale, in particolare attraverso l'adesione da parte del Regno Unito alla CEDU e alla convenzione 108, nonché il suo assoggettamento alla competenza giurisdizionale della Corte europea dei diritti dell'uomo. Tali obblighi derivanti da strumenti internazionali giuridicamente vincolanti, riguardanti in particolare la protezione dei dati personali, costituiscono pertanto un elemento di particolare importanza del quadro giuridico valutato nella presente decisione.

2.3. **Ambito di applicazione materiale e territoriale**

(20) Analogamente al regolamento (UE) 2016/679, il GDPR del Regno Unito si applica al trattamento di dati personali svolto interamente o in parte ricorrendo a mezzi automatizzati, o ad altri trattamenti, se i dati personali costituiscono parte di un sistema di archiviazione ([26]). Le definizioni di «dati personali», «interessato» e «trattamento» di cui al GDPR del Regno Unito sono identiche a quelle del regolamento (UE) 2016/679 ([27]). Inoltre il GDPR del Regno Unito si applica al trattamento manuale e non strutturato di dati personali ([28]) detenuti da talune autorità pubbliche del Regno Unito ([29]), sebbene i principi e i diritti del GDPR del Regno Unito che non sono pertinenti per tali dati personali non vengano applicati ai sensi degli articoli 24 e 25 della legge del 2018 sulla protezione dei dati. Analogamente a quanto previsto dal regolamento (UE) 2016/679, il GDPR del Regno Unito non si applica al trattamento di dati personali da parte di una persona fisica nel contesto di un'attività puramente personale o domestica ([30]).

(21) Il GDPR del Regno Unito estende il proprio ambito di applicazione anche al trattamento nel corso di un'attività che, immediatamente prima della fine del periodo di transizione, ricadeva al di fuori dell'ambito di applicazione del diritto dell'Unione europea (ad esempio sicurezza nazionale) ([31]) oppure rientrava nell'ambito di applicazione del titolo 5, capo 2, del trattato sull'Unione europea (attività relative alla politica estera e di sicurezza comune) ([32]). Come nel sistema in vigore nell'Unione europea, il GDPR del Regno Unito non si applica al trattamento di dati personali da parte di un'autorità competente per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, compresa la salvaguardia contro, e la prevenzione di, minacce alla sicurezza

([26]) Articolo 2, paragrafi 1 e 5, del GDPR del Regno Unito.

([27]) Articolo 4, paragrafi 1 e 2, del GDPR del Regno Unito.

([28]) Il trattamento manuale non strutturato di dati personali è definito all'articolo 2, paragrafo 5, lettera b), come il trattamento di dati personali che non è un trattamento automatizzato o strutturato di dati personali.

([29]) L'articolo 2, paragrafo 1A, del GDPR del Regno Unito prevede che il regolamento si applichi anche al trattamento manuale non strutturato di dati personali detenuti da un'autorità pubblica del settore della libertà di informazione. Il riferimento alle autorità pubbliche del settore della libertà di informazione riguarda le autorità pubbliche come definite nella *Freedom of Information Act 2000* (legge del 2000 sulla libertà di informazione) o le autorità pubbliche scozzesi come definite nella *Freedom of Information (Scotland) Act 2002 (asp 13)* (legge del 2002 sulla libertà di informazione — Scozia). Sezione 21, paragrafo 5, della legge del 2018 sulla protezione dei dati.

([30]) Articolo 2, paragrafo 2, lettera a), del GDPR del Regno Unito.

([31]) Le attività di sicurezza nazionale rientrano nell'ambito di applicazione del GDPR del Regno Unito soltanto nella misura in cui non sono svolte da un'autorità competente per finalità di contrasto, nel qual caso si applica la parte 3 della legge del 2018 sulla protezione dei dati, o da o per conto di un servizio di intelligence, le cui attività sono escluse dall'ambito di applicazione del GDPR del Regno Unito e soggette alla parte 4 della legge del 2018 sulla protezione dei dati ai sensi dell'articolo 2, paragrafo 2, lettera c), del GDPR del Regno Unito. Ad esempio una forza di polizia può condurre verifiche di sicurezza nei confronti di un dipendente per garantire che possa essere considerato affidabile ai fini dell'accesso a materiale di sicurezza nazionale. Nonostante le forze di polizia siano un'autorità competente per finalità di contrasto, il trattamento in questione non avviene per tali finalità e si applicherebbe quindi il GDPR del Regno Unito. Cfr. Regno Unito, *Explanatory Framework for Adequacy Discussions, section H: National Security Data Protection and Investigatory Powers Framework*, pagina 8, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf.

([32]) Articolo 2, paragrafo 1, lettere a) e b), del GDPR del Regno Unito.

pubblica (cosiddette «finalità di contrasto») (tale trattamento è invece disciplinato dalla parte 3 della legge del 2018 sulla protezione dei dati, come avviene per la direttiva (UE) 2016/680 ai sensi del diritto dell'Unione europea) né al trattamento di dati personali da parte dei servizi di intelligence (il *Security Service*, il *Secret Intelligence Service* e il *Government Communications Headquarters*) che rientra nell'ambito di applicazione della parte 4 della legge del 2018 sulla protezione dei dati ([33]).

(22) L'ambito di applicazione territoriale del GDPR del Regno Unito è specificato all'articolo 3 del GDPR del Regno Unito ([34]) e comprende il trattamento di dati personali (indipendentemente da dove avviene) nel contesto delle attività di uno stabilimento di un titolare del trattamento o di un responsabile del trattamento nel Regno Unito, nonché il trattamento di dati personali di interessati che si trovano nel Regno Unito, quando le attività di trattamento sono legate all'offerta di beni o servizi a tali interessati o al monitoraggio del loro comportamento ([35]). Ciò riflette l'approccio adottato dall'articolo 3 del regolamento (UE) 2016/679.

2.4. **Definizioni di dati personali e concetti di titolare del trattamento e responsabile del trattamento**

(23) Le definizioni di dati personali, trattamento, titolare del trattamento e responsabile del trattamento, così come la definizione di pseudonimizzazione, stabilite nel regolamento (UE) 2016/679 sono state mantenute senza modifiche sostanziali nel GDPR del Regno Unito ([36]). Inoltre le categorie particolari di dati sono definite dall'articolo 9, paragrafo 1, del GDPR del Regno Unito allo stesso modo del regolamento (UE) 2016/679 («[dati] che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona»). La sezione 205 della legge del 2018 sulla protezione dei dati fornisce la definizione di «dati biometrici» ([37]), «dati relativi alla salute» ([38]) e «dati genetici» ([39]).

2.5. **Garanzie, diritti e obblighi**

2.5.1. *Liceità e correttezza del trattamento*

(24) I dati personali dovrebbero essere trattati in maniera lecita e corretta.

(25) I principi di liceità, correttezza e trasparenza e le basi per il trattamento lecito sono 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, che sono identici alle rispettive disposizioni del regolamento (UE) 2016/679 ([40]). La sezione 8 della legge del 2018 sulla protezione dei dati integra l'articolo 6, paragrafo 1, lettera e), prevedendo che il trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera e), del GDPR del Regno Unito (necessario per lo svolgimento di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento), comprende il

([33]) Articolo 2, paragrafo 2, lettere b) e c), del GDPR del Regno Unito.

([34]) Il medesimo ambito di applicazione territoriale si applica al trattamento di dati personali ai sensi della parte 2 della legge del 2018 sulla protezione dei dati che integra il GDPR del Regno Unito (sezione 207, paragrafo 1A).

([35]) Ciò significa, in particolare, che la legge del 2018 sulla protezione dei dati, e quindi la presente decisione, non si applicano alle dipendenze della Corona britannica (Jersey, Guernsey e Isola di Man) e ai territori d'oltremare del Regno Unito, come ad esempio le isole Falkland e il territorio di Gibilterra.

([36]) Articolo 4, paragrafi 1, 2, 5, 7 e 8, del GDPR del Regno Unito.

([37]) Per «dati biometrici» si intendono i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

([38]) Per «dati relativi alla salute» si intendono i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

([39]) Per «dati genetici» si intendono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

([40]) Ai sensi dell'articolo 6, paragrafo 1, del GDPR del Regno Unito, il trattamento è lecito soltanto se e nella misura in cui: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; o f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

trattamento dei dati personali necessario per l'amministrazione della giustizia, l'esercizio di una funzione di una delle due camere del parlamento, l'esercizio di una funzione conferita a una persona da un atto o da una norma, l'esercizio di una funzione della Corona, di un ministro della Corona o di un dipartimento governativo oppure un'attività che sostiene o promuove l'impegno democratico.

(26) Per quanto concerne il consenso (una delle basi per il trattamento lecito), anche il GDPR del Regno Unito mantiene inalterate le condizioni previste dall'articolo 7 del regolamento (UE) 2016/679, ossia: il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso; una richiesta scritta di consenso deve essere presentata utilizzando un linguaggio semplice e chiaro; l'interessato deve avere il diritto di revocare il proprio consenso in qualsiasi momento; e, nel valutare se il consenso sia stato liberamente prestato, si deve tenere conto dell'eventualità che l'esecuzione di un contratto sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto. Inoltre, ai sensi dell'articolo 8 del GDPR del Regno Unito, nel contesto dell'erogazione di servizi della società dell'informazione il consenso di un minore è lecito soltanto se il minore ha almeno 13 anni. Tale soglia rientra nella fascia di età stabilita dall'articolo 8 del regolamento (UE) 2016/679.

2.5.2. *Trattamento di categorie particolari di dati personali*

(27) Garanzie specifiche dovrebbero essere applicate al trattamento di «categorie particolari» di dati.

(28) Il GDPR del Regno Unito e la legge del 2018 sulla protezione dei dati contengono norme specifiche per quanto riguarda il trattamento di categorie particolari di dati personali, definite dall'articolo 9, paragrafo 1, del GDPR del Regno Unito allo stesso modo del regolamento (UE) 2016/679 (cfr. considerando 23). Ai sensi dell'articolo 9 del GDPR del Regno Unito, il trattamento di categorie particolari di dati è in linea di principio vietato, fatto salvo il caso in cui si applichi un'eccezione specifica.

(29) Tali eccezioni (elencate all'articolo 9, paragrafi 2 e 3, del GDPR del Regno Unito) non apportano modifiche sostanziali a quelle previste dall'articolo 9, paragrafi 2 e 3, del regolamento (UE) 2016/679. Fatto salvo il caso in cui l'interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati personali, il trattamento di categorie particolari di dati personali è consentito soltanto in circostanze specifiche e limitate. Nella maggior parte dei casi, il trattamento di dati sensibili deve essere necessario per una finalità specifica definita nella disposizione pertinente (cfr. articolo 9, paragrafo 2, lettere b), c), f), g), h), i) e j)).

(30) Inoltre, quando un'eccezione ai sensi dell'articolo 9, paragrafo 2, del GDPR del Regno Unito richiede un'autorizzazione di legge o fa riferimento all'interesse pubblico, affinché possano essere invocate tali eccezioni occorre che siano soddisfatte le condizioni ulteriormente specificate dalla sezione 10 della legge del 2018 sulla protezione dei dati unitamente all'allegato 1 della medesima legge. Ad esempio nel caso di trattamento di dati sensibili per la tutela della «salute pubblica» (articolo 9, paragrafo 2, lettera i), del GDPR del Regno Unito), l'allegato 1, parte 1, paragrafo 3, lettera b), richiede che, oltre alla verifica della necessità, tale trattamento sia effettuato «da un operatore sanitario o sotto la sua responsabilità» oppure «da un'altra persona soggetta a un obbligo di riservatezza in base a un atto legislativo o una norma di legge», anche ai sensi dell'obbligo di riservatezza ben consolidato nella «common law».

(31) Quando dati sensibili vengono trattati per motivi di interesse pubblico rilevante (articolo 9, paragrafo 2, lettera g), del GDPR del Regno Unito), l'allegato 1, parte 2, della legge del 2018 sulla protezione dei dati riporta un elenco esaustivo di finalità che possono essere considerate di interesse pubblico rilevante e, per ciascuna di esse, fissa condizioni aggiuntive specifiche. Ad esempio la promozione della diversità razziale ed etnica ad alti livelli dirigenziali di organizzazioni è riconosciuta come un interesse pubblico rilevante. Il trattamento di dati sensibili per questa finalità specifica è soggetto a requisiti dettagliati, tra cui il fatto che il trattamento sia effettuato nel contesto di un processo di individuazione delle persone idonee a ricoprire posizioni di alto livello, sia necessario per promuovere la diversità razziale ed etnica e non sia suscettibile di causare un danno sostanziale o una sofferenza sostanziale all'interessato.

(32) La sezione 11, paragrafo 1, della legge del 2018 sulla protezione dei dati stabilisce le condizioni per il trattamento di dati personali nelle circostanze descritte dall'articolo 9, paragrafo 3, del GDPR del Regno Unito relative all'obbligo di segretezza. Rientrano in tale contesto circostanze nelle quali il trattamento viene svolto da o sotto la responsabilità di un professionista sanitario o sociale o da un'altra persona che in quelle circostanze è soggetta a un obbligo di riservatezza ai sensi di un atto legislativo o di una norma di legge.

(33) Inoltre, molte eccezioni elencate all'articolo 9, paragrafo 2, del GDPR del Regno Unito richiedono garanzie adeguate e specifiche per essere invocate. A seconda della natura del trattamento e del livello di rischio per i diritti e le libertà degli interessati, le condizioni per il trattamento di cui all'allegato 1 della legge del 2018 sulla protezione dei dati stabiliscono garanzie differenti. L'allegato 1 stabilisce le condizioni per ciascuna situazione di trattamento individualmente.

(34) In alcuni casi la legge del 2018 sulla protezione dei dati disciplina e limita il tipo di dati sensibili che possono essere trattati affinché sia rispettata una base giuridica specifica. Ad esempio il paragrafo 8 dell'allegato 1 autorizza il trattamento di dati sensibili per finalità di promozione della parità di opportunità o di trattamento. Tale condizione di trattamento può essere utilizzata soltanto se i dati rivelano l'origine razziale o etnica, le convinzioni religiose o filosofiche, l'orientamento sessuale oppure se si tratta di dati relativi alla salute.

(35) In alcuni casi la legge del 2018 sulla protezione dei dati limita il tipo di titolare del trattamento che può invocare la condizione di trattamento. Ad esempio il paragrafo 23 dell'allegato 1 prevede il trattamento di dati sensibili in relazione alle risposte di rappresentanti eletti al pubblico. Tale condizione di trattamento può essere utilizzata soltanto se il titolare del trattamento è il rappresentante eletto o agisce sotto l'autorità di quest'ultimo.

(36) In alcuni altri casi la legge del 2018 sulla protezione dei dati fissa dei limiti alle categorie di interessati affinché sia possibile utilizzare una condizione di trattamento. Ad esempio il paragrafo 21 dell'allegato 1 disciplina il trattamento di dati sensibili per regimi pensionistici. Tale condizione può essere utilizzata soltanto se l'interessato è un fratello, un genitore, un nonno o bisnonno del membro di tale regime.

(37) Inoltre, quando si fa affidamento sulle eccezioni di cui all'articolo 9, paragrafo 2, del GDPR del Regno Unito che sono ulteriormente specificate nella sezione 10 della legge del 2018 sulla protezione dei dati unitamente all'allegato 1 della medesima legge, nella maggior parte dei casi il titolare del trattamento è tenuto a redigere un «documento adeguato di informativa». Tale documento deve descrivere le procedure del titolare del trattamento per garantire la conformità rispetto ai principi di cui all'articolo 5 del GDPR del Regno Unito. Deve inoltre stabilire le politiche per la conservazione e la cancellazione, con un'indicazione del periodo di conservazione probabile. I titolari del trattamento devono riesaminare ed aggiornare tale documento come opportuno. Il titolare del trattamento deve conservare il documento di informativa per sei mesi dopo che il trattamento si è concluso e deve renderlo disponibile all'*Information Commissioner* su richiesta ([41]).

(38) Conformemente al paragrafo 41 dell'allegato 1 della legge del 2018 sulla protezione dei dati, il documento di informativa deve essere sempre accompagnato da un registro dei trattamenti più approfondito. Tale registro deve tenere traccia degli impegni inclusi nel documento di informativa, ossia indicare se i dati vengono cancellati o conservati in conformità con le politiche. Se le politiche non sono state seguite, il registro deve registrarne i motivi. Il registro deve altresì descrivere in che modo il trattamento soddisfa l'articolo 6 del GDPR del Regno Unito (liceità del trattamento) e la condizione specifica invocata di cui all'allegato 1 della legge del 2018 sulla protezione dei dati.

(39) Infine, come avviene per il regolamento (UE) 2016/679, il GDPR del Regno Unito prevede altresì delle garanzie generali per determinati trattamenti di categorie particolari di dati. L'articolo 35 del GDPR del Regno Unito richiede una valutazione d'impatto sulla protezione dei dati se categorie particolari di dati vengono trattate su larga scala. Ai sensi dell'articolo 37 del GDPR del Regno Unito, il titolare del trattamento o il responsabile del trattamento deve designare un responsabile della protezione dei dati laddove le sue attività principali consistano in trattamenti di categorie particolari di dati su larga scala.

(40) Per quanto concerne i dati personali relativi a condanne penali e reati, l'articolo 10 del GDPR del Regno Unito è identico all'articolo 10 del regolamento (UE) 2016/679. Tale articolo consente il trattamento di dati personali relativi a condanne penali e reati soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto interno che preveda garanzie appropriate per i diritti e le libertà degli interessati.

(41) Se il trattamento di dati relativi a condanne penali e reati non viene effettuato sotto il controllo dell'autorità pubblica, la sezione 10, paragrafo 5, della legge del 2018 sulla protezione dei dati prevede che tale trattamento possa avvenire soltanto per le finalità specifiche/nelle situazioni specifiche di cui all'allegato 1, parti 1, 2 e 3, della legge del 2018 sulla protezione dei dati e sia soggetto ai requisiti specifici stabiliti per ciascuna di tali finalità/situazioni. Ad esempio i dati relativi alle condanne penali possono essere trattati da organismi senza scopo di lucro se il trattamento è effettuato: a) nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali e b) a condizione che i) il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e b) che i dati personali non siano comunicati all'esterno senza il consenso degli interessati.

([41]) Paragrafi da 38 a 40 dell'allegato 1 della legge del 2018 sulla protezione dei dati.

(42) Inoltre l'allegato 1, parte 3, della legge del 2018 sulla protezione dei dati stabilisce ulteriori circostanze nelle quali i dati relativi alle condanne penali possono essere utilizzati, che corrispondono alle basi giuridiche per il trattamento dei dati sensibili di cui all'articolo 9, paragrafo 2, del regolamento (UE) 2016/679 e del GDPR del Regno Unito (ad esempio, il consenso dell'interessato, un interesse vitale di una persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso, se i dati sono già stati resi manifestamente pubblici dall'interessato, se il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria, ecc.).

2.5.3 *Limitazione della finalità, esattezza, minimizzazione dei dati, limitazione della conservazione e sicurezza dei dati*

(43) I dati personali dovrebbero essere trattati per una finalità specifica ed essere utilizzati successivamente soltanto nella misura in cui l'uso non sia incompatibile con la finalità del trattamento.

(44) Tale principio è sancito dall'articolo 5, paragrafo 1, lettera b), del regolamento (UE) 2016/679 ed è stato mantenuto senza modifiche all'articolo 5, paragrafo 1, lettera b), del GDPR del Regno Unito. Le condizioni in merito a ulteriori trattamenti compatibili a norma dell'articolo 6, paragrafo 4, del regolamento (UE) 2016/679 sono state mantenute senza modifiche sostanziali all'articolo 6, paragrafo 4, lettere da a) ad e), del GDPR del Regno Unito.

(45) Inoltre i dati dovrebbero essere esatti e, se necessario, dovrebbero essere aggiornati. Dovrebbero inoltre essere adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali sono trattati; inoltre, in linea di principio, dovrebbero essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

(46) Tali principi di minimizzazione dei dati, esattezza e limitazione della conservazione sono sanciti dall'articolo 5, paragrafo 1, lettere da c) ad e), del regolamento (UE) 2016/679 e sono mantenuti senza modifiche nell'articolo 5, paragrafo 1, lettere da c) ad e), del GDPR del Regno Unito.

(47) I dati personali dovrebbero inoltre essere trattati in maniera da garantirne la sicurezza, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. A tal fine gli operatori economici dovrebbero adottare misure tecniche o organizzative per proteggere i dati personali da possibili minacce. Tali misure dovrebbero essere valutate tenendo conto dello stato dell'arte e dei costi connessi.

(48) La sicurezza dei dati è sancita dalla legge del Regno Unito attraverso il principio di integrità e della riservatezza di cui all'articolo 5, paragrafo 1, lettera f), e all'articolo 32 del GDPR del Regno Unito, concernenti la sicurezza del trattamento. Tali disposizioni sono identiche alle rispettive disposizioni del regolamento (UE) 2016/679. Inoltre, alle stesse condizioni di quelle di cui agli articoli 33 e 34 del regolamento (UE) 2016/679, il GDPR del Regno Unito richiede la notifica di una violazione dei dati personali all'autorità di controllo (articolo 33 del GDPR del Regno Unito) così come la comunicazione di una violazione dei dati personali all'interessato (articolo 34 del medesimo regolamento).

2.5.4 *Trasparenza*

(49) Gli interessati dovrebbero essere informati dei principali aspetti del trattamento dei dati personali che li riguardano.

(50) Ciò è garantito dagli articoli 13 e 14 del GDPR del Regno Unito, che, oltre a un principio generale di trasparenza, prevede norme sulle informazioni da fornire all'interessato ([42]). Il GDPR del Regno Unito non introduce modifiche sostanziali a tali norme rispetto agli articoli corrispondenti del regolamento (UE) 2016/679. Tuttavia, come ai sensi del regolamento (UE) 2016/679, i requisiti di trasparenza di cui a tali articoli sono soggetti a diverse eccezioni stabilite nella legge del 2018 sulla protezione dei dati (cfr. considerando da 55 a 72).

([42]) All'articolo 13, paragrafo 1, lettera f), e all'articolo 14, paragrafo 1, lettera f), i riferimenti a decisioni di adeguatezza della Commissione sono stati sostituiti da riferimenti all'equivalente strumento del Regno Unito, ossia i regolamenti di adeguatezza ai sensi della legge del 2018 sulla protezione dei dati. Inoltre alla sezione 14, paragrafo 5, lettere c) e d), i riferimenti al diritto dell'UE o degli Stati membri sono stati sostituiti con un riferimento al diritto interno (come esempi di tale diritto nazionale che possono rientrare nell'ambito di applicazione della sezione 14, paragrafo 5, lettera c), il Regno Unito ha menzionato la sezione 7 della *Scrap Metal Dealers Act 2013* (legge del 2013 sui rivenditori di rottami metallici) che prevede norme per il registro delle licenze per i rottami metallici oppure la parte 35 del *Companies Act 2006* (legge del 2006 sulle imprese) che prevede le norme per il registro delle imprese. Analogamente, un esempio di diritto interno che può rientrare nell'ambito di applicazione dell'articolo 14, paragrafo 5, lettera d), potrebbe comprendere la legislazione che stabilisce norme in materia di segreto professionale oppure gli obblighi riflessi nei contratti di lavoro o il dovere di riservatezza sancito dalla «common law» (come i dati personali trattati da professionisti sanitari, da uffici risorse umane, da assistenti sociali, ecc.).

2.5.5 *Diritti delle persone fisiche*

(51) Gli interessati dovrebbero disporre di determinati diritti 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. Allo stesso tempo, tali diritti possono essere soggetti a limitazioni, nella misura in cui tali limitazioni siano necessarie e proporzionate per salvaguardare la sicurezza pubblica o altri importanti obiettivi di interesse pubblico generale.

2.5.5.1 I diritti sostanziali

(52) Il GDPR del Regno Unito garantisce alle persone fisiche i medesimi diritti azionabili di cui al regolamento (UE) 2016/679. Le disposizioni che riconoscono tali diritti delle persone fisiche sono state mantenute nel GDPR del Regno Unito senza modifiche sostanziali.

(53) Tra tali diritti figurano il diritto di accesso dell'interessato (articolo 15 del GDPR del Regno Unito), il diritto di rettifica (articolo 16 del GDPR del Regno Unito), il diritto alla cancellazione (articolo 17 del GDPR del Regno Unito), il diritto di limitazione del trattamento (articolo 18 del GDPR del Regno Unito), un obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (articolo 19 del GDPR del Regno Unito), il diritto alla portabilità dei dati (articolo 20 del GDPR del Regno Unito) e il diritto di opposizione (articolo 21 del GDPR del Regno Unito) ([43]). Quest'ultimo comprende anche il diritto dell'interessato di opporsi al trattamento di dati personali per finalità di marketing diretto di cui all'articolo 21, paragrafi 2 e 3, del regolamento (UE) 2016/679. Inoltre, ai sensi della sezione 122 della legge del 2018 sulla protezione dei dati, l'*Information Commissioner* deve preparare un codice di pratica in relazione allo svolgimento di attività di marketing diretto in conformità con i requisiti della legislazione in materia di protezione dei dati [e i *Privacy and Electronic Communications (EC Directive) Regulations 2003* — regolamenti del 2003 sulla tutela della vita privata e le comunicazioni elettroniche (direttiva CE)] nonché degli altri orientamenti destinati a promuovere buone pratiche nel contesto del marketing diretto che l'*Information Commissioner* ritiene adeguati. L'ufficio dell'*Information Commissioner* (ICO, *Information Commissioner's Office*) sta attualmente sviluppando il codice sul marketing diretto ([44]).

(54) Il diritto dell'interessato a non essere soggetto a una decisione basata unicamente su un trattamento automatizzato che produca effetti giuridici che lo riguardano o che incida analogamente in modo significativo sullo stesso, come previsto dall'articolo 22 del regolamento (UE) 2016/679, è stato anch'esso mantenuto nel GDPR del Regno Unito senza modifiche sostanziali. Tuttavia, è stato aggiunto un nuovo paragrafo (3A) per indicare che la sezione 14 della legge del 2018 sulla protezione dei dati stabilisce garanzie per i diritti, le libertà e i legittimi interessi degli interessati quando il trattamento è effettuato ai sensi dell'articolo 22, paragrafo 2, lettera b), del GDPR del Regno Unito. Ciò si applica solo quando la base per tale decisione è un'autorizzazione o un requisito ai sensi del diritto del Regno Unito, e non si applica se la decisione è necessaria ai sensi di un contratto o se effettuata con il consenso esplicito dell'interessato. Quando si applica la sezione 14 della legge del 2018 sulla protezione dei dati, non appena ragionevolmente fattibile, il titolare del trattamento deve notificare all'interessato per iscritto che è stata adottata una decisione basata unicamente sul trattamento automatizzato. L'interessato ha quindi il diritto, entro un mese dalla ricezione della notifica, di richiedere al titolare del trattamento di riconsiderare la decisione o di adottare una nuova decisione non basata unicamente sul trattamento automatizzato. Al segretario di Stato sono conferiti poteri per adottare ulteriori garanzie per quanto concerne il processo decisionale automatizzato. Tali poteri non sono ancora stati esercitati.

2.5.5.2 Limitazioni dei diritti individuali e altre disposizioni

(55) La legge del 2018 sulla protezione dei dati stabilisce diverse limitazioni a diritti individuali che si inseriscono nel quadro dell'articolo 23 del GDPR del Regno Unito. In tale contesto non viene introdotta alcuna limitazione relativa al diritto di opposizione al marketing diretto come previsto dall'articolo 21, paragrafi 2 e 3, del GDPR del Regno Unito o al diritto di non essere soggetti a un processo decisionale automatizzato come previsto dall'articolo 22 del GDPR del Regno Unito.

(56) Le limitazioni sono dettagliate negli allegati da 2 a 4 della legge del 2018 sulla protezione dei dati. Le autorità del Regno Unito hanno spiegato di seguire due principi: il principio di specificità (adottando un approccio granulare, suddividendo limitazioni di ampia portata in un numero maggiore di disposizioni più specifiche) e il principio di condizionalità (ciascuna disposizione è integrata da garanzie sotto forma di limitazioni o condizioni per prevenire abusi) ([45]).

([43]) All'articolo 17, paragrafo 1, lettera e), e all'articolo 17, paragrafo 3, lettera b), i riferimenti al diritto dell'Unione o degli Stati membri sono stati sostituiti con un riferimento al diritto interno (come esempi di tale diritto nazionale ai sensi della sezione 17, paragrafo 1, lettera e), il Regno Unito ha menzionato gli *Education (Pupil Information) (England) Regulations 2006* (regolamenti del 2006 sull'istruzione (informazione agli allievi) (Inghilterra)) i quali impongono che i nomi degli allievi vengano cancellati dai registri scolastici dopo che hanno lasciato la scuola oppure la *Medical Act 1983* (legge del 1983 sul settore medico), sezione 34F, che stabilisce le norme concernenti la rimozione dei nomi dal registro dei medici generici e dal registro degli specialisti).

([44]) Il progetto di codice di pratica è disponibile al seguente indirizzo: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf.

([45]) Regno Unito, *Explanatory Framework for Adequacy Discussions, Section E: Restrictions*, pag. 1, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

(57) Le limitazioni di cui all'articolo 23, paragrafo 1, del GDPR del Regno Unito sono progettate per garantire che esse si applichino soltanto in circostanze specifiche, ove necessario in una società democratica e proporzionato in relazione alla finalità legittima perseguita. Inoltre, conformemente alla giurisprudenza consolidata in materia di interpretazione di limitazioni, un'esenzione dal regime di protezione dei dati può applicarsi soltanto in un caso particolare laddove sia necessario e proporzionato procedere in tal senso ([46]). È richiesto che la verifica della necessità sia «rigorosa e richieda che qualsiasi ingerenza nei diritti dell'interessato sia proporzionata alla gravità della minaccia per l'interesse pubblico. Tale esercizio comporta pertanto una classica analisi della proporzionalità ([47])».

(58) Gli obiettivi perseguiti da tali limitazioni corrispondono a quelli elencati dall'articolo 23 del regolamento (UE) 2016/679, fatta eccezione per le limitazioni per la sicurezza nazionale e la difesa che sono invece disciplinate dalla sezione 26 della legge del 2018 sulla protezione dei dati, ma che sono soggette ai medesimi requisiti in termini di necessità e proporzionalità (cfr. considerando da 63 a 66).

(59) Alcune delle limitazioni, ad esempio quelle relative alla prevenzione o all'accertamento di reati, all'arresto o al perseguimento di autori di reati e alla valutazione o alla riscossione di imposte o diritti ([48]), consentono limitazioni in relazione a tutti i diritti individuali e agli obblighi di trasparenza (esclusi i diritti di cui all'articolo 21, paragrafo 2, e all'articolo 22). La portata di altre limitazioni è limitata agli obblighi di trasparenza e ai diritti di accesso, come nel caso delle limitazioni relative al segreto professionale ([49]), al diritto alla libertà dall'obbligo di fornire informazioni che porterebbero a un'autoincriminazione ([50]) e alla finanza d'impresa, in particolare la prevenzione dell'abuso di informazioni privilegiate (*insider trading*) ([51]). Sono poche le limitazioni che consentono una limitazione rispetto all'obbligo del titolare del trattamento di comunicare una violazione dei dati a un interessato e ai principi di limitazione della finalità, nonché di liceità, correttezza e trasparenza del trattamento ([52]).

(60) Alcune delle limitazioni si applicano automaticamente «integralmente» a un certo tipo di trattamento di dati personali (ad esempio l'applicazione degli obblighi di trasparenza e dei diritti individuali è esclusa quando i dati personali vengono trattati per finalità di valutazione dell'idoneità di una persona a ricoprire una carica giudiziaria oppure quando i dati personali vengono trattati da un organo giurisdizionale o da una persona fisica che agisce nell'esercizio delle proprie funzioni giurisdizionali).

(61) Tuttavia, nella maggior parte dei casi, il paragrafo pertinente dell'allegato 2 della legge del 2018 specifica che la limitazione si applica soltanto quando (e nella misura in cui) l'applicazione delle disposizioni «possa pregiudicare» l'obiettivo legittimo perseguito da tale limitazione: ad esempio, le disposizioni elencate del GDPR del Regno Unito non si applicano ai dati personali trattati a fini di prevenzione o accertamento di reati, arresto o perseguimento di autori di reati, oppure valutazione o riscossione di imposte o diritti «nella misura in cui l'applicazione di tali disposizioni possa pregiudicare» una di tali finalità ([53]).

(62) Secondo l'interpretazione costante degli organi giurisdizionali del Regno Unito, l'espressione «possa pregiudicare» indica «una probabilità molto significativa e seria di pregiudicare gli interessi pubblici individuati» ([54]). Una limitazione soggetta al criterio del pregiudizio può pertanto essere invocata solo se, e nella misura in cui, vi sia una probabilità molto significativa e seria che la concessione di un determinato diritto pregiudichi l'interesse pubblico in questione. Spetta al titolare del trattamento valutare caso per caso se tali condizioni siano soddisfatte ([55]).

(63) Oltre alle limitazioni di cui all'allegato 2 della legge del 2018 sulla protezione dei dati, la sezione 26 della legge del 2018 sulla protezione dei dati prevede un'esenzione che può essere applicata a talune disposizioni del GDPR del Regno Unito e della legge del 2018 sulla protezione dei dati se tale esenzione è necessaria al fine di salvaguardare la sicurezza nazionale o per finalità di difesa. Tale esenzione si applica ai principi di protezione dei dati (fatta eccezione per il principio di liceità), agli obblighi di trasparenza, ai diritti dell'interessato, all'obbligo di notificare una violazione

([46]) *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.

([47]) *Guriev v Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), punto 43. In merito a questo aspetto cfr. anche *Lin v Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), punto 80.

([48]) Paragrafo 2 dell'allegato 2 della legge del 2018 sulla protezione dei dati.

([49]) Paragrafo 19 dell'allegato 2 della legge del 2018 sulla protezione dei dati.

([50]) Paragrafo 20 dell'allegato 2 della legge del 2018 sulla protezione dei dati.

([51]) Paragrafo 21 dell'allegato 2 della legge del 2018 sulla protezione dei dati.

([52]) Ad esempio le limitazioni in relazione al diritto a una notifica di una violazione dei dati sono consentite soltanto in relazione a reati e tassazione (paragrafo 2 dell'allegato 2 della legge del 2018 sulla protezione dei dati), all'immunità parlamentare (paragrafo 13 dell'allegato 2 della legge del 2018 sulla protezione dei dati) e al trattamento per finalità giornalistiche, accademiche, artistiche e letterarie (paragrafo 26 dell'allegato 2 della legge del 2018 sulla protezione dei dati).

([53]) Paragrafo 2 dell'allegato 2 della legge del 2018 sulla protezione dei dati.

([54]) *R (Lord) v Secretary of State for the Home Department* [2003] EWHC 2073 (Admin), punto 100 e *Guriev v Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), punto 43.

([55]) *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor*, punto 31.

dei dati, alle norme sui trasferimenti internazionali, ad alcune delle mansioni e ad alcuni dei poteri dell'*Information Commissioner*, nonché alle norme sui mezzi di ricorso, sulle responsabilità e sulle sanzioni, fatta eccezione per la disposizione concernente le condizioni generali per l'imposizione di sanzioni amministrative pecuniarie di cui all'articolo 83 e per la disposizione sulle sanzioni di cui all'articolo 84 del GDPR del Regno Unito. Inoltre la sezione 28 della legge del 2018 sulla protezione dei dati modifica l'applicazione dell'articolo 9, paragrafo 1, al fine di consentire il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, del GDPR del Regno Unito nella misura in cui il trattamento venga effettuato per salvaguardare la sicurezza nazionale o per finalità di difesa e con garanzie adeguate per i diritti e le libertà degli interessati ([56]).

(64) L'esenzione può essere applicata soltanto nella misura in cui essa sia necessaria per salvaguardare la sicurezza nazionale o la difesa. Come per le altre esenzioni previste dalla legge del 2018 sulla protezione dei dati, tale esenzione deve essere considerata e invocata dal titolare del trattamento caso per caso. Inoltre qualsiasi applicazione dell'esenzione deve essere conforme alle norme in materia di diritti umani (sostenute dalla legge del 1998 sui diritti umani), secondo le quali qualsiasi ingerenza rispetto ai diritti in materia di tutela della vita privata dovrebbe essere necessaria e proporzionata in una società democratica ([57]).

(65) Tale interpretazione dell'esenzione è confermata dall'ICO, che ha emanato orientamenti dettagliati sull'applicazione dell'esenzione per motivi di sicurezza nazionale e difesa, chiarendo che essa deve essere presa in considerazione e applicata dal titolare del trattamento caso per caso ([58]). In particolare, gli orientamenti sottolineano che «non si tratta di un'esenzione generalizzata» e che, per invocarla, «non è sufficiente che i dati siano trattati a fini di sicurezza nazionale». Il titolare del trattamento che se ne avvale deve «dimostrare l'effettiva possibilità di un effetto negativo sulla sicurezza nazionale» e, se necessario, «fornire [all'ICO] le prove del motivo per cui si è avvalso di tale esenzione». Gli orientamenti contengono una lista di controllo e una serie di esempi per chiarire ulteriormente le condizioni alle quali tale esenzione può essere invocata.

(66) Il fatto che i dati vengano trattati per finalità di difesa o di sicurezza nazionale non è pertanto di per sé sufficiente per applicare tale esenzione. Un titolare del trattamento deve considerare le conseguenze effettive per la sicurezza nazionale qualora dovesse rispettare la disposizione specifica in materia di protezione dei dati. L'esenzione può essere applicata soltanto a quelle disposizioni specifiche che sono state individuate costituire un rischio e deve essere applicata nella maniera più restrittiva possibile ([59]).

(67) Tale approccio è stato confermato dall'*Information Tribunal* ([60]) (tribunale competente in materia di informazione). Nella causa *Baker v Secretary of State for the Home Department* («*Baker v Secretary of State*»), detto organo giurisdizionale ha stabilito che era illecito applicare l'esenzione per motivi di sicurezza nazionale come un'esenzione globale in relazione a richieste di accesso ricevute dai servizi di intelligence. Tale esenzione doveva invece essere applicata caso per caso, esaminando ciascuna richiesta nel merito e tenuto conto del diritto delle persone fisiche al rispetto della loro vita privata ([61]).

([56]) Secondo le informazioni fornite dalle autorità del Regno Unito, nel caso in cui il trattamento avvenga nel contesto della sicurezza nazionale, in genere i titolari del trattamento applicano garanzie e misure di sicurezza superiori al trattamento, circostanza questa che rispecchia la natura sensibile del trattamento. Quali siano le garanzie adeguate dipenderà dai rischi posti dal trattamento intrapreso. In tale contesto potrebbero figurare limitazioni sull'accesso ai dati in ragione delle quali tale accesso potrebbe essere possibile soltanto da parte di persone autorizzate nel rispetto di condizioni di sicurezza adeguate, limitazioni rigorose in relazione alla condivisione dei dati e un livello elevato di sicurezza applicato alle procedure di conservazione e gestione.

([57]) 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.

([58]) Cfr. gli orientamenti dell'ICO sull'eccezione per motivi di sicurezza nazionale e difesa, disponibili al seguente indirizzo: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/

([59]) Secondo un esempio fornito dalle autorità del Regno Unito, se un sospetto terrorista soggetto a un'indagine attiva da parte dell'MI5 ha presentato una richiesta di accesso al ministero dell'Interno (ad esempio poiché è coinvolto in una controversia con tale ministero in relazione a questioni di immigrazione), sarebbe necessario proteggere dalla divulgazione all'interessato eventuali dati che l'MI5 può aver condiviso con il ministero dell'Interno in relazione alle indagini in corso che potrebbero pregiudicare fonti, metodi o tecniche sensibili e/o portare ad un aumento della minaccia costituita da tale persona fisica. In tali circostanze è probabile che la soglia per applicare l'esenzione di cui alla sezione 26 sarebbe soddisfatta e, al fine di salvaguardare la sicurezza nazionale, sarebbe necessaria un'esenzione dalla divulgazione di tali informazioni. Tuttavia se il ministero dell'Interno deteneva anche dati personali su detta persona fisica non riferiti all'indagine dell'MI5 e tali informazioni potevano essere fornite senza rischi di danni per la sicurezza nazionale, l'esenzione per motivi di sicurezza nazionale non sarebbe applicabile in relazione alla divulgazione di informazioni a tale persona fisica. L'ICO sta attualmente preparando orientamenti in merito alle modalità con cui i titolari del trattamento dovrebbero affrontare l'utilizzo dell'esenzione di cui alla sezione 26. Si prevede che tali orientamenti siano pubblicati entro la fine di marzo del 2021.

([60]) L'*Information Tribunal* è stato istituito per esaminare ricorsi in materia di protezione dei dati nel quadro della legge del 1984 sulla protezione dei dati. Nel 2010 l'*Information Tribunal* è diventato parte della *General Regulatory Chamber* (camera di regolamentazione generale) del *First Tier Tribunal* (tribunale di primo grado), nel contesto della riforma della struttura del sistema degli organi giurisdizionali del Regno Unito.

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

2.5.6 *Limitazioni relative ai dati personali trattati per finalità giornalistiche, artistiche, accademiche e letterarie nonché per archiviazione e ricerca*

(68) L'articolo 85, paragrafo 2, del GDPR del Regno Unito consente l'emissione di disposizioni affinché i dati personali trattati per finalità giornalistiche, artistiche, accademiche e letterarie siano esentati dall'applicazione di diverse disposizioni del GDPR del Regno Unito. L'allegato 2, parte 5, della legge del 2018 sulla protezione dei dati stabilisce le esenzioni per il trattamento per tali finalità. Prevede esenzioni rispetto ai principi di protezione dei dati (fatta eccezione per il principio di integrità e riservatezza), alle basi giuridiche per il trattamento (incluse categorie particolari di dati e dati su condanne penali, ecc.), alle condizioni per il consenso, agli obblighi di trasparenza, ai diritti degli interessati, all'obbligo di notificare violazioni dei dati e al requisito di consultare l'*Information Commissioner* prima di un trattamento soggetto a rischio elevato nonché alle norme in materia di trasferimenti internazionali ([62]). A tale riguardo, il GDPR del Regno Unito non si discosta in maniera sostanziale dal regolamento (UE) 2016/679, il quale al suo articolo 85 prevede anch'esso la possibilità di esentare il trattamento effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria da una serie di requisiti sanciti dal regolamento (UE) 2016/679 stesso. Le disposizioni della legge del 2018 sulla protezione dei dati, in particolare l'allegato 2, parte 5, sono compatibili con il GDPR del Regno Unito.

(69) L'esercizio principale di equilibrio da effettuare a norma dell'articolo 85 del GDPR del Regno Unito riguarda l'eventualità che un'esenzione rispetto alle norme in materia di protezione dei dati di cui al considerando 68 sia «necessaria per riconciliare il diritto alla protezione dei dati personali con la libertà di espressione e informazione» ([63]). Conformemente all'allegato 2, paragrafo 26, punti 2 e 3, della legge del 2018 sulla protezione dei dati, il Regno Unito applica una verifica della «convinzione ragionevole» al fine di assicurate tale equilibrio. Affinché il ricorso a un'esenzione sia giustificato, il titolare del trattamento deve ritenere ragionevolmente: i) che la pubblicazione sia nell'interesse pubblico; e ii) che l'applicazione della disposizione pertinente del regolamento generale sulla protezione dei dati sia incompatibile con finalità giornalistiche, accademiche, artistiche o letterarie. Come confermato dalla giurisprudenza ([64]), la verifica della «convinzione ragionevole» presenta tanto una componente soggettiva quanto una componente oggettiva: non è sufficiente per il titolare del trattamento dimostrare che egli stesso riteneva che la conformità fosse incompatibile. La sua convinzione deve essere ragionevole, ossia deve poter essere condivisa da una persona ragionevole che conosca i fatti pertinenti. Il titolare del trattamento deve quindi esercitare la dovuta diligenza quando forma la propria convinzione per essere in grado di dimostrare la ragionevolezza. Secondo le spiegazioni fornite dalle autorità del Regno Unito, la verifica della «convinzione ragionevole» deve essere effettuata in relazione a ogni singola esenzione caso per caso ([65]). Se le condizioni sono soddisfatte, l'esenzione è considerata necessaria e proporzionata ai sensi del diritto del Regno Unito.

(70) Conformemente alla sezione 124 della legge del 2018 sulla protezione dei dati, l'ICO deve preparare un codice di pratica sulla protezione dei dati e il giornalismo. I lavori in relazione a tale codice sono in corso. Sono stati pubblicati orientamenti in merito a questa questione ai sensi della legge del 1998 sulla protezione dei dati che sottolineano in particolare che, per fare affidamento su tale esenzione, non è sufficiente affermare semplicemente che il rispetto delle norme costituirebbe un inconveniente per le attività dei giornalisti, ma deve sussistere un'argomentazione chiara a sostegno del fatto che la disposizione in questione costituisce un ostacolo per il

([62]) Cfr. articolo 85 del GDPR del Regno Unito e allegato 2, parte 5, paragrafo 26, punto 9, della legge del 2018 sulla protezione dei dati.

([63]) Conformemente all'allegato 2, parte 5, paragrafo 26, punto 2, della legge del 2018 sulla protezione dei dati, l'eccezione si applica al trattamento di dati personali effettuato per finalità speciali (finalità di giornalismo, finalità accademiche, finalità artistiche e finalità letterarie), se il trattamento viene effettuato in vista della pubblicazione da parte di una persona di materiale giornalistico, accademico, artistico o letterario e il titolare del trattamento ritiene ragionevolmente che la pubblicazione di tale materiale sarebbe nell'interesse pubblico. Nel determinare se una pubblicazione sarebbe nell'interesse pubblico, il titolare del trattamento deve tenere conto dell'importanza speciale dell'interesse pubblico in relazione alla libertà di espressione e informazione. Inoltre il titolare del trattamento deve considerare i codici di pratica o le linee guida pertinenti per la pubblicazione in questione (*BBC Editorial Guidelines, Ofcom Broadcasting Code* e *Editors' Code of Practice*). Affinché sia possibile applicare un'esenzione, il titolare del trattamento deve inoltre ritenere ragionevolmente che il rispetto della disposizione pertinente sarebbe incompatibile con le finalità speciali (punto 26, punto 3, dell'allegato 2 della legge del 2018 sulla protezione dei dati).

([64]) La sentenza nella causa *NT1* v. *Google* [2018] EWHC 799 (QB), al punto 102, ha affrontato una discussione in merito alla possibilità che il titolare del trattamento dei dati fosse ragionevolmente convinto che la pubblicazione fosse nell'interesse pubblico e che il rispetto delle disposizioni pertinenti fosse incompatibile con le finalità speciali. L'organo giurisdizionale ha affermato che la sezione 32, paragrafo 1, lettere b) e c), della legge del 1998 sulla protezione dei dati presentava un aspetto soggettivo e uno oggettivo: il titolare del trattamento deve stabilire di aver ritenuto che la pubblicazione sarebbe avvenuta nell'interesse pubblico e che tale convinzione era oggettivamente ragionevole; deve stabilire una convinzione soggettiva che il rispetto della disposizione rispetto alla quale cerca di ottenere l'esenzione sarebbe incompatibile con la finalità speciale in questione.

([65]) Un esempio delle modalità di applicazione della «convinzione ragionevole» è incluso nella decisione dell'ICO di irrogare una sanzione pecuniaria a *True Visions Productions*, decisione pronunciata ai sensi della legge del 1998 sulla protezione dei dati. L'ICO ha accolto il fatto che il titolare del trattamento dei mezzi di comunicazione aveva una convinzione soggettiva che il rispetto del primo principio in materia di protezione dei dati (correttezza e legittimità) fosse incompatibile con le finalità giornalistiche. Tuttavia l'ICO non ha accolto il fatto che tale convinzione fosse oggettivamente ragionevole. La decisione dell'ICO è disponibile al seguente indirizzo: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf.

giornalismo responsabile ([66]). L'autorità di regolamentazione per le comunicazioni del Regno Unito, l'Ofcom, e la BBC nelle sue linee guida editoriali hanno pubblicato orientamenti sull'applicazione della verifica dell'interesse pubblico e dell'equilibrio tra interesse pubblico e interesse di una persona fisica alla tutela della sua vita privata ([67]). Tali orientamenti forniscono in particolare esempi di informazioni che possono essere considerate nell'interesse pubblico e spiegano la necessità di essere in grado di dimostrare che l'interesse pubblico prevale sui diritti alla tutela della vita privata in particolari circostanze del caso.

(71) Analogamente a quanto previsto dall'articolo 89 del GDPR del Regno Unito, anche i dati personali trattati per finalità di archiviazione nell'interesse pubblico, per finalità di ricerca scientifica o storica o per finalità statistiche possono essere esentati da una serie di disposizioni elencate dal medesimo regolamento ([68]). Per quanto riguarda la ricerca e la statistica, sono possibili esenzioni rispetto alle disposizioni del GDPR del Regno Unito concernenti la conferma del trattamento, l'accesso ai dati e le garanzie per i trasferimenti verso paesi terzi; il diritto di rettifica; la limitazione di trattamento e l'opposizione al trattamento. Per quanto concerne l'archiviazione nell'interesse pubblico, sono possibili anche esenzioni in relazione all'obbligo di notifica per quanto riguarda la rettifica o la cancellazione di dati personali o la limitazione di trattamento e al diritto alla portabilità dei dati.

(72) Secondo il paragrafo 27, punto 1, e il paragrafo 28, punto 1, dell'allegato 2 della legge del 2018 sulla protezione dei dati, sono possibili esenzioni rispetto alle disposizioni elencate nel GDPR del Regno Unito se l'applicazione delle disposizioni «impedisce o compromette seriamente il conseguimento» delle finalità in questione ([69]).

(73) Data la rilevanza delle esenzioni per l'esercizio effettivo dei diritti individuali, nel contesto del monitoraggio continuo della presente decisione ([70]) si terrà debitamente conto di qualsiasi sviluppo pertinente riguardante l'interpretazione e l'applicazione pratica delle esenzioni summenzionate (oltre a quella relativa al mantenimento dell'effettivo controllo dell'immigrazione, come spiegato al considerando 6), compreso qualsiasi ulteriore sviluppo della giurisprudenza e degli orientamenti dell'ICO e delle azioni di esecuzione.

2.5.7 *Limitazioni ai trasferimenti successivi*

(74) Il livello di protezione offerto ai dati personali trasferiti dall'Unione europea verso titolari del trattamento o responsabili del trattamento nel Regno Unito non deve essere compromesso da ulteriori trasferimenti di tali dati a destinatari che si trovano in un paese terzo. Tali «trasferimenti successivi», che dal punto di vista del titolare del trattamento o del responsabile del trattamento del Regno Unito costituiscono trasferimenti internazionali dal Regno Unito, dovrebbero essere autorizzati soltanto nel caso in cui anche il destinatario successivo al di fuori del Regno Unito sia soggetto a norme che garantiscono un livello di protezione analogo a quello garantito dall'ordinamento giuridico del Regno Unito. Per questo motivo l'applicazione delle norme del GDPR del Regno Unito e della legge del 2018 sulla protezione dei dati in materia di trasferimenti internazionali dei dati personali costituisce un elemento importante per garantire la continuità della protezione nel caso dei dati personali trasferiti dall'Unione europea verso il Regno Unito ai sensi della presente decisione.

([66]) Conformemente a tali orientamenti, le organizzazioni devono essere in grado di spiegare perché rispettare la disposizione pertinente della legge del 1998 sulla protezione dei dati è incompatibile con le finalità di giornalismo. In particolare i titolari del trattamento devono porre su un piatto della bilancia gli effetti negativi sul giornalismo derivanti dal rispetto di tale disposizione rispetto agli effetti negativi per i diritti dell'interessato derivanti dal mancato rispetto di detta disposizione. Se un giornalista può ragionevolmente conseguire i propri obiettivi editoriali nel rispetto delle disposizioni usuali della legge sulla protezione dei dati, deve farlo. Le organizzazioni devono essere in grado di giustificare il loro utilizzo della limitazione per ogni disposizione che non hanno rispettato. «*Data protection and journalism: a guide for the media*», disponibile al seguente indirizzo: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf.

([67]) Esempi di interesse pubblico comprenderebbero la rivelazione o l'accertamento di un reato, la protezione della salute o della sicurezza pubblica, l'esposizione di rivendicazioni fuorvianti promosse da persone fisiche od organizzazioni oppure la divulgazione di incompetenza che incide sul pubblico. Cfr. orientamenti dell'Ofcom disponibili al seguente indirizzo: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf e le linee guida editoriali della BBC disponibili presso il seguente indirizzo: https://www.bbc.com/editorialguidelines/guidelines/privacy.

([68]) Cfr. articolo 89 del GDPR del Regno Unito e paragrafo 27, punto 2 e paragrafo 28, punto 2, della parte 6 dell'allegato 2 della legge del 2018 sulla protezione dei dati.

([69]) Tale aspetto è soggetto al requisito che prevede che i dati personali siano trattati conformemente all'articolo 89, paragrafo 1, del GDPR del Regno Unito, come integrati dalla sezione 19 della legge del 2018 sulla protezione dei dati.

([70]) Cfr. considerando da (281) a(287).

(75) Il regime in materia di trasferimenti internazionali di dati personali dal Regno Unito è definito agli articoli da 44 a 49 del GDPR del Regno Unito, integrati dalla legge del 2018 sulla protezione dei dati, ed è sostanzialmente identico alle norme stabilite al capo V del regolamento (UE) 2016/679 ([71]). I trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale possono avvenire soltanto sulla base di regolamenti di adeguatezza (lo strumento del Regno Unito equivalente a una decisione di adeguatezza ai sensi del regolamento (UE) 2016/679), o, in assenza di regolamenti di adeguatezza, laddove il titolare del trattamento o il responsabile del trattamento abbia fornito garanzie adeguate conformemente all'articolo 46 del GDPR del Regno Unito. In assenza di regolamenti di adeguatezza o garanzie adeguate, un trasferimento può avvenire soltanto sulla base di deroghe di cui all'articolo 49 del GDPR del Regno Unito.

(76) I regolamenti di adeguatezza emessi dal segretario di Stato possono stabilire che un paese terzo (o un territorio o un settore all'interno di un paese terzo), un'organizzazione internazionale o una descrizione ([72]) di tale paese, territorio, settore od organizzazione assicuri un livello adeguato di protezione dei dati personali. Nel valutare l'adeguatezza del livello di protezione, il segretario di Stato deve tenere conto degli stessi identici elementi che la Commissione è tenuta a valutare ai sensi dell'articolo 45, paragrafo 2, lettere da a) a c), del regolamento (UE) 2016/679, interpretato in combinato disposto con il considerando 104 del regolamento (UE) 2016/679 e con la giurisprudenza dell'UE mantenuta. Ciò significa che, nel valutare il livello di protezione adeguato di un paese terzo, il riferimento pertinente sarà se il paese terzo in questione assicura un livello di protezione «sostanzialmente equivalente» a quello garantito nel Regno Unito.

(77) Per quanto riguarda la procedura, i regolamenti di adeguatezza sono soggetti ai requisiti procedurali «generali» previsti dalla sezione 182 della legge del 2018 sulla protezione dei dati. Secondo tale procedura, quando propone futuri regolamenti di adeguatezza del Regno Unito il segretario di Stato deve consultare l'*Information Commissioner* ([73]). 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 il regolamento e hanno la facoltà di presentare una mozione di annullamento del regolamento stesso entro un termine 40 giorni ([74]).

(78) Ai sensi della sezione 17B, paragrafo 1, della legge del 2018 sulla protezione dei dati, i regolamenti di adeguatezza devono essere riesaminati ad intervalli di tempo non superiori a quattro anni e il segretario di Stato deve monitorare continuativamente gli sviluppi in paesi terzi ed organizzazioni internazionali che potrebbero incidere sulle decisioni di emettere regolamenti di adeguatezza o di modificare o revocare tali regolamenti. Se il segretario di Stato viene a conoscenza del fatto che un determinato paese o una determinata organizzazione non garantisce più un livello adeguato di protezione dei dati personali, deve, nella misura necessaria, modificare o revocare i regolamenti e avviare consultazioni con il paese terzo o l'organizzazione internazionale in questione in maniera da porre rimedio alla mancanza di un livello adeguato di protezione. Tali aspetti procedurali rispecchiano altresì i requisiti corrispondenti del regolamento (UE) 2016/679.

([71]) Fatta eccezione per l'articolo 48 del regolamento (UE) 2016/679, che il Regno Unito ha scelto di non includere nel proprio GDPR. A tale riguardo, occorre innanzitutto ricordare che il criterio da considerare per accertare che sia fornito un livello di protezione adeguato è l'«equivalenza sostanziale» piuttosto che l'identità, come chiarito dalla Corte di giustizia dell'Unione europea (Schrems I, punti da 73 a 74) e riconosciuto dall'EDPB (criteri di riferimento per l'adeguatezza, pag. 3). Pertanto, come spiegato dall'EDPB nei criteri di riferimento per l'adeguatezza, «l'obiettivo non è quello di rispecchiare punto per punto la legislazione europea, ma di stabilire le prescrizioni essenziali e centrali della legislazione in esame». A questo proposito, è importante osservare che, sebbene l'ordinamento giuridico del Regno Unito non contenga formalmente una disposizione identica all'articolo 48, lo stesso effetto è garantito da altre disposizioni e principi giuridici, che prevedono che, in risposta a una richiesta di dati personali da parte di un organo giurisdizionale o un'autorità amministrativa di un paese terzo, i dati personali possono essere trasferiti verso tale paese terzo solo se è in vigore un accordo internazionale — sulla base del quale la sentenza dell'organo giurisdizionale o la decisione amministrativa del paese terzo in questione è riconosciuta o eseguita nel Regno Unito — o se il trasferimento è basato su uno dei meccanismi di trasferimento previsti dal capo V del GDPR del Regno Unito. Più specificatamente, al fine di far rispettare una sentenza straniera, gli organi giurisdizionali del Regno Unito devono essere in grado di fare riferimento alla «common law» o a una legge ordinaria che ne consente l'esecutività. Tuttavia, né la «common law» (cfr. *Adams and Others* v *Cape Industries Plc.*, [1990] 2 W.L.R. 657) né la legge ordinaria prevedono l'esecuzione di sentenze straniere che richiedono il trasferimento di dati in assenza di un accordo internazionale in vigore. Di conseguenza, in assenza di un tale accordo internazionale le richieste di dati non sono soggette ad esecuzione ai sensi del diritto del Regno Unito. Inoltre, qualsiasi trasferimento di dati personali verso paesi terzi — anche su richiesta di un organo giurisdizionale o un'autorità amministrativa stranieri — rimane soggetto alle limitazioni di cui al capo V del GDPR del Regno Unito, che sono identiche alle corrispondenti disposizioni del regolamento (UE) 2016/679, e deve pertanto basarsi su uno dei motivi di trasferimento di cui al capo V, conformemente alle condizioni specifiche cui è soggetto ai sensi di tale capo.

([72]) Le autorità del Regno Unito hanno spiegato che la descrizione di un paese o di un'organizzazione internazionale si riferisce a una situazione nella quale sarebbe necessario effettuare una determinazione specifica e parziale dell'adeguatezza con limitazioni mirate (ad esempio regolamenti di adeguatezza in relazione soltanto a certi tipi di trasferimenti di dati).

([73]) 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.

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

(79) In assenza di regolamenti di adeguatezza, i trasferimenti internazionali possono aver luogo laddove il titolare del trattamento o il responsabile del trattamento abbia fornito garanzie adeguate conformemente all'articolo 46 del GDPR del Regno Unito. Tali garanzie sono analoghe a quelle di cui all'articolo 46 del regolamento (UE) 2016/679. Tra esse figurano strumenti giuridicamente vincolanti e aventi efficacia esecutiva tra autorità pubbliche o organismi pubblici, norme vincolanti d'impresa ([75]), clausole tipo di protezione dei dati, codici di condotta approvati, meccanismi di certificazione approvati e, previa autorizzazione da parte dell'*Information Commissioner*, clausole contrattuali tra titolari del trattamento (o responsabili del trattamento) o accordi amministrativi tra autorità pubbliche. Tuttavia le norme sono state modificate, da un punto di vista procedurale, per funzionare all'interno del quadro del Regno Unito, in particolare le clausole tipo di protezione dei dati possono essere adottate dal segretario di Stato (sezione 17C) o dall'*Information Commissioner* (sezione 119A) in conformità con la legge del 2018 sulla protezione dei dati.

(80) In assenza una decisione di adeguatezza o di garanzie adeguate, un trasferimento può avvenire soltanto sulla base delle deroghe di cui all'articolo 49 del GDPR del Regno Unito ([76]). Il GDPR del Regno Unito non introduce modifiche sostanziali a tali deroghe, rispetto alle norme corrispondenti del regolamento (UE) 2016/679. Ai sensi del GDPR del Regno Unito, così come ai sensi del regolamento (UE) 2016/679, è possibile fare affidamento su talune deroghe soltanto se il trasferimento è occasionale ([77]). Inoltre, nei suoi orientamenti in materia di trasferimenti internazionali, l'ICO chiarisce che: «si dovrebbe fare affidamento su tali deroghe soltanto come vere e proprie 'eccezioni' rispetto alla norma generale secondo la quale non si dovrebbe effettuare un trasferimento limitato fatto salvo il caso in cui esso sia coperto da una decisione di adeguatezza o sussistano garanzie adeguate» ([78]). Per quanto concerne i trasferimenti necessari per importanti motivi di interesse pubblico (articolo 49, paragrafo 1, lettera d)), il segretario di Stato può emettere regolamenti per specificare le circostanze nelle quali un trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale non è necessario per importanti motivi di interesse pubblico. Mediante regolamenti il segretario di Stato può inoltre limitare il trasferimento di una categoria di dati personali verso un paese terzo o un'organizzazione internazionale laddove il trasferimento non possa avvenire sulla base di regolamenti di adeguatezza e il Segretario di Stato ritenga che la limitazione sia necessaria per importanti motivi di interesse pubblico. Ad oggi non sono stati adottati regolamenti di tale sorta.

(81) Questo quadro per i trasferimenti internazionali è diventato applicabile alla fine del periodo di transizione ([79]). Tuttavia il paragrafo 4 dell'allegato 21 della legge del 2018 sulla protezione dei dati (introdotto dai regolamenti DPPEC) prevede che, a partire dalla fine del periodo di transizione, alcuni trasferimenti di dati personali siano trattati come se fossero basati su regolamenti di adeguatezza. Tra tali trasferimenti figurano quelli verso uno Stato SEE, il territorio di Gibilterra, un'istituzione, un organo o un organismo dell'Unione istituito dal trattato UE, o in base ad esso, nonché verso paesi terzi che erano oggetto di una decisione di adeguatezza dell'UE alla fine del periodo di transizione. Di conseguenza i trasferimenti verso tali paesi possono continuare come prima del recesso del Regno Unito dall'Unione europea. Dopo la fine del periodo di transizione, il segretario di Stato deve condurre

([75]) Il GDPR del Regno Unito mantiene le norme di cui all'articolo 47 del regolamento (UE) 2016/679 soggette soltanto a modifiche per adattarle al contesto interno, ad esempio sostituendo i riferimenti all'autorità di controllo competente con l'*Information Commissioner*, eliminando il riferimento al meccanismo di coerenza dal paragrafo 1 ed eliminando l'intero paragrafo 3.

([76]) Ai sensi dell'articolo 49 del GDPR del Regno Unito, i trasferimenti sono possibili se risulta soddisfatta una delle seguenti condizioni: a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate; b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato; c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato; d) il trasferimento sia necessario per importanti motivi di interesse pubblico; e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria; f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto nazionale, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto interno. Inoltre, laddove nessuna delle condizioni di cui sopra sia applicabile, un trasferimento è ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali.

([77]) Il considerando 111 del GDPR del Regno Unito specifica che i trasferimenti in relazione a un contratto o ad un'azione legale sono ammessi soltanto se sono occasionali.

([78]) Linee guida dell'ICO sui trasferimenti internazionali, disponibili al seguente indirizzo: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7.

([79]) Durante un periodo massimo di sei mesi che termina al più tardi il 30 giugno 2021, l'applicabilità di questo nuovo quadro deve essere letta alla luce dell'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 (GU L 444 del 31.12.2020, pag. 14) («l'accordo sugli scambi commerciali e la cooperazione UE-Regno Unito»), disponibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:22020A1231(01)&from=IT.

un riesame di tali accertamenti di adeguatezza entro un termine di quattro anni, ossia entro la fine del dicembre 2024. Secondo la spiegazione fornita dalle autorità del Regno Unito, sebbene il segretario di Stato debba intraprendere tale riesame entro la fine di dicembre 2024, le disposizioni transitorie non comprendono una disposizione relativa alla scadenza e le disposizioni transitorie pertinenti non cesseranno automaticamente di avere effetto se un riesame non viene completato entro la fine di dicembre del 2024.

(82) Infine, per quanto riguarda la futura evoluzione del regime del Regno Unito in materia di trasferimenti internazionali — attraverso l'adozione di nuovi regolamenti di adeguatezza, la conclusione di accordi internazionali o lo sviluppo di altri meccanismi di trasferimento — la Commissione monitorerà attentamente la situazione, valuterà se i diversi meccanismi di trasferimento siano utilizzati in modo da garantire la continuità della protezione e, se necessario, adotterà misure adeguate per affrontare i possibili effetti negativi per tale continuità (cfr. considerando da 278 a 287). Poiché l'UE e il Regno Unito condividono norme analoghe in materia di trasferimenti internazionali, si dovrebbero poter evitare divergenze problematiche anche attraverso la cooperazione, lo scambio di informazioni e la condivisione di esperienze, incluso tra l'ICO e l'EDPB.

2.5.8 *Responsabilizzazione*

(83) Secondo il principio di responsabilizzazione, i soggetti che trattano dati sono tenuti a mettere in atto misure tecniche e organizzative adeguate per rispettare effettivamente i loro obblighi in materia di protezione dei dati e per essere in grado di dimostrare tale rispetto, in particolare all'autorità di controllo competente.

(84) Il principio di responsabilizzazione previsto dal regolamento (UE) 2016/679 è stato mantenuto nell'articolo 5, paragrafo 2, del GDPR del Regno Unito senza modifiche sostanziali e lo stesso vale per l'articolo 24 sulla responsabilità del titolare del trattamento, l'articolo 25 sulla protezione dei dati fin dalla progettazione e protezione per impostazione predefinita e per l'articolo 30 sui registri delle attività di trattamento. Anche gli articoli 35 e 36 sulla valutazione d'impatto sulla protezione dei dati e sulla consultazione preventiva sono stati mantenuti. Gli articoli da 37 a 39 del regolamento (UE) 2016/679 sulla designazione del responsabile della protezione dei dati e sui suoi compiti sono stati mantenuti nel GDPR del Regno Unito senza modifiche sostanziali. Inoltre le disposizioni di cui agli articoli 40 e 42 del regolamento (UE) 2016/679 sui codici di condotta e sulla certificazione sono state mantenute nel GDPR del Regno Unito ([80]).

2.6 **Vigilanza e applicazione**

2.6.1 *Vigilanza indipendente*

(85) Al fine di garantire un adeguato livello di protezione dei dati nella pratica, dovrebbe esistere un'autorità di controllo indipendente cui siano conferiti i poteri di monitorare e assicurare il rispetto delle norme in materia di protezione dei dati. Tale autorità dovrebbe agire in piena indipendenza e imparzialità nell'esercizio delle proprie funzioni e dei propri poteri.

(86) Nel Regno Unito la vigilanza e l'applicazione del rispetto del GDPR del Regno Unito e della legge del 2018 sulla protezione dei dati spettano all'*Information Commissioner*. L'*Information Commissioner* è una «*corporate sole*», ossia un'entità giuridica distinta costituita da un socio unico. Nelle sue attività l'*Information Commissioner* è sostenuto da un ufficio, il cui personale al 31 marzo 2020 era composto di 768 membri permanenti ([81]). Il dipartimento di riferimento dell'*Information Commissioner* è il dipartimento per il Digitale, la cultura, i media e lo sport ([82]).

(87) L'indipendenza dell'*Information Commissioner* è sancita esplicitamente dall'articolo 52 del GDPR del Regno Unito che non attua alcuna modifica sostanziale rispetto all'articolo 52, paragrafi da 1 a 3, del regolamento (UE) 2016/679. L'*Information Commissioner* deve agire in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al GDPR del Regno Unito, non subire pressioni esterne, né dirette né indirette, e non

([80]) Laddove necessario tali riferimenti sono sostituiti con riferimenti alle autorità del Regno Unito. Ad esempio conformemente alla sezione 17 della legge del 2018 sulla protezione dei dati, l'*Information Commissioner* o l'organismo nazionale di accreditamento del Regno Unito può accreditare una persona che soddisfi i requisiti di cui all'articolo 43 del GDPR del Regno Unito affinché monitori il rispetto di una certificazione.

([81]) *Information Commissioner's Annual Report and Financial Statements 2019-2020*, disponibile al seguente indirizzo: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

([82]) Un accordo di gestione disciplina la relazione tra i due. In particolare, tra le principali responsabilità del Dipartimento per il Digitale, la cultura, i media e lo sport in veste di dipartimento promotore figurano: garantire che l'*Information Commissioner* disponga di finanziamenti e risorse adeguati; rappresentare gli interessi dell'*Information Commissioner* in seno al parlamento e presso altri dipartimenti governativi; garantire che sia in atto un quadro nazionale solido di protezione dei dati; e fornire orientamenti e sostegno all'ICO in merito a questioni istituzionali quali questioni immobiliari, relative a locazione finanziaria e appalti (*Management Agreement 2018- 2021*, disponibile al seguente indirizzo: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

sollecitare né accettare istruzioni da alcuno. L'*Information Commissioner* deve astenersi da qualunque azione incompatibile con le proprie funzioni e per tutta la durata del mandato non può esercitare alcuna altra attività incompatibile, remunerata o meno.

(88) Le condizioni per la nomina e la revoca dell'incarico dell'*Information Commissioner* sono stabilite nell'allegato 12 della legge del 2018 sulla protezione dei dati. L'*Information Commissioner* è nominato dalla Regina su raccomandazione del governo in seguito a un concorso equo e aperto. Il candidato deve disporre di qualifiche, competenze e capacità adeguate. In conformità con il *Governance Code on Public Appointments* ([83]) (codice sulla governance sulle nomine pubbliche), un gruppo consultivo di valutazione stila un elenco di candidati nominabili. Prima che il segretario di Stato del dipartimento per il Digitale, la cultura, i media e lo sport finalizzi la propria decisione, la commissione ad hoc pertinente del parlamento deve effettuare uno scrutinio pre-nomina. La posizione di tale commissione è resa pubblica ([84]).

(89) L'*Information Commissioner* resta in carica per un mandato massimo di sette anni. Una persona non può essere nominata *Information Commissioner* più di una volta. Il suo incarico può essere revocato dalla Regina a seguito di una raccomandazione prestata da entrambe le camere del parlamento ([85]). Non può essere presentata alcuna rimozione dall'incarico dell'*Information Commissioner* ad alcuna delle camere del parlamento fintantoché un ministro non abbia presentato una relazione nella quale ha affermato di essere convinto che l'*Information Commissioner* si sia reso colpevole di una colpa grave e/o non soddisfi più le condizioni richieste per lo svolgimento delle sue funzioni spettanti ([86]).

(90) I finanziamenti dell'*Information Commissioner* provengono da tre fonti: i) contributi spese in materia di protezione dei dati versati dai titolari del trattamento, che sono fissati da regolamenti di un segretario di Stato ([87]) (i regolamenti del 2018 in materia di protezione dei dati (contributi spese e informazioni)), e ammontano all'85 %-90 % del bilancio annuale dell'ICO ([88]); ii) una sovvenzione che può essere corrisposta dal governo all'*Information Commissioner*. Una sovvenzione viene utilizzata principalmente per finanziare i costi operativi dell'*Information Commissioner* in relazione a compiti concernenti attività non correlate alla protezione di dati ([89]); e iii) commissioni addebitate per servizi ([90]). Attualmente, tali commissioni non vengono addebitate.

(91) Le funzioni generali dell'*Information Commissioner* in relazione al trattamento di dati personali al quale si applica il GDPR del Regno Unito sono stabilite nell'articolo 57 del GDPR del Regno Unito, il quale rispecchia da vicino le norme corrispondenti del regolamento (UE) 2016/679. Le sue funzioni comprendono il monitoraggio e l'assicurazione del rispetto del GDPR del Regno Unito, la promozione della sensibilizzazione del pubblico, la gestione dei reclami promossi dagli interessati, lo svolgimento di indagini, ecc. Inoltre la sezione 115 della legge del 2018 sulla protezione dei dati stabilisce altre funzioni generali dell'*Information Commissioner* che comprendono un obbligo di consigliare il parlamento, il governo e altre istituzioni e organismi sulle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone in relazione al trattamento dei dati personali, nonché un potere di emettere, su iniziativa propria dell'*Information Commissioner* o su richiesta, pareri indirizzati al parlamento, al governo o altre istituzioni e organismi nonché al pubblico su qualsiasi questione

([83]) *Governance Code on Public Appointments*, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf.

([84]) *Second Report of Session 2015-2016 of the Culture, Media and Sports Committee at the House of Commons*, disponibile al seguente indirizzo: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([85]) Una raccomandazione, in inglese «*address*», è una mozione presentata dinanzi al parlamento che intende rendere il monarca consapevole dei pareri del parlamento in merito a una questione specifica.

([86]) Paragrafo 3, punto 3, dell'allegato 12 della legge del 2018 sulla protezione dei dati.

([87]) Sezione 137 della legge del 2018 sulla protezione dei dati, cfr. considerando 17.

([88]) Gli articoli 137 e 138 della legge del 2018 sulla protezione dei dati contengono diverse garanzie destinate ad assicurare che i contributi spese siano fissati a un livello adeguato. In particolare la sezione 137, paragrafo 4, elenca le questioni che il segretario di Stato deve considerare quando emette regolamenti che specificano l'importo che le diverse organizzazioni devono versare; in secondo luogo la sezione 138, paragrafo 1, e la sezione 182, della legge del 2018 sulla protezione dei dati contengono un requisito giuridico che impone al segretario di Stato di consultare l'*Information Commissioner* e altri rappresentanti delle persone che potrebbero essere interessate dai regolamenti prima di emettere questi ultimi affinché i loro pareri possano essere presi in considerazione. Inoltre, ai sensi della sezione 138, paragrafo 2, della legge del 2018 sulla protezione dei dati, l'*Information Commissioner* è tenuto a mantenere sotto riesame i regolamenti relativi ai diritti e agli onorari e può presentare proposte al segretario di Stato per emendamenti da effettuare in relazione a tali regolamenti. Infine, fatta eccezione nel caso in cui i regolamenti siano emessi semplicemente per tenere conto di un aumento dell'indice dei prezzi al dettaglio (nel qual caso saranno soggetti alla procedura di risoluzione negativa), i regolamenti sono soggetti alla procedura di risoluzione affermativa e non possono essere emessi fino a quando non sono stati approvati mediante una risoluzione di ogni camera del parlamento.

([89]) Il *Management Agreement* ha chiarito che «il segretario di Stato può effettuare pagamenti all'ICO utilizzando somme di denaro messe a disposizione dal parlamento ai sensi del paragrafo 9 dell'allegato 12 della legge del 2018 sulla protezione dei dati. In seguito a consultazione con l'*Information Commissioner*, il dipartimento per il Digitale, la cultura, i media e lo sport corrisponderà all'ICO somme adeguate (la sovvenzione) per i costi amministrativi e per l'esercizio delle funzioni dell'ICO in relazione a una serie di funzioni specifiche, compresa la libertà di informazione» (*Management Agreement 2018-2021*, punto 1.12, cfr. nota 82).

([90]) Sezione 134 della legge del 2018 sulla protezione dei dati.

relativa alla protezione dei dati personali. Ai fini del mantenimento dell'indipendenza del potere giudiziario, l'*Information Commissioner* non è autorizzato a esercitare le sue funzioni in relazione al trattamento di dati personali da parte di un soggetto o di un organo giurisdizionale che agisce nell'esercizio delle proprie funzioni giurisdizionali. Tuttavia la vigilanza sul potere giudiziario è assicurata da organismi specializzati (cfr. considerando da 99 a 103).

2.6.2 *Applicazione (sanzioni comprese)*

(92) I poteri dell'*Information Commissioner* sono stabiliti dall'articolo 58 del GDPR del Regno Unito, che non introduce modifiche sostanziali al corrispondente articolo del regolamento (UE) 2016/679. La legge del 2018 sulla protezione dei dati stabilisce norme supplementari sulle modalità con cui tali poteri possono essere esercitati. In particolare, l'*Information Commissioner* dispone dei poteri per: a) ordinare al titolare del trattamento e al responsabile del trattamento (e in determinate circostanze a qualsiasi altra persona) di fornire informazioni necessarie notificando un avviso di informazione («avviso di informazione») ([91]); b) effettuare indagini e verifiche trasmettendo un avviso di valutazione, che può imporre al titolare del trattamento o al responsabile del trattamento di consentire all'*Information Commissioner* di accedere a locali specificati, ispezionare o esaminare documenti o apparecchiature, e interrogare persone che trattano dati personali per conto del titolare del trattamento, ecc. («avviso di valutazione») ([92]); c) ottenere altrimenti l'accesso a documenti, ecc. di titolari del trattamento e responsabili del trattamento così come accesso ai loro locali in conformità con la sezione 154 della legge del 2018 sulla protezione dei dati («poteri di accesso e ispezione»); d) esercitare poteri correttivi, anche mediante avvertimenti e ammonimenti, oppure emettere ordini per mezzo di un avviso di esecuzione, che impone ai titolari del trattamento/responsabili del trattamento di adottare o di astenersi dall'adottare misure specificate, in particolare di compiere qualsiasi azione specificata dall'articolo 58, paragrafo 2, lettere da c) a g) e lettera j) del GDPR del Regno Unito («avviso di esecuzione») ([93]); e) comminare sanzioni amministrative pecuniarie sotto forma di un avviso di irrogazione di sanzioni («avviso di irrogazione di sanzioni») ([94]). Quest'ultimo può essere emesso anche qualora un'autorità pubblica non abbia rispettato le disposizioni del GDPR del Regno Unito ([95]).

(93) Il documento *Regulatory Action Policy* dell'ICO stabilisce le circostanze nelle quali l'*Information Commissioner* emetterà un avviso di informazione, valutazione, esecuzione e irrogazione di sanzioni ([96]). Un avviso di esecuzione notificato a seguito di un inadempimento da parte di un titolare del trattamento o di un responsabile del trattamento può esclusivamente imporre i requisiti che l'*Information Commissioner* ritiene opportuni al fine di porre rimedio a tale inadempimento. Gli avvisi di esecuzione e di irrogazione di sanzioni possono essere emessi nei confronti di un titolare del trattamento o di un responsabile del trattamento in relazione a violazioni del capo II del GDPR del Regno Unito (principi di trattamento), degli articoli da 12 a 22 (diritti dell'interessato), degli articoli da 25 a 39 (obblighi dei titolari del trattamento e dei responsabili del trattamento) e degli articoli da 44 a 49 (trasferimenti internazionali) del GDPR del Regno Unito. Un avviso di esecuzione può essere notificato anche nel caso in cui un titolare del trattamento non abbia rispettato l'obbligo di versare un contributo spese fissato in regolamenti emessi ai sensi della sezione 137 della legge del 2018 sulla protezione dei dati. Inoltre un organismo di controllo ai sensi dell'articolo 41 o un fornitore di certificazione può vedersi notificare un avviso di esecuzione nel caso in cui non rispetti gli obblighi cui è soggetto ai sensi del GDPR del Regno Unito. Un avviso di irrogazione di sanzioni può essere notificato anche a una persona che non ha rispettato un avviso di informazione, un avviso di valutazione o un avviso di esecuzione.

(94) L'avviso di irrogazione di sanzioni impone a una persona di corrispondere all'*Information Commissioner* un importo specificato nell'avviso stesso. Nello stabilire se notificare un avviso di irrogazione di sanzioni a una persona e determinare l'ammontare della sanzione, l'*Information Commissioner* deve tener conto delle questioni elencate all'articolo 83, paragrafi 1 e 2, del GDPR del Regno Unito, che sono disposizioni identiche alle norme corrispondenti del regolamento (UE) 2016/679 ([97]). Conformemente all'articolo 83, paragrafi 4 e 5, gli importi massimi delle sanzioni amministrative pecuniarie in caso di mancato rispetto degli obblighi di cui a tali disposizioni sono rispettivamente 8 700 000 GBP o 17 500 000 GBP. Nel caso di un'impresa, l'*Information Commissioner* può altresì imporre sanzioni pecuniarie espresse in percentuale rispetto al fatturato mondiale annuo, laddove superiore.

([91]) Sezione 142 della legge del 2018 sulla protezione dei dati (soggetto alle limitazioni di cui alla sezione 143 della medesima legge).
([92]) Sezione 146 della legge del 2018 sulla protezione dei dati (soggetto alle limitazioni di cui alla sezione 147 della medesima legge).
([93]) Sezioni da 149 a 151 della legge del 2018 sulla protezione dei dati (soggetto alle limitazioni di cui alla sezione 152 della legge del 2018 sul recesso del 2018).
([94]) Sezione 155 della legge del 2018 sulla protezione dei dati e articolo 83 del GDPR del Regno Unito.
([95]) Ciò risulta dalla sezione 155, paragrafo 1, in combinato disposto con la sezione 149, paragrafi 2 e 5, della legge del 2018 sulla protezione dei dati, e dalla sezione 156, punto 4, della medesima legge, che limita l'emissione di avvisi di irrogazione di sanzioni solo nei confronti dei *Crown Estate Commissioners* e dei titolari del trattamento per la *Royal Household* ai sensi della sezione 209, punto 4, della medesima legge.
([96]) *Regulatory Action Policy*, disponibile al seguente indirizzo: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([97]) Compresi la natura e la gravità della violazione (in considerazione della natura, dell'oggetto o della finalità del trattamento in questione nonché del numero di interessati e del livello del danno da essi subito), le misure adottate dal titolare del trattamento per attenuare il danno subito dagli interessati, il grado di responsabilità del titolare del trattamento o del responsabile del trattamento (tenendo conto delle misure tecniche e organizzative da essi messe in atto), eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento; il grado di cooperazione con l'*Information Commissioner*, le categorie di dati personali interessate dalla violazione, eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Come nelle disposizioni equivalenti del regolamento (UE) 2016/679, tali importi sono fissati al 2 % e al 4 % all'articolo 83, paragrafi 4 e 5, rispettivamente. In caso di mancato rispetto di un avviso di informazione, di un avviso di valutazione o un di avviso di esecuzione, l'importo massimo della sanzione che può essere comminata da un avviso di irrogazione di sanzioni è 17 500 000 GBP o, nel caso di un'impresa, il 4 % del fatturato mondiale annuo, se più elevato.

(95) Il GDPR del Regno Unito unitamente alla legge del 2018 sulla protezione dei dati hanno anche rafforzato altri poteri dell'*Information Commissioner*. Ad esempio l'*Information Commissioner* può ora condurre audit obbligatori in relazione a tutti i titolari del trattamento e i responsabili del trattamento attraverso l'uso di avvisi di valutazione, mentre nel contesto della legislazione precedente, la legge del 1998 sulla protezione dei dati, l'*Information Commissioner* disponeva di tale potere soltanto nei confronti di organizzazioni del governo centrale e di organizzazioni della sanità, mentre gli altri soggetti dovevano acconsentire di sottoporsi a un audit.

(96) Dall'introduzione del regolamento (UE) 2016/679, l'ICO gestisce circa 40 000 reclami l'anno promossi da interessati ([98]) e, in aggiunta, svolge circa 2 000 indagini d'ufficio ([99]). La maggior parte dei reclami è correlata ai diritti di accesso e alla comunicazione di dati. A seguito delle sue indagini, l'*Information Commissioner* sta adottando misure di esecuzione in un'ampia gamma di settori. Più specificamente, secondo l'ultima relazione annuale dell'*Information Commissioner* (2019-2020) ([100]), quest'ultimo ha emesso 54 avvisi di informazione, 8 avvisi di valutazione, 7 avvisi di esecuzione, 4 diffide, ha avviato 8 procedimenti giudiziari e ha irrogato 15 sanzioni pecuniarie durante il periodo di riferimento ([101]).

(97) Queste misure comprendono diverse sanzioni pecuniarie significative imposte ai sensi del regolamento (UE) 2016/679 e della legge del 2018 sulla protezione dei dati. In particolare, nell'ottobre del 2020, l'*Information Commissioner* ha irrogato una sanzione pecuniaria di 20 milioni di GBP a una compagnia aerea britannica per una violazione dei dati che ha interessato più di 400 000 clienti. Alla fine di ottobre del 2020, una catena alberghiera internazionale si è vista imporre una sanzione pecuniaria di 18,4 milioni di GBP per non aver garantito la sicurezza dei dati personali di milioni di clienti; mentre nel novembre del 2020 una sanzione pecuniaria di 1,25 milioni di GBP è stata irrogata a un fornitore britannico di servizi che vende online biglietti per eventi per non aver protetto i dettagli di pagamento dei clienti ([102]).

(98) Oltre ai poteri di esecuzione dell'*Information Commissioner* descritti al considerando 92, talune violazioni della legislazione in materia di protezione dei dati costituiscono reati e possono pertanto essere soggette a sanzioni penali (sezione 196 della legge del 2018 sulla protezione dei dati). Si tratta ad esempio dell'ottenimento e della comunicazione, in modo consapevole o incauto, di dati personali senza il consenso del titolare del trattamento, della trasmissione di dati personali a un'altra persona senza il consenso del titolare del trattamento ([103]), della reidentificazione di informazioni a partire da dati personali anonimizzati senza il consenso del titolare del trattamento responsabile dell'anonimizzazione dei dati personali ([104]), dell'ostruzione intenzionale dell'esercizio dei poteri dell'*Information Commissioner* in relazione all'ispezione di dati personali conformemente agli obblighi internazionali ([105]), del rilascio di dichiarazioni false in risposta a un avviso di informazione o della distruzione di informazioni relative ad avvisi di informazione e valutazione ([106]).

([98]) Secondo le informazioni fornite dalle autorità del Regno Unito, nel periodo oggetto della relazione annuale 2019-2020 dell'*Information Commissioner*, nel 25 % circa dei casi non è stata riscontrata alcuna violazione; nel 29 % circa dei casi l'interessato è stato invitato a far presente la preoccupazione innanzitutto al titolare del trattamento, ad attendere la risposta del titolare del trattamento o a continuare un dialogo in corso con il titolare del trattamento; nel 17 % circa dei casi, non è stata riscontrata alcuna violazione ma è stato fornito un consiglio al titolare del trattamento; in circa il 25 % dei casi l'*Information Commissioner* ha riscontrato una violazione e ha fornito un consiglio al titolare del trattamento oppure ha imposto a quest'ultimo di intraprendere determinate azioni; in circa il 3 % dei casi è stato stabilito che il reclamo non rientrava nell'ambito di applicazione del regolamento (UE) 2016/679; mentre circa l'1 % dei casi è stato deferito a un'altra autorità di protezione dei dati nel quadro del comitato europeo per la protezione dei dati.

([99]) L'ICO può avviare tali indagini sulla base di informazioni ricevute da una varietà di fonti, comprese le notifiche di violazione dei dati personali, i rinvii da altre autorità pubbliche del Regno Unito o da autorità straniere di protezione dei dati, nonché i reclami da parte di persone fisiche o di organizzazioni della società civile.

([100]) *Information Commissioner's Annual Report and Financial Statements 2019-2020* (cfr. nota 81).

([101]) Secondo la precedente relazione annuale riguardante il periodo 2018-2019, l'*Information Commissioner* aveva emesso 22 avvisi di irrogazione di sanzioni ai sensi della legge del 1998 sulla protezione dei dati durante il periodo di riferimento, irrogando sanzioni pecuniarie per un importo complessivo pari a 3 010 610 GBP, comprese due sanzioni pecuniarie di 500 000 GBP (l'importo massimo consentito dalla legge del 1998 sulla protezione dei dati). Nel 2018 l'*Information Commissioner* ha in particolare condotto un'indagine in merito all'utilizzo di analisi dei dati per finalità politiche in seguito alle rivelazioni di Cambridge Analytica. Tale indagine ha portato a una relazione strategica, una serie di raccomandazioni, una sanzione pecuniaria di 500 000 GBP nei confronti di Facebook e un avviso di esecuzione indirizzato ad Aggregate IQ, un intermediario di dati canadese, tramite il quale è stato ordinato all'azienda di cancellare i dati personali da essa detenuti in merito a cittadini e residenti del Regno Unito (cfr. *Information Commissioner's Annual Report and Financial Statement 2018-2019*, disponibile al seguente indirizzo: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf).

([102]) Per una sintesi delle azioni di applicazione adottate, cfr. sito web dell'ICO, disponibile al seguente indirizzo: https://ico.org.uk/action-weve-taken/enforcement/.

([103]) Sezione 170 della legge del 2018 sulla protezione dei dati.

([104]) Sezione 171 della legge del 2018 sulla protezione dei dati.

([105]) Sezione 119 della legge del 2018 sulla protezione dei dati.

([106]) Sezioni 144 e 148 della legge del 2018 sulla protezione dei dati.

2.6.3 *Vigilanza sul potere giudiziario*

(99) La vigilanza sul trattamento di dati personali da parte di organi giurisdizionali e della magistratura è duplice. Se un titolare di funzioni giurisdizionali o un organo giurisdizionale non agisce nell'esercizio delle proprie funzioni giurisdizionali, la vigilanza è esercitata dall'ICO. Quando il titolare del trattamento opera nell'esercizio delle proprie funzioni giurisdizionali, l'ICO non può esercitare le sue funzioni di vigilanza ([107]) e detta vigilanza è esercitata da organismi speciali. Ciò riflette l'approccio adottato dal regolamento (UE) 2016/679 (articolo 55, paragrafo 3).

(100) In particolare, nel secondo caso, per gli organi giurisdizionali di Inghilterra e Galles e per gli organi giurisdizionali di primo grado e di grado superiore di Inghilterra e Galles, tale vigilanza è attuata dal *Judicial Data Protection Panel* ([108]) (comitato sulla protezione dei dati da parte del potere giudiziario). Inoltre il *Lord Chief Justice* (Lord Giudice capo) e il *Senior President of Tribunals* (Presidente senior degli organi giurisdizionali) hanno emesso un'informativa sulla protezione dei dati ([109]) che stabilisce le modalità con cui gli organi giurisdizionali di Inghilterra e Galles trattano personali per espletare una funzione giudiziaria. Un'informativa analoga è stata emessa dalla magistratura dell'Irlanda del Nord ([110]) e della Scozia ([111]).

(101) Inoltre, in Irlanda del Nord, il Lord Giudice capo dell'Irlanda del Nord ha nominato un giudice dell'Alta Corte *Data Supervisory Judge* (DSJ, Giudice incaricato del controllo sui dati) ([112]), e ha rivolto alla magistratura dell'Irlanda del Nord orientamenti in merito alle azioni da intraprendere in caso di perdita o potenziale perdita di dati e al processo per affrontare qualsiasi problema derivante da tale circostanza ([113]).

(102) In Scozia il *Lord President* (Lord Presidente) ha nominato un Giudice incaricato del controllo sui dati affinché indaghi su eventuali reclami per motivi di protezione dei dati. Ciò è sancito nelle norme sui reclami in materia giudiziaria che rispecchiano quelle stabilite per Inghilterra e Galles ([114]).

(103) Infine, nell'ambito della Corte suprema uno dei giudici è incaricato di vigilare in merito alla protezione dei dati.

2.6.4 *Mezzi di ricorso*

(104) Al fine di assicurare una protezione adeguata e, in particolare, il rispetto dei diritti individuali, l'interessato dovrebbe avere a disposizione mezzi di ricorso effettivi in sede amministrativa e giudiziale, compreso il risarcimento dei danni.

([107]) Sezione 117 della legge del 2018 sulla protezione dei dati.

([108]) Tale comitato è competente per l'erogazione di orientamenti e formazione alla magistratura. Si occupa inoltre di reclami promossi da interessati in relazione al trattamento di dati personali da parte degli organi giurisdizionali e di persone fisiche che agiscono nell'esercizio delle proprie funzioni giurisdizionali. Tale comitato mira a mettere a disposizione mezzi attraverso i quali possa essere risolto qualsiasi reclamo. Qualora un reclamante non sia soddisfatto di una decisione del comitato e abbia fornito ulteriori prove, il comitato potrebbe riconsiderare la propria decisione. Sebbene il comitato in sé non commini sanzioni pecuniarie, laddove il comitato ritenga che sussista una violazione sufficientemente grave della legge del 2018 sulla protezione dei dati, può riferirlo all'*Judicial Conduct Investigation Office* (Ufficio investigativo sulla condotta giudiziaria, JCIO), che indagherà in merito al reclamo. Qualora il reclamo venga accolto, spetta al *Lord Chancellor* (Lord Cancelliere) e al Lord Giudice capo (o a un alto magistrato delegato ad agire per suo conto) decidere quale azione dovrebbe essere intrapresa nei confronti del funzionario in questione. Ciò potrebbe comprendere, in base alla gravità: consiglio formale, avvertimento formale e ammonimento e, in ultima istanza, revoca dell'incarico. Se una persona fisica non è soddisfatta del modo in cui il reclamo è stato indagato dal JCIO può proporre ulteriore reclamo presso il *Judicial Appointments and Conduct Ombudsman* (mediatore per la condotta e le nomine in ambito giudiziario) (cfr. https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Tale mediatore ha il potere di chiedere a JCIO di effettuare un'ulteriore indagine in merito a un reclamo e può proporre che il reclamante riceva un risarcimento laddove ritenga che quest'ultimo abbia subito un danno in ragione della cattiva amministrazione.

([109]) L'informativa sulla protezione dei dati emessa dal Lord Giudice capo e dal Presidente senior degli organi giurisdizionali è disponibile al seguente indirizzo: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([110]) L'informativa sulla protezione dei dati emessa dal Lord Giudice capo dell'Irlanda del Nord è disponibile al seguente indirizzo: https://judiciaryni.uk/data-privacy.

([111]) L'informativa sulla protezione dei dati per gli organi giurisdizionali della Scozia è disponibile al seguente indirizzo: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([112]) Il Giudice incaricato del controllo sui dati fornisce indicazioni alla magistratura e indaga in merito a violazioni e/o reclami in relazione al trattamento di dati personali da parte di organi giurisdizionali o persone fisiche che agiscono nell'esercizio delle proprie funzioni giurisdizionali.

([113]) Laddove si ritenga che il reclamo o la violazione sia grave, il caso viene rinviato al *Judicial Complaints Officer* (Funzionario per i reclami in materia giudiziaria) per ulteriori indagini conformemente al codice di pratica sui reclami dell'Irlanda del Nord del Lord Giudice capo. L'esito di tale reclamo potrebbe comprendere: nessuna ulteriore azione, un consiglio, formazione o tutoraggio, un avvertimento informale, un avvertimento formale, un avvertimento finale, una limitazione dell'esercizio della professione o un rinvio a un organo giurisdizionale. Il codice di pratica sui reclami pubblicato dal Lord Giudice capo in Irlanda del Nord è disponibile al seguente indirizzo: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf.

([114]) Qualsiasi reclamo fondato è oggetto di indagine da parte del Giudice incaricato del controllo sui dati e rinviato al Lord Presidente che ha il potere di emettere un consiglio, un avvertimento formale o un ammonimento qualora ritenga ciò necessario (norme equivalenti esistono per i membri degli organi giurisdizionali e sono disponibili al seguente indirizzo: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

(105) Innanzitutto l'interessato ha il diritto di proporre reclamo presso l'*Information Commissioner* qualora ritenga che, in relazione ai dati personali che lo riguardano, sia stata commessa una violazione del GDPR del Regno Unito ([115]). Il GDPR del Regno Unito mantiene le norme di cui all'articolo 77 del regolamento (UE) 2016/679 in merito a tale diritto senza modifiche sostanziali. Lo stesso vale per l'articolo 57, paragrafo 1, lettera f) e per l'articolo 57, paragrafo 2, che stabiliscono i compiti dell'*Information Commissioner* in relazione alla gestione dei reclami. Come descritto nei considerando 92 e 98, l'*Information Commissioner* ha il potere di valutare il rispetto del GDPR del Regno Unito e della legge del 2018 sulla protezione dei dati da parte del titolare del trattamento e del responsabile del trattamento, di richiede loro di adottare, o di astenersi dall'adottare, misure necessarie in caso di non conformità nonché di irrogare sanzioni pecuniarie.

(106) In secondo luogo il GDPR del Regno Unito e la legge del 2018 sulla protezione dei dati riconoscono il diritto di ricorso nei confronti dell'*Information Commissioner*. Ai sensi dell'articolo 78, paragrafo 1, del GDPR del Regno Unito, una persona fisica ha diritto ad un ricorso giurisdizionale effettivo nei confronti di una decisione giuridicamente vincolante dell'*Information Commissioner* che la riguarda. Nel contesto del controllo giurisdizionale, l'organo giurisdizionale esamina la decisione impugnata nel ricorso e valuta se l'*Information Commissioner* ha agito in maniera lecita. Inoltre, a norma dell'articolo 78, paragrafo 2, del GDPR del Regno Unito, se l'*Information Commissioner* non gestisce in maniera adeguata un reclamo promosso da un interessato ([116]) il reclamante ha accesso al ricorso giurisdizionale e può adire un *First-tier Tribunal* chiedendogli di ordinare all'*Information Commissioner* di adottare misure adeguate per dare seguito al reclamo oppure di informare il reclamante in merito ai progressi compiuti in relazione al reclamo ([117]). Inoltre qualsiasi persona che riceva la notifica di uno degli avvisi di cui sopra (di informazione, di valutazione, di esecuzione o di irrogazione di sanzioni) dall'*Information Commissioner* può impugnarlo adendo un *First-tier Tribunal* ([118]). Laddove quest'ultimo ritenga che la decisione dell'*Information Commissioner* non sia conforme alla legge o che questi avrebbe dovuto esercitare il proprio potere discrezionale in modo diverso, detto organo deve accogliere il ricorso oppure sostituire l'avviso o la decisione con un altro avviso o un'altra decisione che l'*Information Commissioner* avrebbe potuto emettere o rendere.

(107) In terzo luogo le persone fisiche possono proporre un ricorso giurisdizionale nei confronti di titolari del trattamento e responsabili del trattamento direttamente adendo gli organi giurisdizionali conformemente all'articolo 79 del GDPR del Regno Unito e alla sezione 167 della legge del 2018 sulla protezione dei dati. Se, su domanda di un interessato, un organo giurisdizionale è convinto che sia stata commessa una violazione dei diritti dell'interessato sanciti dalla legislazione in materia di protezione dei dati, esso può ordinare al titolare del trattamento, in relazione al trattamento, o a un responsabile del trattamento che agisce per conto di tale titolare del trattamento, di adottare le misure specificate nell'ordinanza oppure di astenersi dall'adottare le misure specificate nell'ordinanza.

(108) Inoltre, a norma dell'articolo 82 del GDPR del Regno Unito e della sezione 168 della legge del 2018 sulla protezione dei dati, chiunque subisca un danno materiale o immateriale a causa di una violazione del GDPR del Regno Unito ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento. Le norme relative al risarcimento e alla responsabilità di cui all'articolo 82, paragrafi da 1 a 5, del GDPR del Regno Unito sono identiche alle norme corrispondenti del regolamento (UE) 2016/679. Conformemente alla sezione 168 della legge del 2018 sulla protezione dei dati, i danni immateriali comprendono anche la sofferenza. Ai sensi dell'articolo 80 del GDPR del Regno Unito, l'interessato ha altresì il diritto di incaricare un organismo rappresentativo o un'organizzazione rappresentativa affinché promuova reclamo presso l'*Information Commissioner* per suo conto (ai sensi dell'articolo 77 del GDPR del Regno Unito) ed eserciti per suo conto i diritti di cui all'articolo 78 (diritto a un ricorso giurisdizionale effettivo nei confronti dell'*Information Commissioner*), all'articolo 79 (diritto a un ricorso giurisdizionale effettivo nei confronti di un titolare del trattamento o di un responsabile del trattamento) e all'articolo 82 (diritto al risarcimento e responsabilità) del GDPR del Regno Unito.

(109) In quarto luogo, e in aggiunta ai mezzi di ricorso sopra citati, nella misura in cui una persona ritenga che i suoi diritti, anche in materia di tutela della vita privata e protezione dei dati, siano stati violati da autorità pubbliche, può ottenere rimedio adendo gli organi giurisdizionali del Regno Unito conformemente alla legge del 1998 sui diritti umani ([119]). Una persona fisica che sostenga che un'autorità pubblica ha agito (o propone di agire) in maniera incompatibile con un diritto sancito da una convenzione e pertanto in maniera illecita ai sensi della sezione 6, paragrafo 1, della legge del 1998 sui diritti umani può avviare un procedimento contro l'autorità in questione dinanzi l'organo giurisdizionale adeguato oppure fare affidamento sui diritti interessati nel contesto di qualsiasi procedimento legale, quando tale persona è (o diventi) vittima dell'atto illecito.

(110) Laddove l'organo giurisdizionale constati che un atto di un'autorità pubblica è illecito, può concedere tale misura o provvedimento oppure emettere una tale ordinanza, entro i suoi poteri, nella misura che ritiene giusta ed adeguata ([120]). L'organo giurisdizionale può altresì dichiarare che una disposizione del diritto primario è incompatibile con un diritto garantito dalla convenzione.

([115]) Articolo 77 del GDPR del Regno Unito.

([116]) La sezione 166 della legge del 2018 sulla protezione dei dati fa riferimento specificamente alle seguenti situazioni: a) l'*Information Commissioner* non adotta misure adeguate per dare seguito al reclamo; b) l'*Information Commissioner* non fornisce al reclamante informazioni in merito ai progressi compiuti in relazione al reclamo o in merito all'esito del reclamo prima dello scadere di un termine di 3 mesi a decorrere dal momento della ricezione del reclamo da parte dello stesso; oppure c) laddove l'esame del reclamo da parte dell'*Information Commissioner* non venga concluso entro tale termine, quest'ultimo non fornisce al reclamante tali informazioni durante un successivo periodo di 3 mesi.

([117]) Articolo 78, paragrafo 2, del GDPR del Regno Unito e sezione 166 della legge del 2018 sulla protezione dei dati.

([118]) Articolo 78, paragrafo 1, del GDPR del Regno Unito e sezione 162 della legge del 2018 sulla protezione dei dati.

([119]) Sezione 7, paragrafo 1, della legge del 1998 sui diritti umani. Conformemente alla sezione 7, paragrafo 7, una persona è vittima di un atto illecito soltanto se lo sarebbe ai sensi della sezione 34 della convenzione europea dei diritti dell'uomo qualora venisse presentato un ricorso alla Corte europea dei diritti dell'uomo in relazione a tale atto.

([120]) Sezione 8, paragrafo 1, della legge del 1998 sui diritti umani.

(111) Infine, dopo aver esperito i mezzi di ricorso nazionali, una persona fisica può ottenere rimedio adendo la Corte europea dei diritti dell'uomo per violazioni dei diritti garantiti ai sensi della convenzione europea dei diritti dell'uomo.

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

(112) La Commissione ha inoltre valutato il quadro giuridico del Regno Unito per la raccolta e l'uso successivo dei dati personali trasferiti ad operatori economici nel Regno Unito da parte delle autorità pubbliche del Regno Unito nell'interesse pubblico, in particolare per attività di contrasto penale e per finalità di sicurezza nazionale (in appresso denominato «accesso da parte di pubbliche amministrazioni»). Nel valutare se le condizioni in base alle quali l'accesso da parte delle pubbliche amministrazioni ai dati trasferiti verso il Regno Unito ai sensi della presente decisione soddisfino la verifica dell'«equivalenza sostanziale» ai sensi dell'articolo 45, paragrafo 1, del regolamento (UE) 2016/679, come interpretato dalla Corte di giustizia dell'Unione europea alla luce della Carta dei diritti fondamentali, la Commissione ha tenuto conto in particolare dei criteri illustrati in appresso.

(113) Innanzitutto qualsiasi limitazione dell'esercizio del diritto alla protezione dei dati personali deve essere prevista dalla legge e implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato ([121]).

(114) In secondo luogo, per soddisfare il requisito di proporzionalità secondo cui le deroghe e le limitazioni alla protezione dei dati personali devono operare nei limiti dello stretto necessario in una società democratica per soddisfare gli obbiettivi specifici di interesse generale equivalenti a quelli riconosciuti dall'Unione, la legislazione del paese terzo in questione che consente tale ingerenza deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura in questione e impongano requisiti minimi in modo che le persone i cui dati sono trasferiti dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi ([122]). In particolare, essa deve indicare in quali circostanze e a quali condizioni possa essere adottata una misura che prevede il trattamento di siffatti dati ([123]) nonché assoggettare il soddisfacimento di tali requisiti alla vigilanza indipendente ([124]).

(115) In terzo luogo tale legislazione deve essere giuridicamente vincolante ai sensi del diritto interno e tali requisiti giuridici devono non solo essere vincolanti per le autorità, ma anche azionabili dinanzi gli organi giurisdizionali nei confronti di autorità del paese terzo di cui trattasi ([125]). In particolare gli interessati devono disporre della possibilità di esperire mezzi di ricorso dinanzi a un giudice indipendente e imparziale al fine di avere accesso a dati personali che li riguardano, o di ottenere la rettifica o la soppressione di tali dati ([126]).

3.1 Quadro giuridico generale

(116) Trattandosi di un esercizio di poteri da parte di un'autorità pubblica, l'accesso da parte delle pubbliche amministrazioni nel Regno Unito deve avvenire nel pieno rispetto della legge. Il Regno Unito ha ratificato la convenzione europea dei diritti dell'uomo (cfr. considerando 9) e tutte le autorità pubbliche del Regno Unito sono tenute ad agire in conformità con tale convenzione ([127]). L'articolo 8 della convenzione prevede che qualsiasi ingerenza in relazione alla tutela della vita privata debba avvenire in conformità con la legge, nell'interesse di uno degli obiettivi di cui all'articolo 8, paragrafo 2, e in maniera proporzionata alla luce di tale obiettivo. L'articolo 8 richiede inoltre che tale ingerenza sia «prevedibile», ossia che la sua base giuridica sia chiara e precisa, e che la legislazione specifichi le garanzie adeguate per prevenire gli abusi.

(117) Inoltre, nella sua giurisprudenza, la Corte europea dei diritti dell'uomo ha specificato che qualsiasi ingerenza nel diritto alla tutela della vita privata e alla protezione dei dati dovrebbe essere soggetta ad un sistema di vigilanza efficace, indipendente e imparziale da parte di un giudice o un altro organo indipendente ([128]) (ad esempio un'autorità amministrativa o un organo parlamentare).

([121]) Cfr. *Schrems II*, punti 174 e 175 e giurisprudenza citata. Cfr. anche, per quanto riguarda l'accesso da parte di autorità pubbliche di Stati membri, sentenza della Corte di giustizia del 6 ottobre 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, punto 65; e sentenza della Corte di giustizia del 6 ottobre 2020, *La Quadrature du Net e a.*, cause riunite C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791, punto 175.

([122]) Cfr. *Schrems II*, punti 176 e 181, nonché la giurisprudenza citata. Cfr. anche, per quanto riguarda l'accesso da parte di autorità pubbliche di Stati membri, *Privacy International*, punto 68; e *La Quadrature du Net and Others*, punto 132.

([123]) Cfr. *Schrems II*, punto 176. Cfr. anche, per quanto riguarda l'accesso da parte di autorità pubbliche di Stati membri, *Privacy International*, punto 68; e *La Quadrature du Net and Others*, punto 132.

([124]) Cfr. *Schrems II*, punto 179.

([125]) Cfr. *Schrems II*, punti 181 e 182.

([126]) Cfr. *Schrems I*, punto 95 e Schrems *II*, punto 194. A tale riguardo la Corte di giustizia dell'Unione europea ha sottolineato in particolare che il rispetto dell'articolo 47 della Carta dei diritti fondamentali, garantendo il diritto a un ricorso effettivo dinanzi un organo giurisdizionale indipendente e imparziale, «è anch'esso parte del livello di protezione richiesto all'interno dell'Unione e [...] deve essere constatato dalla Commissione prima di adottare una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 1, del [regolamento (UE) 2016/679]» (*Schrems II*, punto 186).

([127]) Sezione 6 della legge del 1998 sui diritti umani.

([128]) Corte europea dei diritti dell'uomo, *Klass e altri c. Germania*, ricorso n. 5029/71, punti da 17 a 51.

(118) Inoltre alle persone fisiche deve essere riconosciuto un ricorso effettivo, e la Corte europea dei diritti dell'uomo ha chiarito che tale ricorso deve essere offerto da un organismo indipendente e imparziale che abbia adottato il proprio regolamento interno e sia costituito da membri che svolgono o abbiano svolto funzioni giurisdizionali di alto livello o siano avvocati esperti, e che non deve sussistere alcun onere probatorio per poter adire tale organismo. Nell'intraprendere l'esame dei reclami presentati da persone fisiche, detto organismo indipendente e imparziale dovrebbe avere accesso a tutte le informazioni pertinenti, comprese quelle riservate. Infine dovrebbe disporre di poteri per porre rimedio ai casi di non conformità ([129]).

(119) Il Regno Unito ha inoltre ratificato la convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (convenzione 108) e, nel 2018, ha firmato il protocollo che modifica tale convenzione (noto come convenzione 108+) ([130]). L'articolo 9 della convenzione 108 prevede che le deroghe ai principi generali in materia di protezione dei dati (articolo 5 Qualità dei dati), alle norme che disciplinano le categorie particolari di dati (articolo 6 Categorie particolari di dati) e ai diritti degli interessati (articolo 8 Garanzie supplementari per l'interessato) siano ammissibili soltanto laddove previste dalla legge della Parte e costituiscano una misura necessaria, in una società democratica, nell'interesse della protezione della sicurezza dello Stato, della sicurezza pubblica, degli interessi monetari dello Stato o della repressione di reati o per proteggere l'interessato o i diritti e le libertà altrui ([131]).

(120) Di conseguenza, attraverso l'adesione al Consiglio d'Europa, l'adesione alla convenzione europea dei diritti dell'uomo e l'assoggettamento alla competenza giurisdizionale della Corte europea dei diritti dell'uomo, il Regno Unito è soggetto a una serie di obblighi, sanciti dal diritto internazionale, che inquadrano il suo sistema di accesso da parte delle pubbliche amministrazioni sulla base di principi, garanzie e diritti individuali simili a quelli garantiti dal diritto dell'Unione e applicabili agli Stati membri. Come sottolineato al considerando 19, la continua adesione a tali strumenti costituisce pertanto un aspetto particolarmente importante della valutazione sulla quale si basa la presente decisione.

(121) Inoltre la legge del 2018 sulla protezione dei dati prevede ulteriori garanzie e diritti specifici in materia di protezione dei dati nell'ambito del trattamento dei dati da parte delle autorità pubbliche, comprese le autorità di contrasto e gli organismi preposti alla sicurezza nazionale.

(122) In particolare il regime per il trattamento dei dati personali nel contesto delle attività di contrasto penale è stabilito nella parte 3 della legge del 2018 sulla protezione dei dati, emanata per recepire la direttiva (UE) 2016/680. La parte 3 della legge del 2018 sulla protezione dei dati si applica al trattamento di 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 contro, e la prevenzione di, minacce alla sicurezza pubblica ([132]).

(123) Ai sensi della sezione 30 della legge sulla protezione dei dati, per «autorità competente» si intende una persona elencata nell'allegato 7 della legge del 2018 sulla protezione dei dati e qualsiasi altra persona nella misura in cui svolga funzioni fissate dalla legge per una delle finalità di contrasto ([133]). Come spiegato di seguito (cfr. considerando 139), alcune autorità competenti (ad esempio la *National Crime Agency*) possono avvalersi, a determinate condizioni, dei poteri conferiti dalla legge del 2016 sui poteri di indagine (*Investigatory Power Act*). In tal caso, le garanzie previste dalla legge del 2016 sui poteri di indagine si applicheranno in aggiunta a quelle previste dalla parte 3 della legge del 2018 sulla protezione dei dati. I servizi di intelligence (*Secret Intelligence Service, Security Service e Government Communications Headquarters*) non sono «autorità competenti» ([134]) ai sensi della parte 3 della legge del 2018 sulla protezione dei dati, pertanto le norme ivi previste non si applicano ad alcuna delle loro attività. Una parte specifica della legge del 2018 sulla protezione dei dati (parte 4) è dedicata al trattamento dei dati personali ad opera dei servizi di intelligence (per maggiori dettagli si veda il considerando 125).

([129]) Corte europea dei diritti dell'uomo, *Kennedy c. Regno Unito*, ricorso n. 26839/05, («*Kennedy*»), punti 167 e 190.

([130]) Per ulteriori informazioni sulla convenzione europea dei diritti dell'uomo e la sua integrazione nel diritto del Regno Unito attraverso la legge del 1998 sui diritti umani, così come sulla convenzione 108, cfr. considerando 9.

([131]) Analogamente, a norma dell'articolo 11 della convenzione 108+, le limitazioni a determinati diritti e obblighi specifici della convenzione per finalità di sicurezza nazionale o di prevenzione, indagine e perseguimento di reati, nonché di esecuzione di sanzioni penali sono ammesse soltanto quando tali limitazioni sono previste dalla legge, rispettano l'essenza dei diritti e delle libertà fondamentali e costituiscono una misura necessaria e proporzionata in una società democratica. Le attività di trattamento per finalità di sicurezza nazionale e difesa devono altresì essere soggette a riesame e supervisione indipendenti ed efficaci ai sensi della legislazione interna della Parte corrispondente della convenzione.

([132]) Sezione 31 della legge del 2018 sulla protezione dei dati.

([133]) Le autorità competenti elencate nell'allegato 7 comprendono non soltanto le forze di polizia, ma anche tutti i dipartimenti governativi ministeriali del Regno Unito nonché altre autorità aventi funzioni investigative (ad esempio *Commissioner for Her Majesty's Revenue and Customs, National Crime Agency, Welsh Revenue Authority, Competition and Markets Authority o Her Majesty's Land Register*), le procure, altri organi di giustizia penale e altri titolari od organizzazioni che svolgono attività di contrasto (tra tali soggetti, l'allegato 7 della legge del 2018 sulla protezione dei dati elenca i direttori degli uffici dei pubblici ministeri, il direttore dei pubblici ministeri per l'Irlanda del Nord o l'*Information Commission*).

([134]) Sezione 30, paragrafo 2, della legge del 2018 sulla protezione dei dati.

(124) Analogamente alla direttiva (UE) 2016/680, la parte 3 della legge del 2018 sulla protezione dei dati stabilisce i principi di liceità e correttezza ([135]), limitazione delle finalità ([136]), minimizzazione dei dati ([137]), esattezza ([138]), limitazione della conservazione ([139]) e sicurezza ([140]). La legislazione impone obblighi specifici di trasparenza ([141]) e riconosce alle persone fisiche il diritto di accesso ([142]), di rettifica e di cancellazione ([143]) così come il diritto di non essere soggette a un processo decisionale automatizzato ([144]). Le autorità competenti sono altresì tenute ad attuare la protezione dei dati fin dalla progettazione e per impostazione predefinita, a tenere registri dei trattamenti e, per determinati trattamenti, a effettuare valutazioni d'impatto sulla protezione dei dati e a consultare preventivamente l'*Information Commissioner* ([145]). Ai sensi della sezione 56 della legge del 2018 sulla protezione dei dati, tali autorità sono tenute a dimostrare la propria conformità. Inoltre sono tenute a mettere in atto misure adeguate per garantire la sicurezza del trattamento ([146]) e sono soggette ad obblighi specifici in caso di violazione dei dati, compresa la notifica di tali violazioni all'*Information Commissioner* e agli interessati ([147]). Come nel caso della direttiva (UE) 2016/680, il titolare del trattamento è soggetto altresì all'obbligo (fatto salvo il caso in cui si tratti di un organo giurisdizionale o di un'altra autorità giudiziaria che agisce nell'esercizio delle proprie funzioni giurisdizionali) di designare un responsabile della protezione dei dati (RPD) ([148]) che gli fornisca assistenza nel rispettare i propri obblighi così come nel monitorare tale rispetto delle norme ([149]). La legislazione impone altresì requisiti specifici per i trasferimenti internazionali di dati personali per finalità di contrasto verso paesi terzi od organizzazioni internazionali al fine di assicurare la continuità della protezione ([150]). Alla stessa data della presente decisione, la Commissione ha adottato una decisione di adeguatezza a norma dell'articolo 36, paragrafo 3, della direttiva (UE) 2016/680, constatando che il regime di protezione dei dati applicabile al trattamento da parte delle autorità di contrasto penale del Regno Unito assicura un livello di protezione sostanzialmente equivalente a quello garantito dalla direttiva (UE) 2016/680.

(125) La parte 4 della legge del 2018 sulla protezione dei dati si applica a tutti i trattamenti effettuati da o per conto dei servizi di intelligence. In particolare stabilisce i principali principi in materia di protezione dei dati (liceità, equità e trasparenza ([151]); limitazione della finalità ([152]); minimizzazione dei dati ([153]); esattezza ([154]); limitazione ([155]) e sicurezza ([156]) della conservazione), impone le condizioni relative al trattamento di categorie particolari di dati ([157]), fissa i diritti degli interessati ([158]), richiede la

([135]) Sezione 35 della legge del 2018 sulla protezione dei dati.
([136]) Sezione 36 della legge del 2018 sulla protezione dei dati.
([137]) Sezione 37 della legge del 2018 sulla protezione dei dati.
([138]) Sezione 38 della legge del 2018 sulla protezione dei dati.
([139]) Sezione 39 della legge del 2018 sulla protezione dei dati.
([140]) Sezione 40 della legge del 2018 sulla protezione dei dati.
([141]) Sezione 44 della legge del 2018 sulla protezione dei dati.
([142]) Sezione 45 della legge del 2018 sulla protezione dei dati.
([143]) Sezioni 46 e 47 della legge del 2018 sulla protezione dei dati.
([144]) Sezioni 49 e 50 della legge del 2018 sulla protezione dei dati.
([145]) Sezioni da 56 a 65 della legge del 2018 sulla protezione dei dati.
([146]) Sezione 66 della legge del 2018 sulla protezione dei dati.
([147]) Sezioni da 67 a 68 della legge del 2018 sulla protezione dei dati.
([148]) Sezioni da 69 a 71 della legge del 2018 sulla protezione dei dati.
([149]) Sezioni da 67 a 68 della legge del 2018 sulla protezione dei dati.
([150]) Parte 3, capo 5, della legge del 2018 sulla protezione dei dati.
([151]) Conformemente alla sezione 86, paragrafo 6, della legge del 2018 sulla protezione dei dati, al fine di stabilire la correttezza e la trasparenza del trattamento, occorre tenere conto del metodo con cui si conseguono tali obiettivi. In tal senso il requisito di correttezza e trasparenza è soddisfatto se i dati vengono ottenuti da una persona legittimamente autorizzata o tenuta a fornirli.
([152]) Conformemente alla sezione 87 della legge del 2018 sulla protezione dei dati, le finalità del trattamento devono essere specificate, esplicite e legittime. I dati non devono essere trattati in maniera incompatibile con le finalità per le quali vengono raccolti. Ai sensi della sezione 87, paragrafo 3, della legge del 2018 sulla protezione dei dati, l'ulteriore trattamento compatibile dei dati personali può essere consentito soltanto se il titolare del trattamento è autorizzato dalla legge a trattare i dati per tale finalità e il trattamento è necessario e proporzionato rispetto a tale finalità. Il trattamento dovrebbe essere considerato compatibile, se consiste in un trattamento per finalità di archiviazione nell'interesse pubblico, per finalità di ricerca scientifica o storica oppure per finalità statistiche, ed è soggetto a garanzie adeguate (sezione 87, paragrafo 4, della legge del 2018 sulla protezione dei dati).
([153]) I dati personali devono essere adeguati, pertinenti e non eccedenti (sezione 88 della legge del 2018 sulla protezione dei dati).
([154]) I dati personali devono essere esatti ed aggiornati (sezione 89 della legge del 2018 sulla protezione dei dati).
([155]) I dati personali devono essere conservati per un arco di tempo non superiore a quanto necessario (sezione 90 della legge del 2018 sulla protezione dei dati).
([156]) Secondo il sesto principio di protezione dei dati, i dati personali devono essere trattati in maniera tale da includere l'adozione di misure di sicurezza adeguate per quanto concerne i rischi che derivano dal trattamento di dati personali. I rischi comprendono (ma non sono limitati a) l'accesso accidentale o non autorizzato oppure la distruzione, la perdita, l'uso, la modifica o la comunicazione di dati personali (sezione 91 della legge del 2018 sulla protezione dei dati). La sezione 107 richiede inoltre che: 1) ciascun titolare del trattamento debba attuare misure di sicurezza adeguate conformi ai rischi derivanti dal trattamento dei dati personali; e 2) nel caso di trattamento automatizzato, ciascun titolare del trattamento e ciascun responsabile del trattamento attui misure preventive o di attenuazione basate su una valutazione del rischio.
([157]) Sezione 86, paragrafo 2, lettera b) e allegato 10 della legge del 2018 sulla protezione dei dati.
([158]) Parte 4, capo 3, della legge del 2018 sulla protezione dei dati, in particolare i diritti: di accesso, di rettifica e di cancellazione, di opposizione al trattamento e di non essere sottoposti a un processo decisionale automatizzato, di intervenire nel processo decisionale automatizzato e di essere informati in merito al processo decisionale. Inoltre il titolare del trattamento deve fornire agli interessati informazioni in merito al trattamento dei loro dati personali. Come spiegato negli orientamenti dell'ICO sul trattamento da parte dei servizi di intelligence, le persone fisiche possono esercitare tutti i loro diritti (compresa una richiesta di rettifica) presentando un reclamo all'ICO o rivolgendosi a un organo giurisdizionale (cfr. gli orientamenti dell'ICO per il trattamento da parte dei servizi di intelligence, disponibili al seguente indirizzo: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

protezione dei dati fin dalla progettazione ([159]) e disciplina i trasferimenti internazionali di dati personali ([160]). L'ICO ha recentemente pubblicato orientamenti dettagliati sul trattamento da parte delle agenzie di intelligence a norma della parte 4 della legge del 2018 sulla protezione dei dati ([161]).

(126) Allo stesso tempo, la sezione 110 della legge del 2018 sulla protezione dei dati prevede un'esenzione da disposizioni specifiche nella parte 4 della legge del 2018 sulla protezione dei dati ([162]) quando tale esenzione è necessaria per salvaguardare la sicurezza nazionale. Tale esenzione può essere invocata sulla base di un'analisi caso per caso ([163]). Come spiegato dalle autorità del Regno Unito e confermato dalla giurisprudenza, «(il) titolare del trattamento deve considerare le conseguenze effettive per la sicurezza nazionale o la difesa qualora fosse tenuto a rispettare la disposizione specifica in materia di protezione dei dati e potesse ragionevolmente rispettare la norma abituale senza ripercussioni per la sicurezza nazionale o la difesa» ([164]). Il ricorso adeguato o meno a tale esenzione è soggetto a vigilanza da parte dell'ICO ([165]).

(127) Inoltre, in relazione alla possibilità di limitare per motivi di protezione della «sicurezza nazionale» l'applicazione delle disposizioni sopra specificate, conformemente alla sezione 111 della legge del 2018 sulla protezione dei dati, il titolare del trattamento può richiedere un certificato firmato da un ministro o dal procuratore o dall'avvocato generale che certifichi che una limitazione di tali diritti è una misura necessaria e proporzionata per la protezione della sicurezza nazionale ([166]).

(128) Il governo del Regno Unito ha pubblicato orientamenti per fornire assistenza ai titolari del trattamento nel momento in cui valutano l'eventualità di presentare domanda per ottenere un certificato di sicurezza nazionale ai sensi della legge del 2018 sulla protezione dei dati, che sottolineano in particolare che qualsiasi limitazione ai diritti degli interessati a favore della protezione della sicurezza nazionale deve essere proporzionata e necessaria ([167]). Tutti i certificati di sicurezza nazionale devono essere pubblicati sul sito web dell'ICO ([168]).

([159]) Sezione 103 della legge del 2018 sulla protezione dei dati.

([160]) Sezione 109 della legge del 2018 sulla protezione dei dati. I trasferimenti dei dati personali ad organizzazioni internazionali o verso paesi al di fuori del Regno Unito sono possibili se il trasferimento costituisce una misura necessaria e proporzionata attuata per l'adempimento delle finalità del titolare del trattamento previste dalla legge o per altre finalità previste negli articoli specifici della legge del 1989 sul servizio di sicurezza e della legge del 1994 sui servizi di intelligence.

([161]) Linee guida dell'ICO, cfr. nota 158.
Sezione 30 della legge del 2018 sulla protezione dei dati e allegato 7 della legge del 2018 sulla protezione dei dati.

([162]) La sezione 110, paragrafo 2, della legge del 2018 sulla protezione dei dati elenca le disposizioni rispetto alle quali è consentita un'esenzione. Comprende i principi di protezione dei dati (fatta eccezione per il principio di liceità), i diritti degli interessati, l'obbligo di informare l'*Information Commissioner* in merito a una violazione dei dati, i poteri di ispezione dell'*Information Commissioner* in conformità con gli obblighi internazionali, alcuni dei poteri di esecuzione dell'*Information Commissioner,* le disposizioni che qualificano come reato determinate violazioni in materia di protezione dei dati nonché le disposizioni relative a finalità speciali di trattamento, quali le finalità giornalistiche, accademiche o artistiche.

([163]) Cfr. *Baker v Secretary of State*, cfr. nota 61.

([164]) Regno Unito, *Explanatory Framework for Adequacy Discussions, section H: National Security Data Protection and Investigatory Powers Framework*, pag. 15 e 16 (cfr. nota 31). Cfr. anche *Baker v Secretary of State* (cfr. nota 61), causa nella quale l'organo giurisdizionale ha annullato un certificato di sicurezza nazionale rilasciato dall'*Home Secretary* (segretario di Stato per gli Affari interni) che confermava l'applicazione dell'eccezione di sicurezza nazionale, considerando che non vi era motivo per concedere un'eccezione globale in merito all'obbligo di rispondere a richieste di accesso e che consentire tale eccezione in tutte le circostanze senza un'analisi caso per caso andava oltre quanto necessario e proporzionato ai fini della protezione della sicurezza nazionale.

([165]) Cfr. protocollo d'intesa tra l'ICO e la *UK Intelligence Community* (comunità di intelligence del Regno Unito) secondo il quale «quando riceve un reclamo da un interessato, l'ICO vorrà accertarsi che la questione sia stata gestita correttamente e, se del caso, che l'applicazione di un'eventuale esenzione sia stata utilizzata in maniera adeguata». Protocollo d'intesa tra l'ICO e la *UK Intelligence Community* (comunità di intelligence del Regno Unito), punto 16, disponibile al seguente indirizzo: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf.

([166]) La legge del 2018 sulla protezione dei dati ha abrogato la possibilità di rilasciare certificati a norma della sezione 28, paragrafo 2, della legge del 1998 sulla protezione dei dati. Tuttavia, la possibilità di rilasciare «vecchi certificati» esiste ancora nella misura in cui vi è una contestazione storica della legge del 1998 (cfr. allegato 20, parte 5, paragrafo 17 della legge del 2018 sulla protezione dei dati). Tuttavia, tale possibilità sembra molto rara e si applicherà solo in casi limitati, ad esempio qualora l'interessato contesti il ricorso all'esenzione per motivi di sicurezza nazionale in relazione a un trattamento effettuato da un'autorità pubblica ai sensi della legge del 1998. Va osservato che in questi casi la sezione 28 della legge del 1998 sulla protezione dei dati si applicherà nella sua interezza, compresa pertanto la possibilità per l'interessato di contestare il certificato dinanzi all'organo giurisdizionale.

([167]) Orientamenti governativi del Regno Unito sui certificati di sicurezza nazionale ai sensi della legge del 2018 sulla protezione dei dati, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf Secondo la spiegazione fornita dalle autorità britanniche, sebbene costituisca una prova definitiva del fatto che, per quanto concerne i dati o il trattamento descritti nel certificato, l'esenzione è applicabile, un certificato non elimina l'obbligo per il titolare del trattamento di considerare se sia necessario invocare l'esenzione caso per caso.

([168]) Ai sensi della sezione 130 della legge del 2018 sulla protezione dei dati, l'ICO può decidere di non pubblicare il testo o parte del testo del certificato qualora ciò sia contrario all'interesse della sicurezza nazionale o all'interesse pubblico o rischi di compromettere la sicurezza di una persona. In questi casi l'ICO pubblicherà tuttavia l'informazione secondo cui il certificato è stato emesso.

(129) Il certificato dovrebbe avere una durata fissa non superiore a cinque anni, in maniera da essere riesaminato regolarmente dal potere esecutivo ([169]). Il certificato deve individuare i dati personali o le categorie di dati personali soggetti ad esenzione nonché le disposizioni della legge del 2018 sulla protezione dei dati a cui si applica l'esenzione ([170]).

(130) È importante notare che i certificati di sicurezza nazionale non prevedono un ulteriore motivo per limitare i diritti alla protezione dei dati per motivi di sicurezza nazionale. In altre parole, il titolare del trattamento o il responsabile del trattamento può basarsi su un certificato soltanto quando ha concluso che è necessario basarsi sull'esenzione per motivi di sicurezza nazionale, che, come spiegato in precedenza, deve essere applicata caso per caso ([171]). Anche se un certificato di sicurezza nazionale si applica alla questione in esame, l'ICO può indagare per stabilire se l'affidamento sull'esenzione prevista per motivi di sicurezza nazionale fosse giustificato in un caso specifico ([172]).

(131) Qualsiasi persona direttamente interessata dal rilascio del certificato può presentare ricorso all'*Upper Tribunal* ([173]) (tribunale superiore) contro il certificato ([174]) oppure, laddove il certificato individui i dati mediante una descrizione generale, impugnare l'applicazione del certificato a dati specifici ([175]). Detto organo giurisdizionale riesamina la decisione di emettere un certificato e decide se vi erano motivi ragionevoli per il suo rilascio ([176]). Può prendere in considerazione una vasta gamma di questioni, tra le quali la necessità, la proporzionalità e la liceità, tenendo conto dell'impatto sui diritti degli interessati e dell'equilibrio rispetto alla necessità di salvaguardare la sicurezza nazionale. Di conseguenza tale organo giurisdizionale può stabilire che il certificato non si applica a dati personali specifici oggetto del ricorso ([177]).

(132) Un insieme diverso di possibili limitazioni riguarda quelle applicabili, ai sensi dell'articolo 11 della legge del 2018 sulla protezione dei dati, a talune disposizioni della parte 4 della legge del 2018 sulla protezione dei dati ([178]) per salvaguardare altri importanti obiettivi di interesse pubblico generale o interessi tutelati quali ad esempio l'immunità parlamentare, il segreto professionale, lo svolgimento di procedimenti giudiziari o l'efficacia di combattimento delle forze armate ([179]). L'applicazione di tali disposizioni è esentata per determinate categorie di informazioni (esenzione «basata sulla classificazione») oppure esentata nella misura in cui l'applicazione di tali disposizioni potrebbe compromettere l'interesse tutelato (esenzione «basata sul pregiudizio») ([180]). Le esenzioni basate sul pregiudizio possono essere invocate soltanto nella misura in cui l'applicazione della disposizione di protezione dei

([169]) Orientamenti governativi del Regno Unito sui certificati di sicurezza nazionale, punto 15, cfr. nota 167.

([170]) Orientamenti governativi del Regno Unito sui certificati di sicurezza nazionale, punto 5, cfr. nota 167.

([171]) Cfr. nota 164.

([172]) La sezione 102 della legge del 2018 sulla protezione dei dati impone al titolare del trattamento di essere in grado di dimostrare di aver rispettato detta legge. Ciò implica che un servizio di intelligence dovrebbe dimostrare all'ICO che quando fa affidamento sull'esenzione, ha considerato le circostanze specifiche del caso. L'ICO pubblica altresì un registro dei certificati di sicurezza nazionale, disponibile al seguente indirizzo: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([173]) L'*Upper Tribunal* è l'organo giurisdizionale competente a pronunciarsi in merito a ricorsi contro le decisioni prese da organi giurisdizionali di grado inferiore e ha competenze specifiche per impugnazioni dirette di decisioni di determinati organismi governativi.

([174]) Sezione 111, paragrafo 3, della legge del 2018 sulla protezione dei dati.

([175]) Sezione 111, paragrafo 5, della legge del 2018 sulla protezione dei dati.

([176]) Nella causa *Baker v Secretary of State* (cfr. nota 61), l'*Information Tribunal* (tribunale competente in materia di informazione) ha annullato un certificato di sicurezza nazionale rilasciato dal segretario di Stato per gli Affari interni, considerando che non vi era motivo per concedere un'eccezione globale in merito all'obbligo di rispondere a richieste di accesso e che consentire tale eccezione in ogni circostanza senza un'analisi caso per caso andava oltre quanto necessario e proporzionato ai fini della protezione della sicurezza nazionale.

([177]) Orientamenti governativi del Regno Unito sui certificati di sicurezza nazionale, punto 25, cfr. nota 167.

([178]) Rientrano in tale contesto: i) i principi di protezione dei dati di cui alla parte 4, fatta eccezione per il requisito di liceità del trattamento nel contesto del primo principio e per il fatto che il trattamento deve soddisfare una delle condizioni pertinenti stabilite negli allegati 9 e 10; ii) i diritti degli interessati; e iii) i doveri relativi alla segnalazione di violazioni all'ICO.

([179]) La parte 4 della legge del 2018 sulla protezione dei dati stabilisce il quadro giuridico applicabile a tutti i tipi di trattamento di dati personali effettuati dalle agenzie di intelligence (e non solo all'esercizio dei loro compiti di sicurezza nazionale). Pertanto, la parte 4 si applica anche quando le agenzie di intelligence trattano dati, ad esempio, a fini di gestione delle risorse umane o nell'ambito di controversie o di appalti pubblici. Le limitazioni elencate nell'allegato 11 sono destinate principalmente ad applicarsi in questi altri ambiti. Ad esempio, nell'ambito di una controversia con un dipendente può essere invocata la limitazione a fini di un «procedimento giudiziario», oppure nell'ambito di un appalto pubblico può essere invocata la limitazione a fini di «negoziazione», ecc. Ciò si riflette negli orientamenti dell'ICO sul trattamento da parte dei servizi di intelligence, che menzionano la negoziazione di una transazione tra un'agenzia di intelligence e un ex dipendente che esercita una pretesa lavorativa come esempio per l'applicazione delle limitazioni di cui all'allegato 11 (cfr. nota 161). Va inoltre osservato che le stesse limitazioni sono a disposizione di altre autorità pubbliche ai sensi dell'allegato 2, parte 2, della legge del 2018 sulla protezione dei dati.

([180]) Secondo il quadro esplicativo (*Explanatory Framework*) del Regno Unito le eccezioni «basate sulla classificazione» sono: i) informazioni sul conferimento di onorificenze e dignità della Corona; ii) il segreto professionale; iii) referenze riservate in relazione a occupazione, formazione o istruzione; e iv) tracce e voti di esame. Le eccezioni «basate sul pregiudizio» riguardano le seguenti questioni: i) la prevenzione o l'accertamento di reati; l'arresto e il perseguimento di autori di reati; ii) l'immunità parlamentare; iii) procedimenti giudiziari; iv) l'efficacia di combattimento delle forze armate della Corona; v) il benessere economico del Regno Unito; vi) negoziati con l'interessato; vii) finalità di ricerca scientifica o storica o finalità statistiche; viii) l'archiviazione nell'interesse pubblico. Regno Unito, *Explanatory Framework for Adequacy Discussions, section H: National Security*, pag. 13, cfr. nota 31.

dati elencati possa pregiudicare lo specifico interesse in questione. L'uso di un'esenzione deve quindi essere sempre giustificato facendo riferimento al pregiudizio pertinente che potrebbe verificarsi nel singolo caso. L'esenzione basata sulla classificazione può essere invocata soltanto rispetto alla categoria di informazioni specifiche, strettamente definita, per la quale è concessa. Si tratta di esenzioni analoghe, in termini di finalità ed effetto, a numerose delle eccezioni di cui al GDPR del Regno Unito (conformemente all'allegato 2 della legge del 2018 sulla protezione dei dati) che, a loro volta, riflettono quelle previste dall'articolo 23 del regolamento generale sulla protezione dei dati dell'Unione europea.

(133) Da quanto precede consegue che tali limitazioni e tali condizioni si attuano nel quadro di disposizioni giuridiche del Regno Unito applicabili, come interpretato anche dagli organi giurisdizionali e dall'ICO, al fine di assicurare che tali esenzioni e limitazioni rimangano all'interno dei limiti di ciò che è necessario e proporzionato per proteggere la sicurezza nazionale.

3.2 **Accesso e uso da parte delle autorità pubbliche del Regno Unito per motivi di contrasto penale**

(134) Il diritto del Regno Unito impone una serie di limitazioni in materia di accesso e uso di dati personali per finalità di contrasto penale e prevede meccanismi di vigilanza e ricorso in questo settore che sono in linea con i requisiti di cui ai considerando da 113 a 115 della presente decisione. Le condizioni in cui tale accesso può avvenire e le garanzie applicabili all'uso di tali poteri sono valutate in dettaglio nelle sezioni che seguono.

3.2.1 *Basi giuridiche e limitazioni/garanzie applicabili*

(135) Conformemente al principio di liceità, garantito dalla sezione 35, della legge del 2018 sulla protezione dei dati, il trattamento di dati personali per una delle finalità di contrasto è lecito soltanto se si basa sulla legge e l'interessato ha prestato il proprio consenso al trattamento per tale finalità ([181]) oppure se il trattamento è necessario per lo svolgimento di uno dei compiti effettuati per tale finalità da un'autorità competente.

3.2.1.1 Mandati di perquisizione e ordini di produzione

(136) Nel quadro giuridico del Regno Unito, la raccolta di dati personali da operatori economici, compresi quelli che tratterebbero dati trasferiti dall'UE ai sensi della presente decisione di adeguatezza, per finalità di contrasto penale è consentita sulla base di mandati di perquisizione ([182]) e ordinanze per la consegna di prove ([183]).

(137) I mandati di perquisizione sono emessi da un organo giurisdizionale, di norma su domanda presentata dal funzionario incaricato dell'indagine. Tali mandati consentono a un operatore di polizia di accedere a locali per cercare materiale o persone fisiche pertinenti per la sua indagine e di trattenere qualsiasi cosa per la quale sia stato autorizzato un mandato, compresi documenti o materiali pertinenti contenenti dati personali ([184]). Un'ordinanza per la consegna di prove, che deve anch'essa essere emessa da un organo giurisdizionale, impone alla persona in essa specificata di presentare o di fornire accesso a materiale in suo possesso o soggetto al suo controllo. Il richiedente deve specificare all'organo giurisdizionale il motivo della necessità di tale mandato od ordinanza, oltre a indicare il motivo per cui ciò è nell'interesse pubblico. Vi sono diversi poteri statutari che consentono l'emissione di

([181]) Il ricorso al consenso non sembra pertinente in uno scenario di adeguatezza dato che in una situazione di trasferimento, i dati non saranno stati raccolti direttamente da un interessato dell'UE da un'autorità di contrasto del Regno Unito sulla base di un consenso.

([182]) Per la base giuridica pertinente, cfr. gli articoli 8 e seguenti della PACE 1984 (legge del 1984 sulle prove) (per Inghilterra e Galles), gli articoli 10 e seguenti della *Police and Criminal Evidence Order (Northern Ireland) 1989* (ordinanza del 1989 sulle prove nelle attività di polizia e di azione penale — Irlanda del Nord), mentre per la Scozia si ottiene ai sensi del *common law* (cfr. sezione 46 della *Criminal Justice (Scotland) Act 2016)* (legge del 2016 sulla giustizia penale — Scozia) e della sezione 23B del *Criminal Law (Consolidation) (Scotland)* [diritto penale (consolidamento) — Scozia]. Per il mandato di perquisizione emesso dopo l'arresto la base giuridica è la sezione 18 della legge del 1984 sulle prove (per Inghilterra e Galles), gli articoli 20 e seguenti dell'ordinanza del 1989 sulle prove nelle attività di polizia e di azione penale — Irlanda del Nord, mentre per la Scozia è ottenuto ai sensi della «common law» (cfr. sezione 46 della legge del 2016 sulla giustizia penale — Scozia). Le autorità del Regno Unito hanno chiarito che i mandati di perquisizione sono emessi da un organo giurisdizionale su domanda presentata dal funzionario incaricato dell'indagine. Tali mandati consentono a un funzionario di accedere a locali per cercare materiale o persone fisiche pertinenti per la sua indagine; l'esecuzione del mandato richiederà spesso l'assistenza di un agente di polizia.

([183]) Quando l'indagine riguarda il riciclaggio di denaro (compresa la confisca e il procedimento civile di recupero), la base giuridica corrispondente per l'applicazione di un'ordinanza per la consegna di prove è data dagli articoli 345 e seguenti per Inghilterra, Galles e Irlanda del Nord oppure dalle sezioni 380 e seguenti della *Proceeds of Crime Act 2002* (legge del 2002 sui proventi da reato) per la Scozia. Quando l'indagine riguarda altre questioni rispetto al riciclaggio di denaro, è possibile presentare una domanda per l'ottenimento di un'ordinanza per la consegna di prove ai sensi della sezione 9 e dell'allegato 1 della legge del 1984 sulle prove per Inghilterra e Galles, mentre per l'Irlanda del Nord la base giuridica è data dagli articoli 10 e seguenti dell'ordinanza del 1989 sulle prove nelle attività di polizia e di azione penale — Irlanda del Nord. Per la Scozia tale ordinanza si ottiene di norma in virtù della «common law» (cfr. sezione 46 della legge del 2016 sulla giustizia penale — Scozia) e della sezione 23B del diritto penale (consolidamento) — Scozia. Le autorità del Regno Unito hanno chiarito che un'ordinanza per la consegna di prove richiede che la persona specificata in detto documento presenti o dia accesso al materiale in suo possesso o soggetto al suo controllo (cfr. paragrafo 4 dell'allegato 1 della legge del 1984 sulle prove).

([184]) Ad esempio la legge del 1984 sulle prove, agli articoli 8 e 18, contiene poteri per sequestrare e trattenere qualsiasi cosa per la quale è stato autorizzato un mandato.

mandati di perquisizione e di ordinanze per la consegna di prove. Ciascuna disposizione è accompagnata da una serie di condizioni statutarie che devono essere soddisfatte affinché sia possibile emettere un mandato ([185]) o un'ordinanza per la consegna di prove ([186]).

(138) Le ordinanze per la consegna di prove e i mandati di perquisizione possono essere contestati mediante controllo giurisdizionale ([187]). In termini di garanzie, tutte le autorità di contrasto penale rientranti nell'ambito di applicazione della parte 3 della legge del 2018 sulla protezione dei dati possono accedere ai dati personali (accesso che costituisce una forma di trattamento) soltanto in linea con i principi e i requisiti di cui alla legge del 2018 sulla protezione dei dati (cfr. considerando 122 e 124). Di conseguenza una richiesta formulata da una qualsiasi autorità di contrasto

([185]) Ad esempio la sezione 8 e la sezione 18 della legge sulle prove disciplinano rispettivamente il potere di un giudice di pace di autorizzare un mandato e di un operatore di polizia di perquisire una proprietà. Nel primo caso (sezione 8), prima di emettere un mandato, un giudice di pace deve innanzitutto assicurarsi che vi siano motivi ragionevoli per ritenere che: i) sia stato commesso un reato perseguibile; ii) presso i locali vi siano materiali che è probabile siano di valore sostanziale (di per sé o in associazione ad altri materiali) per l'indagine in merito al reato; iii) è probabile che tali materiali costituiscano prove pertinenti; iv) il materiale non consti di o comprenda oggetti coperti da segreto professionale, materiale escluso o materiale soggetto a procedura speciale; e v) non sarebbe possibile ottenere l'accesso ai locali senza ricorrere a un mandato. Nel secondo caso, la sezione 18 consente a un operatore di polizia di perquisire i locali di una persona arrestata per un reato perseguibile alla ricerca di materiale diverso da quello coperto da segreto professionale, qualora abbia motivi ragionevoli per sospettare che vi siano prove presso tali locali che si riferiscono al reato in questione o a un reato perseguibile analogo o collegato. Tale perquisizione deve limitarsi a rinvenire detto materiale e deve essere autorizzato, per iscritto, da un operatore di polizia avente quanto meno il grado di ispettore fatto salvo il caso in cui sia necessario per l'indagine del reato. In quest'ultimo caso occorre informare, non appena possibile dopo lo svolgimento della perquisizione, un operatore di polizia avente quanto meno il grado di ispettore. Occorre registrare i motivi alla base della perquisizione e la natura delle prove. Inoltre gli articoli 15 e 16 della legge del 1984 sulle prove prevedono garanzie di legge che devono essere rispettate quando si richiede un mandato di perquisizione. La sezione 15 specifica i requisiti applicabili per l'ottenimento di un mandato di perquisizione (compreso il contenuto della domanda effettuata dall'agente di polizia e il fatto che il mandato deve specificare, tra le altre cose, l'atto legislativo sulla base del quale viene emesso, nonché individuare, per quanto possibile, gli oggetti e le persone da cercare e i locali da sottoporre a perquisizione). La sezione 16 disciplina il modo in cui deve essere effettuata una perquisizione ai sensi di un mandato (ad esempio: la sezione 16, paragrafo 5, prevede che l'agente di polizia che esegue il mandato fornisca all'occupante dei locali una copia del mandato; la sezione 16, paragrafo 11, richiede che il mandato, una volta eseguito, sia conservato per un periodo di 12 mesi; la sezione 16, paragrafo 12, riconosce all'occupante dei locali il diritto di ispezionare il mandato durante tale periodo qualora lo desideri). Tali articoli contribuiscono a garantire il rispetto della sezione 8 CEDU (cfr. ad esempio *Kent Pharmaceuticals v Director of the Serious Fraud Office* [2002] EWHC 3023 (QB) punto [30] pronunciata dal giudice Woolf CJ). In caso di mancato rispetto di tali garanzie la perquisizione può essere dichiarata illecita (tra gli esempi figurano *R (Brook) v Preston Crown Court* [2018] EWHC 2024 (admin), [2018] ACD 95; *R (Superior Import / Export Ltd) v Revenue and Customs Commissioners* [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115; e *R (F) v Blackfriars Crown Court* [2014] EWHC 1541 (Admin)). Gli articoli 15 e 16 della legge del 1984 sulle prove sono integrati dal Codice B della legge sulle prove, un codice di pratica che disciplina l'esercizio dei poteri di polizia in relazione alla perquisizione di locali.

([186]) Ad esempio quando viene emessa un'ordinanza per la consegna di prove nel contesto della legge del 2002 sui proventi da reato, oltre alla necessità di disporre di ragionevoli motivi per soddisfare le condizioni di cui all'articolo 346, paragrafo 2, della legge sui proventi da reato, vi dovrebbero essere ragionevoli motivi per ritenere che la persona in questione sia in possesso del materiale così specificato o abbia il controllo sullo stesso e dovrebbe essere probabile che il materiale presenti un valore sostanziale. Inoltre un ulteriore requisito per l'emissione di un'ordinanza per la consegna di prove consiste nel fatto che devono esservi ragionevoli motivi per ritenere che la presentazione di tale materiale o la concessione dell'accesso allo stesso sia nell'interesse pubblico, tenendo conto: a) del beneficio che potrebbe derivare per l'indagine, qualora si ottenesse detto materiale; e b) le circostanze ai sensi delle quali la persona, che la domanda indica sembrare essere in possesso o avere controllo del materiale, detiene le informazioni in questione. Analogamente un organo giurisdizionale che esamina una domanda per un'ordinanza per la consegna di prove ai sensi dell'allegato 1 della legge del 1984 sulle prove deve accertarsi che siano soddisfatte condizioni specifiche. In particolare l'allegato 1 della legge sulle prove stabilisce due distinte serie alternative di condizioni, una delle quali deve essere soddisfatta prima che un giudice possa emettere un'ordinanza per la consegna di prove. La prima serie di condizioni richiede che il giudice disponga di ragionevoli motivi per ritenere che: i) sia stato commesso un reato perseguibile; ii) il materiale che si cerca presso i locali sia costituito da o includa materiale soggetto a procedura speciale ma non materiale escluso; iii) sia probabile che tale materiale presenti un valore sostanziale per l'indagine, di per sé o in associazione ad altro materiale; iv) sia inoltre probabile che si tratti di prove pertinenti; v) altri metodi per ottenere detto materiale sono stati tentati o non sono stati tentati perché sarebbero stati destinati a fallire; e vi) che, avendo considerato il beneficio per l'indagine e le circostanze secondo le quali la persona fisica possiede tale materiale, sia nell'interesse pubblico che il materiale venga presentato o che venga concesso accesso allo stesso. La seconda serie di condizioni richiede: i) che presso i locali vi sia materiale costituito da materiale soggetto a procedura speciale o materiale escluso; ii) se non fosse per il divieto di effettuate perquisizioni sulla base della legislazione emanata prima della legge sulle prove in materia di procedura speciale, materiale escluso o coperto da segreto professionale, sarebbe stato possibile emettere un mandato di perquisizione per il materiale; e iii) sarebbe stato opportuno procedere in tal senso.

([187]) Il controllo giurisdizionale è una procedura legale attraverso la quale le decisioni di un ente pubblico possono essere impugnate dinanzi l'Alta Corte. Gli organi giurisdizionali «controllano», riesaminano, la decisione impugnata e decidono se si possa sostenere che tale decisione sia giuridicamente viziata, considerando i concetti/principi di diritto pubblico. Le basi principali sulle quali si basa il controllo giurisdizionale sono in particolare l'illegittimità, l'irrazionalità, i vizi procedurali, il legittimo affidamento e i diritti umani. A seguito di un controllo giurisdizionale riuscito, un organo giurisdizionale è in grado di ordinare una serie di rimedi differenti; il più comune di tali rimedi è un'ordinanza di annullamento (che annullerebbe o cancellerebbe la decisione originale, ossia la decisione di emettere un mandato di perquisizione), la quale in alcune circostanze può persino comprendere il riconoscimento di un risarcimento pecuniario. Ulteriori dettagli in materia di controllo giurisdizionale nel Regno Unito sono riportati nella pubblicazione del *Government Legal Department «Judge Over Your Shoulder — a guide to good decision-making»*, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf.

dovrebbe essere conforme al principio secondo cui le finalità del trattamento devono essere specificate, esplicite e legittime ([188]) e i dati personali trattati da un'autorità competente devono essere pertinenti per tale finalità e non eccessivi ([189]).

3.2.1.2 Poteri di indagine per finalità di contrasto

(139) Al fine di prevenire o accertare solo reati gravi ([190]), alcune autorità di contrasto, ad esempio la *National Crime Agency* o il capo della polizia ([191]), possono avvalersi di poteri di indagine mirati ai sensi della legge del 2016 sui poteri di indagine. In tal caso, le garanzie previste dalla legge del 2016 sui poteri di indagine si applicheranno in aggiunta a quelle previste dalla parte 3 della legge del 2018 sulla protezione dei dati. 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), la conservazione di dati relativi alle comunicazioni (parte 4 della medesima legge) e l'ingerenza mirata in apparecchiature (parte 5 della medesima legge). L'intercettazione si riferisce all'acquisizione del contenuto di una comunicazione ([192]), mentre l'acquisizione e la conservazione di dati relativi alle comunicazioni non mirano al contenuto delle comunicazioni ma a informazioni sulla comunicazione, quali «chi», «quando», «dove» e «come». Rientra in tale contesto ad esempio l'ora e la durata di una comunicazione, il numero di telefono o l'indirizzo di posta elettronica del mittente e del destinatario della comunicazione, e talvolta l'ubicazione dei dispositivi dai quali viene effettuata la comunicazione, l'abbonato a un servizio telefonico oppure una fattura dettagliata ([193]). Con ingerenza in apparecchiature si intende un insieme di tecniche utilizzate per ottenere una varietà di dati dalle apparecchiature, tra le quali figurano computer, tablet e smartphone, nonché cavi, fili e dispositivi di conservazione ([194]).

(140) Si possono esercitare i poteri di intercettazione mirata anche laddove ciò sia «necessario al fine di dare effetto alle disposizioni di uno strumento di assistenza reciproca dell'UE o un accordo internazionale di assistenza reciproca» (il cosiddetto «*mutual assistance warrant*» ([195]), mandato di assistenza reciproca). I mandati di assistenza reciproca vengono emessi soltanto in relazione all'intercettazione, non per l'acquisizione di dati relativi alle comunicazioni o l'ingerenza in apparecchiature. Tali poteri mirati sono disciplinati dalla *Investigatory Powers Act 2016* ([196]) (legge del 2016 sui poteri di indagine), che, unitamente al *Regulation of Investigatory Powers Act 2000* (RIPA) (legge del 2000 sul regolamento sui poteri di indagine) per Inghilterra, Galles e Irlanda del Nord e al *Regulation of Investigatory Powers (Scotland) Act 2000* (RIPSA) (legge del 2000 sul regolamento sui poteri di indagine — Scozia) per la Scozia, prevede la base giuridica e definisce le limitazioni e le garanzie applicabili all'esercizio di tali poteri. La legge del 2016 sui poteri di indagine stabilisce altresì un regime per l'uso di poteri di indagine massivi, sebbene questi non siano disponibili per le autorità di contrasto (soltanto le agenzie di intelligence possono utilizzarli) ([197]).

([188]) Sezione 36, paragrafo 1, della legge del 2018 sulla protezione dei dati del Regno Unito.

([189]) Sezione 37 della legge del 2018 sulla protezione dei dati del Regno Unito.

([190]) La sezione 263, paragrafo 1, della legge del 2016 sulla protezione dei dati prevede che per «reato grave» si intende un reato per il quale si possa prevedere che un adulto, incensurato, possa ragionevolmente essere condannato a una pena detentiva di 3 anni o superiore oppure se la condotta in questione comporta l'uso della violenza, si traduce in un notevole guadagno finanziario o è adottata da un ampio numero di persone. Inoltre, ai fini dell'acquisizione di dati relativi alle comunicazioni ai sensi della parte 4 della legge del 2016 sui poteri di indagine, la sezione 87, paragrafo 10B, prevede che per «reato grave» si intende un reato per il quale può essere irrogata una pena detentiva di 12 mesi o più oppure un reato commesso da una persona che non è una persona fisica o che comporta, come parte integrante, l'invio di una comunicazione o una violazione della vita privata di una persona.

([191]) In particolare, le seguenti autorità di contrasto possono richiedere un mandato di intercettazione mirata: il direttore generale della *National Crime Agency*, il *Commissioner of Police of the Metropolis*, il *Chief Constable of the Police Service of Northern Ireland*, il *Chief Constable of the Police Service of Scotland*, il *Commissioner for Her Majesty's Revenue and Customs*, il *Chief of Defence Intelligence* così come una persona che sia un'autorità competente di un paese o territorio al di fuori del Regno Unito ai fini di uno strumento di assistenza reciproca dell'UE o di un accordo internazionale di assistenza reciproca (sezione 18, paragrafo 1, della legge del 2016 sulla protezione dei dati).

([192]) Cfr. sezione 4 della legge del 2016 sui poteri di indagine.

([193]) Cfr. sezione 261, paragrafo 5, della legge del 2016 sulla protezione dei dati e il codice di condotta sull'acquisizione in massa di dati relativi alle comunicazioni, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, punto 2.9.

([194]) Codice di pratica sull'ingerenza in apparecchiature, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, punto 2.2.

([195]) Un mandato di assistenza reciproca autorizza un'autorità del Regno Unito a fornire assistenza a un'autorità al di fuori del territorio del Regno Unito per l'intercettazione e la comunicazione del materiale intercettato a tale autorità, in conformità con uno strumento internazionale di assistenza reciproca (sezione 15, paragrafo 4, della legge del 2016 sui poteri di indagine).

([196]) 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.

([197]) Sezione 138, paragrafo 1, sezione 158, paragrafo 1, sezione 178, paragrafo 1, sezione 199 paragrafo 1, della legge del 2016 sui poteri di indagine.

(141) Al fine di esercitare tali poteri, le autorità devono ottenere un mandato ([198]) rilasciato da un'autorità competente ([199]) e approvato da un commissario giudiziario indipendente ([200]) (cosiddetta procedura «a doppia verifica»). L'ottenimento di tale mandato è soggetto a una verifica della necessità e della proporzionalità ([201]). Dato che tali poteri di indagine mirati previsti dalla legge del 2016 sui poteri di indagine sono gli stessi di quelli disponibili per le agenzie di sicurezza nazionale, le condizioni, le limitazioni e le garanzie applicabili a tali poteri sono affrontati in dettaglio nella sezione sull'accesso e sull'uso di dati personali da parte delle autorità pubbliche del Regno Unito per finalità di sicurezza nazionale (cfr. considerando 177 e seguenti).

3.2.2 *Ulteriore utilizzo delle informazioni raccolte*

(142) 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 di determinate condizioni.

(143) Analogamente a quanto previsto dalla sezione 4, paragrafo 2, della direttiva (UE) 2016/680, la sezione 36, paragrafo 3, della legge del 2018 sulla protezione dei dati consente ai dati personali raccolti da un'autorità competente per una finalità di contrasto di poter essere ulteriormente trattati (dal titolare del trattamento originale o da un altro titolare del trattamento) per qualsiasi altra finalità di contrasto, a condizione che il titolare del trattamento sia autorizzato dalla legge a trattare i dati per un'altra finalità e il trattamento sia necessario e proporzionato a tale fine ([202]). In tal caso tutte le garanzie fornite dalla parte 3 della legge del 2018 sulla protezione dei dati, di cui ai considerando 122 e 124 si applicano al trattamento effettuato all'autorità ricevente.

(144) Nell'ordinamento giuridico del Regno Unito, leggi diverse consentono esplicitamente la condivisione successiva. In particolare i) la *Digital Economy Act 2017* (legge del 2017 sull'economia digitale) consente la condivisione tra autorità pubbliche per finalità diverse, ad esempio in caso di frode contro il settore pubblico che comporterebbe una perdita o un rischio di perdita per autorità pubbliche ([203]) o in caso di un debito nei confronti di un'autorità pubblica o della Corona ([204]); ii) la *Crime and Courts Act 2013* (legge del 2013 sui reati e sugli organi giurisdizionali) consente la condivisione di informazioni con la *National Crime Agency* ([205]) (NCA) per contrastare, indagare e perseguire la criminalità organizzata e forme gravi di criminalità; iii) la *Serious Crime Act 2007* (legge del 2007 sui reati gravi) che consente alle autorità pubbliche di divulgare informazioni alle organizzazioni antifrode ai fini della prevenzione delle frodi ([206]).

(145) Tali leggi prevedono esplicitamente che la condivisione di informazioni debba essere conforme ai principi stabiliti nella legge del 2018 sulla protezione dei dati. Inoltre il *College of Policing* ha emesso una pratica professionale autorizzata sulla condivisione di informazioni ([207]) per fornire assistenza alle forze di polizia nel rispettare i loro

([198]) 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.

([199]) 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.

([200]) 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 (per maggiori dettagli cfr. considerando 162 e seguenti).

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

([202]) Sezione 36, paragrafo 3, della legge del 2018 sulla protezione dei dati.

([203]) Sezione 56 della legge del 2017 sull'economia digitale, disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2017/30/section/56.

([204]) Sezione 48 della legge del 2017 sull'economia digitale.

([205]) Sezione 7 della legge del 2013 sui reati e sugli organi giurisdizionali, disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2013/22/section/7.

([206]) Sezione 68 della legge del 2007 sui reati gravi, disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2007/27/contents.

([207]) Pratica professionale autorizzata sulla condivisione delle informazioni, disponibile al seguente indirizzo: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

obblighi di protezione dei dati nel quadro del GDPR del Regno Unito, della legge sulla protezione dei dati e della legge del 1998 sui diritti umani. La conformità della condivisione con il quadro giuridico della protezione dei dati applicabile è, naturalmente, soggetta a controllo giurisdizionale ([208]).

(146) Inoltre, analogamente a quanto previsto all'articolo 9 della direttiva (UE) 2016/680, la legge del 2018 sulla protezione dei dati prevede che i dati personali raccolti per qualsiasi finalità di contrasto possano essere trattati per una finalità diversa da quelle di contrasto quando tale trattamento è autorizzato dalla legge ([209]).

(147) Questo tipo di condivisione riguarda due scenari: 1) quello in cui un'autorità di contrasto penale condivide dati con un'autorità di contrasto che non si occupa di materia penale diversa da un'agenzia di intelligence (come ad esempio un'autorità finanziaria o fiscale, un'autorità per la concorrenza, un ufficio per l'assistenza ai giovani, ecc.); e 2) quello in cui un'autorità di contrasto penale condivide dati con un'agenzia di intelligence. Nel primo scenario, il trattamento dei dati personali rientrerà nell'ambito di applicazione del GDPR del Regno Unito nonché in quello della parte 2 della legge del 2018 sulla protezione dei dati. La Commissione ha valutato le garanzie fornite dal GDPR del Regno Unito e dalla parte 2 della legge del 2018 sulla protezione dei dati nei considerando da 12 a 111 ed è giunta alla conclusione che il Regno Unito assicura un livello di protezione adeguato dei dati personali trasferiti ai sensi del regolamento (UE) 2016/679 dall'Unione europea verso il Regno Unito.

(148) Nel secondo scenario, per quanto concerne la condivisione di dati raccolti da un'autorità di contrasto penale con un'agenzia di intelligence per finalità di sicurezza nazionale, la base giuridica che autorizza tale condivisione è la sezione 19 della *Counter Terrorism Act 2008* (legge antiterrorismo del 2008) ([210]). Conformemente a quest'ultima legge, qualsiasi persona può fornire informazioni a uno qualsiasi dei servizi di intelligence ai fini dell'adempimento di una qualsiasi delle funzioni di tale servizio, compresa la «sicurezza nazionale».

(149) Per quanto concerne le condizioni alle quali i dati possono essere condivisi per finalità di sicurezza nazionale, l'*Intelligence Services Act* ([211]) (legge sui servizi di intelligence) e la *Security Service Act* ([212]) (legge sui servizi di sicurezza) limitano la capacità dei servizi di intelligence di ottenere dati a ciò che è necessario per adempiere le loro funzioni statutarie. Le agenzie di contrasto che intendono condividere dati con i servizi di intelligence dovranno considerare una serie di fattori/limitazioni, oltre alle funzioni statutarie delle agenzie stabilite nella legge sui servizi di intelligence e nella legge sui servizi di sicurezza ([213]). La sezione 20 della legge antiterrorismo del 2008 chiarisce che qualsiasi condivisione dei dati ai sensi della sezione 19 di tale legge deve comunque rispettare la legislazione in materia di protezione dei dati; il che significa che si applicano tutte le limitazioni e tutti i requisiti di cui alla parte 3 della legge del 2018 sulla protezione dei dati. Inoltre, essendo autorità pubbliche ai fini della legge del 1998 sui diritti umani, le autorità competenti devono assicurare di agire in conformità con i diritti sanciti dalla convenzione, compreso l'articolo 8 della CEDU. Tali limitazioni assicurano che tutta la condivisione di dati tra le agenzie di contrasto e i servizi di intelligence sia conforme alla legislazione in materia di protezione dei dati e alla CEDU.

([208]) Cfr. ad esempio causa *M, R v the Chief Constable of Sussex Police* [2019] EWHC 975 (Admin) nel contesto della quale è stato chiesto all'Alta Corte di considerare la condivisione di dati tra la polizia e un *Business Crime Reduction Partnership* (BCRP, partenariato per la riduzione dei reati d'impresa), un'organizzazione autorizzata a gestire sistemi di avvisi di esclusione che vieta alle persone di entrare nei locali commerciali dei suoi membri. L'organo giurisdizionale ha esaminato la condivisione di dati che è avvenuta sulla base di un accordo avente la finalità di proteggere il pubblico e prevenire i reati e ha concluso in definitiva che la maggior parte degli aspetti della condivisione dei dati era lecita, fatta eccezione per alcune informazioni sensibili condivise tra la polizia e tale partenariato. Un altro esempio è la causa *Cooper v NCA* [2019] EWCA Civ 16 nell'ambito della quale la Corte d'appello ha confermato la condivisione di dati tra la polizia e la *Serious Organised Crime Agency* (SOCA, Agenzia di contrasto delle forme gravi di criminalità organizzata), un'agenzia di contrasto attualmente parte della NCA.

([209]) Sezione 36, paragrafo 4, della legge del 2018 sulla protezione dei dati.

([210]) Legge antiterrorismo del 2008, disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([211]) Legge del 1994 sui servizi di intelligence, disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/1994/13/contents.

([212]) Legge del 1989 sui servizi di sicurezza, disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/1989/5/contents.

([213]) L'articolo 2, paragrafo 2, della legge del 1994 sui servizi di intelligence prevede che «il capo del servizio di intelligence risponda dell'efficienza di tale servizio e che sia suo dovere assicurare: a) che vi siano dispositivi in essere destinati a garantire che nessuna informazione sia ottenuta dal servizio di intelligence, fatta eccezione nella misura necessaria per il corretto adempimento delle sue funzioni e che non sia divulgata alcuna informazione fatta eccezione per quanto necessario: i) a tale finalità; ii) nell'interesse della sicurezza nazionale; iii) ai fini della prevenzione o dell'accertamento di reati gravi; o iv) ai fini di qualsiasi procedimento penale; e b) che il servizio di intelligence non intraprenda alcuna azione per promuovere gli interessi di alcun partito politico del Regno Unito»; mentre la sezione 2, paragrafo 2, della legge del 1989 sui servizi di sicurezza prevede che «il direttore generale risponda dell'efficienza di tale servizio e che sia suo dovere assicurare: a) che vi siano dispositivi in essere destinati a garantire che nessuna informazione sia ottenuta dal servizio, fatta eccezione nella misura necessaria per il corretto adempimento delle sue funzioni, e che non sia divulgata alcuna informazione, fatta eccezione per quanto necessario a tale finalità o per finalità di prevenzione e accertamento [di reati gravi o ai fini di qualsiasi procedimento penale]; e b) che il servizio non intraprenda alcuna azione per promuovere gli interessi di alcun partito politico; e c) che vi siano accordi, concordati con il direttore generale della *National Crime Agency*, per il coordinamento delle attività del servizio in base alla sezione 1, paragrafo 4, del presente atto con le attività delle forze di polizia, la *National Crime Agency* e altre agenzie di contrasto».

(150) Quando un'autorità competente intende condividere dati personali trattati ai sensi della parte 3 della legge del 2018 sulla protezione dei dati con autorità di contrasto di un paese terzo, si applicano requisiti specifici ([214]). In particolare tali trasferimenti possono avvenire quando si basano su regolamenti di adeguatezza emessi dal segretario di Stato oppure, in assenza di tali regolamenti, devono essere assicurate garanzie adeguate. Secondo l'articolo 75 della legge del 2018 sulla protezione dei dati sussistono garanzie adeguate quando le garanzie sono stabilite da uno strumento giuridico che vincola il destinatario previsto, oppure se il titolare del trattamento, avendo valutato tutte le circostanze relative ai trasferimenti di tale tipo di dati personali verso il paese terzo o l'organizzazione internazionale, conclude che esistono garanzie adeguate per la protezione dei dati.

(151) Se non si basa su un regolamento di adeguatezza o su garanzie adeguate, il trasferimento può avvenire soltanto in determinate circostanze specifiche, indicate come «circostanze speciali» ([215]). Ciò si verifica quando il trasferimento è necessario: a) per tutelare un interesse vitale dell'interessato o di un'altra persona; b) per salvaguardare i legittimi interessi dell'interessato; c) per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un paese terzo; d) in singoli casi per qualsiasi finalità di contrasto; o e) in singoli casi per una finalità di legge (come in relazione a procedimenti giudiziari o per ottenere consulenza legale). Si può notare che le lettere d) ed e) non si applicano se i diritti e le libertà dell'interessato prevalgono sull'interesse pubblico al trasferimento. Tale serie di circostanze corrisponde alle situazioni e alle condizioni specifiche che si qualificano come «deroghe» ai sensi dell'articolo 38 della direttiva (UE) 2016/680.

(152) Inoltre, quando il materiale acquisito dalle autorità di contrasto in base a un mandato che autorizza l'utilizzo dell'intercettazione o dell'ingerenza in apparecchiature viene consegnato a un paese terzo, la legge del 2016 sui poteri di indagine impone garanzie ulteriori. In particolare, tale comunicazione, definita come «comunicazione all'estero», è consentita soltanto se l'autorità emittente ritiene che sussista un regime adeguato specifico che limita il numero di persone a cui vengono comunicati i dati, la misura in cui qualsiasi materiale viene divulgato o reso disponibile così come la misura in cui una parte qualsiasi di tale materiale viene copiata e il numero di copie effettuate. Inoltre l'autorità emittente può considerare che sia necessario un regime adeguato per assicurare che ogni copia fatta di qualsiasi parte di tale materiale sia distrutta non appena non sussistono più motivi pertinenti per conservarla (laddove non distrutta prima) ([216]).

(153) Infine, forme specifiche di trasferimenti successivi dal Regno Unito verso gli Stati Uniti potrebbero in futuro avvenire sulla base dell'*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* («l'accordo UK-US» o «l'accordo») ([217]), concluso nell'ottobre del 2019 ([218]). Sebbene l'accordo UK-US non sia ancora entrato in vigore al momento dell'adozione della presente decisione, la sua prevedibile entrata in vigore può incidere sui trasferimenti successivi verso gli Stati Uniti di dati trasferiti per la prima volta verso il Regno Unito sulla base della presente decisione. Più specificamente i dati trasferiti dall'UE verso fornitori di servizi nel Regno Unito potrebbero essere soggetti a ordinanze per la consegna di prove elettroniche emesse da autorità di contrasto statunitensi e rese applicabili nel Regno Unito ai sensi di detto accordo. Per questi motivi la valutazione delle condizioni e delle garanzie nel rispetto delle quali è possibile emettere tali ordinanze e dare loro esecuzione è pertinente ai fini della presente decisione.

([214]) Cfr. parte 3, capo 5, della legge del 2018 sulla protezione dei dati.

([215]) Sezione 76 della legge del 2018 sulla protezione dei dati.

([216]) Sezione 54 e sezione 130 della legge del 2016 sui poteri di indagine. Le autorità emittenti devono considerare la necessità di imporre garanzie specifiche al materiale consegnato alle autorità straniere, in maniera da assicurarsi che i dati siano soggetti a garanzie in termini di conservazione, distruzione e divulgazione di dati analoghe a quelle imposte nella sezione 53 e nella sezione 129 della legge del 2016 sui poteri di indagine.

([217]) *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.

([218]) Si tratta del primo accordo conseguito ai sensi della *US Clarifying Lawful Overseas Use of Data (CLOUD) Act* (legge statunitense che chiarisce l'utilizzo lecito oltremare di dati — legge CLOUD). La legge CLOUD è una legge federale statunitense che è stata adottata il 23 marzo 2018 e che chiarisce, attraverso una modifica della *Stored Communications Act* (legge sulle comunicazioni conservate) del 1986, che i fornitori di servizi statunitensi sono tenuti a rispettare le ordinanze statunitensi di divulgazione dei contenuti e dei dati non relativi ai contenuti, indipendentemente dall'ubicazione in cui tali dati sono conservati. La legge CLOUD consente altresì la conclusione di accordi esecutivi con governi stranieri, sulla base dei quali fornitori di servizi statunitensi sarebbero in grado di fornire dati sui contenuti direttamente a tali governi stranieri (il testo della legge CLOUD è disponibile al seguente indirizzo: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

(154) A tale riguardo occorre osservare che, in primo luogo, per quanto concerne il suo ambito di applicazione materiale, l'accordo è applicabile soltanto ai reati punibili con una pena detentiva della durata massima di almeno tre anni (definiti come «reati gravi») ([219]), comprese le «attività terroristiche». In secondo luogo, i dati trattati nell'altra giurisdizione possono essere ottenuti ai sensi di tale accordo soltanto in seguito a una «ordinanza [...] soggetta a riesame o vigilanza ai sensi del diritto interno della parte emittente da parte di un organo giurisdizionale, un giudice, un magistrato o un'altra autorità indipendente prima di o durante i procedimenti riguardanti l'applicazione dell'ordinanza» ([220]). In terzo luogo, qualsiasi ordinanza deve «essere basata su requisiti per una giustificazione ragionevole basata su fatti articolabili e credibili, particolarità, legalità e gravità relativi alla condotta oggetto di indagine» ([221]) nonché «essere mirata su conti specifici e individuare una persona specifica o un conto, un indirizzo o un dispositivo personale specifico oppure qualsiasi altro identificatore specifico» ([222]). In quarto luogo, i dati ottenuti ai sensi di tale accordo beneficiano di protezioni equivalenti alle garanzie specifiche previste dal cosiddetto «accordo quadro UE-US» ([223]), un accordo generale in materia di protezione dei dati concluso nel dicembre 2016 dall'UE e dagli Stati Uniti e che stabilisce le garanzie e i diritti applicabili ai trasferimenti di dati nel settore della cooperazione tra autorità di contrasto, che sono tutte integrate in tale accordo mediante riferimento, *mutatis mutandis*, per tenere conto in particolare della natura specifica dei trasferimenti (ossia trasferimenti da operatori privati a un'autorità di contrasto, piuttosto che trasferimenti tra autorità di contrasto) ([224]). L'accordo UK-US prevede specificamente che verranno applicate protezioni equivalenti a quelle previste dall'accordo quadro UE-USA «a tutte le informazioni personali prodotte nell'esecuzione di ordinanze soggette all'accordo in maniera da produrre protezioni equivalenti» ([225]).

(155) I dati trasferiti ad autorità statunitensi ai sensi dell'accordo UK-US dovrebbero pertanto beneficiare di protezioni fornite da uno strumento del diritto dell'Unione, con gli adattamenti necessari per riflettere la natura dei trasferimenti in questione. Le autorità del Regno Unito hanno inoltre confermato che le protezioni dell'accordo quadro si applicheranno a tutte le informazioni personali prodotte o conservate ai sensi dell'accordo, indipendentemente dalla natura o dal tipo di organismo che presenta la richiesta (ad esempio tanto le autorità di contrasto federali quanto quelle statali degli Stati Uniti), di conseguenza in tutti i casi deve essere fornita una protezione equivalente. Tuttavia le autorità del Regno Unito hanno altresì spiegato che i dettagli dell'attuazione concreta delle garanzie in materia di protezione dei dati sono ancora oggetto di discussioni tra il Regno Unito e gli Stati Uniti. Nel contesto dei colloqui con i servizi della Commissione europea in merito alla presente decisione, le autorità del Regno Unito hanno confermato che consentiranno all'accordo di entrare in vigore soltanto dopo aver accertato che la sua attuazione sia conforme agli obblighi giuridici in esso previsti, compresa la chiarezza rispetto alla conformità con i livelli di protezione dei dati per eventuali dati richiesti ai sensi di tale accordo. Dato che una possibile entrata in vigore di tale accordo può incidere sul livello di protezione valutato nella presente decisione, qualsiasi informazione e chiarimento futuro riguardante il modo in cui gli Stati Uniti rispetteranno i loro obblighi nell'ambito dell'accordo dovrebbe essere comunicato dal Regno Unito alla Commissione europea, non appena si renda disponibile e in ogni caso prima dell'entrata in vigore dell'accordo, in maniera da garantire un corretto monitoraggio della presente decisione in linea con l'articolo 45, paragrafo 4, del regolamento (UE) 2016/679. Particolare attenzione sarà prestata all'applicazione e all'adattamento delle protezioni di cui all'accordo quadro in relazione al tipo specifico di trasferimenti oggetto dell'accordo UK-US.

(156) Più in generale, qualsiasi sviluppo pertinente per quanto concerne l'entrata in vigore e l'applicazione dell'accordo sarà debitamente preso in considerazione nel contesto del monitoraggio continuo della presente decisione, anche rispetto alle necessarie conseguenze da trarre in caso di indicazione che non sia più garantito un livello di protezione sostanzialmente equivalente.

3.2.3 *Vigilanza*

(157) A seconda dei poteri utilizzati dalle autorità competenti durante il 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), organismi diversi assicurano la vigilanza sull'utilizzo di tali poteri. In particolare l'*Information Commissioner* vigila sul

([219]) Articolo 1, paragrafo 14, dell'accordo.
([220]) Articolo 5, paragrafo 2, dell'accordo.
([221]) Articolo 5, paragrafo 1, dell'accordo.
([222]) Articolo 4, paragrafo 5, dell'accordo. Un livello aggiuntivo e più rigoroso si applica in relazione all'intercettazione in tempo reale: le ordinanze devono avere una durata limitata, che non deve essere più lunga di quanto sia ragionevolmente necessario per realizzare le finalità dell'ordinanza, e devono essere emesse soltanto se le stesse informazioni non avrebbero potuto essere ragionevolmente ottenute ricorrendo a un metodo meno intrusivo (articolo 5, paragrafo 3, dell'accordo).
([223]) 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), disponibile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:22016A1210(01)&from=IT.
([224]) Articolo 9, paragrafo 1, dell'accordo.
([225]) Articolo 9, paragrafo 1, dell'accordo.

trattamento di dati personali quando quest'ultimo rientra nell'ambito di applicazione della parte 3 della legge del 2018 sulla protezione dei dati ([226]). La vigilanza indipendente e giudiziaria sull'uso dei poteri di indagine ai sensi della legge del 2016 sui poteri di indagine è assicurata dall'*Investigatory Powers Commissioner Office* (IPCO) ([227]) (questo aspetto è affrontato nei considerando da 250 a 255). Inoltre una vigilanza aggiuntiva è garantita dal parlamento così come da altri organismi.

3.2.3.1 Vigilanza sulla parte 3 della legge del 2018 sulla protezione dei dati

(158) Le funzioni generali dell'*Information Commissioner* di cui l'indipendenza e l'organizzazione sono spiegate al considerando 87 — in relazione al trattamento di dati personali che rientra nell'ambito di applicazione della parte 3 della legge del 2018 sulla protezione dei dati sono stabilite nell'allegato 13 di detta legge. Il compito principale dell'ICO consiste nel monitorare e far rispettare la parte 3 della legge del 2018 sulla protezione dei dati, nel promuovere la sensibilizzazione del pubblico e nel consigliare il parlamento, il governo e altre istituzioni e organismi. Ai fini del mantenimento dell'indipendenza del potere giudiziario, l'*Information Commissioner* non è autorizzato a esercitare le sue funzioni in relazione al trattamento di dati personali da parte di un soggetto o di un organo giurisdizionale che agisce nell'esercizio delle proprie funzioni giurisdizionali. In tali circostanze altri organismi esercitano le funzioni di vigilanza, come spiegato ai considerando da 99 a 103.

(159) All'*Information Commissioner* sono riconosciuti poteri generali di indagine, correttivi, autorizzativi e consultivi in relazione al trattamento di dati personali al quale si applica la parte 3. In particolare l'*Information Commissioner* ha il potere di notificare al titolare del trattamento o al responsabile del trattamento una presunta violazione della parte 3 della legge del 2018 sulla protezione dei dati, di emettere avvertimenti o ammonimenti nei confronti di un titolare del trattamento o di un responsabile del trattamento che abbia violato le disposizioni della parte 3 di detta legge, nonché di emettere di propria iniziativa o su richiesta, pareri indirizzati al parlamento, al governo o ad altre istituzioni e ad altri organismi nonché al pubblico in merito a qualsiasi questione relativa alla protezione dei dati personali ([228]).

(160) Inoltre l'*Information Commissioner* ha il potere di emettere avvisi di informazione ([229]), avvisi di valutazione ([230]) e avvisi di esecuzione ([231]) nonché il potere di accedere ai documenti di titolari del trattamento e responsabili del trattamento, di accedere ai loro locali ([232]) ed emettere sanzioni amministrative pecuniarie sotto forma di avvisi di irrogazione di sanzioni ([233]). La *Regulatory Action Policy* dell'ICO stabilisce le circostanze in cui l'Ufficio emette rispettivamente avvisi di informazione, di valutazione, di esecuzione e di irrogazione di sanzioni ([234]) (cfr. anche il considerando 93 e la decisione di adeguatezza sulla direttiva (UE) 2016/680, considerando 101 e 102).

(161) Secondo le sue ultime relazioni annuali (2018– 2019 ([235]), 2019- 2020 ([236])), l'*Information Commissioner* ha condotto una serie di indagini ed adottato misure di esecuzione in relazione al trattamento di dati da parte delle autorità di contrasto. Ad esempio l'*Information Commissioner* ha condotto un'indagine e ha pubblicato un parere nell'ottobre del 2019 in merito all'utilizzo da parte delle autorità di contrasto di tecnologie di riconoscimento facciale nei luoghi pubblici. Tale indagine si è concentrata in particolare sull'uso delle capacità di riconoscimento facciale nel contesto del servizio di polizia del Galles meridionale e del servizio di polizia metropolitano. L'*Information Commissioner* ha indagato altresì in merito a «Gangs Matrix» ([237]) del servizio di polizia metropolitano e ha riscontrato una serie di gravi violazioni della legge sulla protezione dei dati che potrebbero compromettere la fiducia del pubblico nella matrice e nelle modalità di utilizzo dei dati. Nel novembre del 2018 l'*Information Commissioner* ha emesso un avviso di esecuzione e il servizio di polizia

([226]) Sezione 116 della legge del 2018 sulla protezione dei dati.
([227]) Cfr. legge del 2016 sui poteri di indagine e in particolare la parte 8, capo 1.
([228]) Paragrafo 2 dell'allegato 13 della legge del 2018 sulla protezione dei dati.
([229]) Che ordina al titolare del trattamento e al responsabile del trattamento (e in certe circostanze a qualsiasi altra persona) di fornire le informazioni necessarie (articolo 142 della legge del 2018 sulla protezione dei dati).
([230]) Che consente lo svolgimento di indagini e verifiche, che possono imporre al titolare del trattamento o al responsabile del trattamento di consentire all'*Information Commissioner* di accedere a locali specificati, ispezionare o esaminare documenti o apparecchiature, esaminare persone che trattano dati personali per conto del titolare del trattamento (articolo 146 della legge del 2018 sulla protezione dei dati).
([231]) Che consente l'esercizio di poteri correttivi, che richiede ai titolari del trattamento/ai responsabili del trattamento di adottare o di astenersi dall'adottare le misure specificate (sezione 149 della legge del 2018 sulla protezione dei dati).
([232]) Sezione 154 della legge del 2018 sulla protezione dei dati.
([233]) Sezione 155 della legge del 2018 sulla protezione dei dati.
([234]) *Regulatory Action Policy*, cfr. nota 96.
([235]) *Information Commissioner's Annual Report and Financial Statements 2018-19*, cfr. nota 101.
([236]) *Information Commissioner's Annual Report and Financial Statements 2019-20*, cfr. nota 82.
([237]) Una banca dati che registrava intelligence in merito a presunti membri di bande criminali e vittime di reati correlati alle bande.

metropolitano ha successivamente adottato le misure necessarie per aumentare la sicurezza e la responsabilizzazione nonché per assicurare che i dati venissero utilizzati in maniera proporzionale. Un ulteriore esempio di un'azione di esecuzione in questo settore è la sanzione pecuniaria di 325 000 GBP comminata dall'*Information Commissioner* nel maggio del 2018 nei confronti del *Crown Prosecution Service*, per aver perso DVD non crittografati contenenti registrazioni di interrogatori di polizia. L'*Information Commissioner* ha condotto inoltre indagini su argomenti di più ampia portata; ad esempio nella prima metà del 2020 ha indagato sull'uso dell'estrazione di dati da telefoni cellulari per finalità di polizia nonché sul trattamento di dati di vittime da parte della polizia. Inoltre l'*Information Commissioner* sta attualmente indagando in merito a un caso che implica l'accesso da parte delle autorità di contrasto a dati detenuti da un soggetto del settore privato, Clearview AI Inc ([238]).

(162) Oltre ai poteri di esecuzione dell'*Information Commissioner* menzionati ai considerando 160 e 161, talune violazioni della legislazione in materia di protezione dei dati costituiscono reati e possono pertanto essere soggette a sanzioni penali (articolo 196 della legge del 2018 sulla protezione dei dati). Si tratta ad esempio dell'ottenimento, della comunicazione o della conservazione di dati personali senza il consenso del titolare del trattamento, e della trasmissione di dati personali a un'altra persona senza il consenso del titolare del trattamento ([239]); della reidentificazione di informazioni a partire da dati personali anonimizzati senza il consenso del titolare del trattamento responsabile dell'anonimizzazione dei dati personali ([240]); dell'ostruzione intenzionale dell'esercizio da parte dell'*Information Commissioner* dei suoi poteri in relazione all'ispezione di dati personali conformemente agli obblighi internazionali ([241]), del rilascio di dichiarazioni false in risposta a un avviso di informazione o della distruzione di informazioni in relazione ad avvisi di informazione e di valutazione ([242]).

3.2.3.2 Altri organismi di vigilanza nel settore delle attività di contrasto penale

(163) Oltre all'*Information Commissioner*, vi sono diversi organismi di vigilanza nel settore delle attività di contrasto in materia penale aventi mandati specifici pertinenti per questioni concernenti la protezione dei dati. Tra di essi figurano il *Biometrics Commissioner* ([243]) (commissario per la conservazione e l'uso di materiale biometrico) e il *Surveillance Camera Commissioner* ([244]) (commissario per le telecamere di sorveglianza).

3.2.3.3 Vigilanza parlamentare nel settore delle attività di contrasto penale

(164) L'*Home Affairs Select Committee* (HASC, commissione ad hoc per gli affari interni) assicura la vigilanza parlamentare nel settore delle attività di contrasto. Tale commissione è costituita da 11 membri del parlamento, appartenenti ai tre maggiori partiti politici. Detta commissione ha il compito di esaminare le spese, l'amministrazione e la politica del ministero dell'Interno e degli organismi pubblici associati, ossia in particolare le forze di polizia e la NCA, il cui lavoro può essere in particolare oggetto di esame da parte della commissione ([245]).

([238]) Cfr. dichiarazione dell'ICO, disponibile al seguente indirizzo: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/.

([239]) Sezione 170 della legge del 2018 sulla protezione dei dati.

([240]) Sezione 171 della legge del 2018 sulla protezione dei dati.

([241]) Sezione 119, paragrafo 6, della legge del 2018 sulla protezione dei dati.

([242]) Durante l'esercizio finanziario che copre il periodo dal 1° aprile 2019 al 31 marzo 2020, le indagini dell'ICO hanno portato a quattro diffide e otto procedimenti giudiziari. Tali casi sono stati perseguiti ai sensi della sezione 55 della legge del 1998 sulla protezione dei dati, della sezione 77 della legge del 2000 sulla libertà di informazione e della sezione 170 della legge del 2018 sulla protezione dei dati. Nel 75 % dei casi, i convenuti si sono dichiarati colpevoli evitando la necessità di lunghi procedimenti giudiziari, così come i costi associati. (*Information Commissioner's Annual Report and Financial Statements 2019/2020*, cfr. nota 87, pagina 40).

([243]) Il *Biometrics Commissioner* è stato istituito dalla *Protection of Freedoms Act 2012* (legge del 2012 sulla protezione delle libertà) (cfr. https://www.legislation.gov.uk/ukpga/2012/9/contents). Tra le altre funzioni, il *Biometrics Commissioner* decide se la polizia possa o meno conservare registrazioni dei profili DNA e impronte digitali ottenute da persone arrestate ma non accusate di un reato qualificato (sezione 63G della legge del 1984 sulle prove nelle attività di polizia e di azione penale). Inoltre al *Biometrics Commissioner* spetta la competenza generale per sottoporre ad esame la conservazione e l'utilizzo di DNA e impronte digitali, così come la conservazione per motivi di sicurezza nazionale (sezione 20, paragrafo 2, della legge del 2012 sulla protezione delle libertà). Il *Biometrics Commissioner* è nominato conformemente al codice per le nomine pubbliche (disponibile al seguente indirizzo: https://www.gov.uk/government/publications/governance-code-for-public-appointments) e il suo mandato precisa che può essere rimosso dalle sue funzioni solo dal segretario di Stato in presenza di una serie di circostanze rigorosamente definite, tra cui l'inadempimento delle proprie funzioni per un periodo di tre mesi, la condanna per un reato o il mancato rispetto del mandato.

([244]) Il *Surveillance Camera Commissioner* è stato istituito dalla legge del 2012 sulla protezione delle libertà e ha il ruolo di incoraggiare il rispetto del codice di pratica in merito alle telecamere di sorveglianza; riesaminare il funzionamento di tale codice; e fornire consulenza ai ministri in merito all'eventualità che tale codice necessiti di modifiche. Detto commissario è nominato in base alle stesse norme dei *Biometrics Commissioner* e gode di analoghi poteri, risorse e tutele dalla rimozione.

([245]) Cfr. https://committees.parliament.uk/committee/83/home-affairs-committee/news/100537/work-of-the-national-crime-agency-scrutinised/

(165) Nel rispetto dei limiti del suo mandato, tale commissione può scegliere il proprio oggetto di inchiesta, compresi casi specifici, a condizione che la questione non sia *sub iudice*. Tale commissione può altresì cercare di ottenere prove scritte e orali da una vasta gamma di gruppi e di persone fisiche pertinenti. Produce relazioni sulle sue risultanze ed emette raccomandazioni indirizzate al governo ([246]). Il governo deve rispondere a ciascuna delle raccomandazioni di una relazione entro 60 giorni ([247]).

(166) Nel settore della sorveglianza, la commissione ha prodotto anche una relazione relativa alla legge del 2000 sul regolamento sui poteri di indagine (RIPA 2000) ([248]), dalla quale è emerso che tale legge non era adeguata alla finalità. Tale relazione è stata presa in considerazione durante la sostituzione di parti significative della RIPA 2000 con la legge del 2016 sui poteri di indagine. Un elenco completo delle indagini è disponibile sul sito web della commissione ([249]).

(167) In Scozia i compiti della commissione ad hoc per gli affari interni sono svolti dalla *Justice Subcommittee on Policing* (sottocommissione per la giustizia sulle attività di polizia), mentre in Irlanda del Nord sono svolti dalla *Committee for Justice* (commissione per la giustizia) ([250]).

3.2.4 *Mezzi di ricorso*

(168) Per quanto concerne il trattamento di dati da parte delle autorità di contrasto, meccanismi di ricorso sono disponibili ai sensi della parte 3 della legge del 2018 sulla protezione dei dati e della legge del 2016 sui poteri di indagine, nonché ai sensi della legge del 1998 sui diritti umani.

(169) Tale serie di meccanismi offre agli interessati mezzi di ricorso effettivi in sede amministrativa e giudiziale che consentono loro in particolare di assicurare i loro diritti, compreso il diritto di avere accesso ai propri dati personali o di ottenerne la rettifica o la cancellazione.

(170) Innanzitutto, ai sensi della sezione 165 della legge del 2018 sulla protezione dei dati, l'interessato ha il diritto di proporre reclamo presso l'*Information Commissioner* qualora ritenga che, in relazione ai dati personali che lo riguardano, sia stata commessa una violazione della parte 3 della legge del 2018 sulla protezione dei dati ([251]). L'*Information Commissioner* ha il potere di valutare il rispetto della legge del 2018 sulla protezione dei dati da parte del titolare del trattamento e del responsabile del trattamento, di richiedere loro di adottare misure necessarie in caso di non conformità nonché di irrogare sanzioni pecuniarie.

([246]) Le commissioni ad hoc, compresa quella per gli affari interni, sono soggette ad ordinanze permanenti della Camera dei Comuni. Le ordinanze permanenti sono norme, concordate dalla Camera dei Comuni, che disciplinano il modo in cui il parlamento opera. Il mandato delle commissioni ad hoc è ampio, dato che l'ordinanza permanente 152(1) prevede che le «commissioni ad hoc siano nominate per esaminare le spese, l'amministrazione e la politica dei principali dipartimenti governativi di cui al paragrafo 2 della presente ordinanza ed associati ad organismi pubblici». Ciò consente alla commissione ad hoc per gli affari interni di esaminare qualsiasi politica di cui il ministero dell'Interno è titolare, che comprende politiche (e la legislazione correlata) in materia di poteri di indagine. L'ordinanza permanente 152(4) chiarisce inoltre che alle commissioni spettano vari poteri, compresa la capacità di richiedere alle persone di fornire prove o documenti in merito a una questione particolare e di produrre relazioni. Le indagini attuali e precedenti indagini della commissione sono disponibili al seguente indirizzo: https://committees.parliament.uk/committee/83/home-affairs-committee/.

([247]) I poteri della commissione ad hoc per gli affari interni in Inghilterra e Galles sono riportati nelle ordinanze permanenti della Camera dei Comuni, disponibili al seguente indirizzo: https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

([248]) Disponibile al seguente indirizzo: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm.

([249]) Disponibile al seguente indirizzo: https://committees.parliament.uk/committee/83/home-affairs-committee.

([250]) Le norme per la sottocommissione per la giustizia sulle attività di polizia in Scozia sono disponibili al seguente indirizzo: https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx; mentre le norme per la commissione per la giustizia in Irlanda del Nord sono illustrate al seguente indirizzo: http://www.niassembly.gov.uk/assembly-business/standing-orders/.

([251]) L'ultima relazione annuale dell'ICO riporta una ripartizione della natura dei reclami ricevuti e chiusi. In particolare, il numero di reclami ricevuti in relazione a «registri di polizia e penali» rappresenta il 6 % del numero totale di reclami ricevuti (con un aumento dell'1 % rispetto all'esercizio finanziario precedente). La relazione annuale mostra inoltre che i reclami riguardanti le richieste di accesso degli interessati rappresentano il valore più elevato (46 % rispetto al numero totale di reclami, con un aumento dell'8 % rispetto all'esercizio finanziario precedente) (ICO, *Annual report 2019-2020*, pag. 55; cfr. nota 88).

(171) In secondo luogo la legge del 2018 sulla protezione dei dati prevede il diritto a disporre di un mezzo di ricorso nei confronti dell'*Information Commissioner* qualora non gestisca adeguatamente un reclamo presentato dall'interessato. Più specificamente se l'*Information Commissioner* non fa «progredire» ([252]) un reclamo promosso dall'interessato, il reclamante ha accesso a un ricorso giurisdizionale, in quanto può adire un *First-tier Tribunal* ([253]) (tribunale di primo grado) affinché quest'ultimo ordini all'*Information Commissioner* di adottare misure adeguate per dare seguito al reclamo oppure di informare il reclamante in merito ai progressi compiuti in relazione al reclamo ([254]). Inoltre qualsiasi persona che riceva uno qualsiasi degli avvisi menzionati (di informazione, di valutazione, di esecuzione o di irrogazione di sanzioni) dall'*Information Commissioner* può impugnarlo adendo un *First-tier Tribunal*. Laddove quest'ultimo ritenga che la decisione dell'*Information Commissioner* non sia conforme alla legge o che questi avrebbe dovuto esercitare il proprio potere discrezionale in modo diverso, detto organo deve accogliere il ricorso oppure sostituire l'avviso o la decisione con un altro avviso o un'altra decisione che l'*Information Commissioner* avrebbe potuto emettere o rendere ([255]).

(172) In terzo luogo le persone fisiche possono presentare un ricorso giurisdizionale nei confronti di titolari del trattamento e responsabili del trattamento adendo direttamente gli organi giurisdizionali. In particolare ai sensi della sezione 167 della legge del 2018 sulla protezione dei dati, l'interessato può presentare una domanda dinanzi un organo giurisdizionale in relazione a una violazione di un diritto riconosciutogli dalla legislazione in materia di protezione dei dati e, mediante un'ordinanza, detto organo giurisdizionale può richiedere al titolare del trattamento di adottare (o di astenersi dall'adottare) qualsiasi misura in relazione al trattamento per conformarsi alla legge del 2018 sulla protezione dei dati. Inoltre, ai sensi della sezione 169 della legge del 2018 sulla protezione dei dati, qualsiasi persona che subisca danni a causa di una violazione di un requisito sancito dalla legislazione in materia di protezione dei dati (compresa la parte 3 della legge del 2018 sulla protezione dei dati), diversa dal GDPR del Regno Unito, ha diritto al risarcimento di tali danni da parte del titolare del trattamento o del responsabile del trattamento, fatta eccezione per il caso in cui né titolare del trattamento né il responsabile del trattamento sia in alcun modo responsabile per l'evento che ha cagionato i danni in questione. Tali danni comprendono tanto la perdita finanziaria quanto danni che non contemplano una perdita finanziaria, quali ad esempio la sofferenza.

(173) Infine, qualsiasi persona, nella misura in cui ritenga che i suoi diritti, compresi quelli relativi alla tutela della vita privata e alla protezione dei dati, siano stati violati da qualsiasi autorità pubblica, può ottenere rimedio dinanzi gli organi giurisdizionali del Regno Unito ai sensi della legge del 1998 sui diritti umani ([256]); inoltre, dopo aver esperito i mezzi di ricorso nazionali, una persona, un'organizzazione non governativa così come gruppi di persone fisiche possono ottenere rimedio adendo la Corte europea dei diritti dell'uomo per violazioni dei diritti garantiti ai sensi della convenzione europea dei diritti dell'uomo ([257]) (cfr. considerando 111).

3.2.4.1 Meccanismi di ricorso disponibili ai sensi della legge del 2016 sui poteri di indagine

(174) Le persone fisiche possono ottenere riparazione per violazioni della legge del 2016 sui poteri di indagine adendo l'*Investigatory Powers Tribunal* (organo giurisdizionale competente per i poteri di indagine). I mezzi di ricorso disponibili ai sensi della legge del 2016 sui poteri di indagine sono descritti nei considerando da 263 a 269.

([252]) La sezione 166 della legge del 2018 sulla protezione dei dati fa riferimento specificamente alle seguenti situazioni: a) l'*Information Commissioner* non adotta misure adeguate per dare seguito al reclamo; b) l'*Information Commissioner* non fornisce al reclamante informazioni in merito ai progressi compiuti in relazione al reclamo o in merito all'esito del reclamo prima dello scadere di un termine di 3 mesi a decorrere dal momento della ricezione del reclamo da parte dello stesso; oppure c) laddove l'esame del reclamo da parte dell'*Information Commissioner* non venga concluso entro tale termine, quest'ultimo non fornisce al reclamante tali informazioni durante un successivo periodo di 3 mesi.

([253]) Il *First-tier Tribunal* è l'organo giurisdizionale competente per la gestione di ricorsi nei confronti di decisioni pronunciate da organismi di regolamentazione del governo. Nel caso della decisione dell'*Information Commissioner*, la camera competente è la «*General Regulatory Chamber*» avente competenza giurisdizionale su tutto il Regno Unito.

([254]) Sezione 166 della legge del 2018 sulla protezione dei dati. Tra gli esempi di azioni promosse con successo contro l'ICO dinanzi detto organo si può citare un caso nel contesto del quale l'ICO ha confermato la ricezione di un reclamo da parte di un interessato ma non ha indicato quale linea d'azione intendeva adottare; gli è stato pertanto intimato di confermare, entro 21 giorni di calendario, se intendeva indagare in merito al reclamo e, in caso affermativo, di informare in seguito il reclamante in merito ai progressi dell'indagine almeno ogni 21 giorni di calendario (la sentenza non è ancora stata pubblicata). In un altro caso, il *First-tier Tribunal* ha ritenuto che non fosse chiaro se la risposta dell'ICO a un reclamante costituisse o meno l'«esito» adeguato del reclamo (cfr. *Susan Milne v The Information Commissioner* [2020], sentenza disponibile al seguente indirizzo: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

([255]) Sezioni 162 e 163 della legge del 2018 sulla protezione dei dati.

([256]) Cfr. ad esempio *Brown v Commissioner of Police of the Metropolis & Anor* [2019] EWCA Civ 1724 nel contesto della quale è stato riconosciuto un risarcimento per danni pari a 9 000 GBP ai sensi della legge del 1998 sulla protezione dei dati e della legge del 1998 sui diritti umani in ragione dell'ottenimento e dell'utilizzo improprio di informazioni personali così come la sentenza nella causa *R (on the application of Bridges) v Chief Constable of South Wales* [2020] EWCA Civ 1058 nel contesto della quale la Corte d'appello ha dichiarato illecito l'impiego di un sistema di riconoscimento facciale da parte delle forze di polizia del Galles, in quanto violava l'articolo 8 della CEDU e la valutazione d'impatto sulla protezione dei dati presentata dal titolare del trattamento non era conforme alla legge del 2018 sulla protezione dei dati.

([257]) L'articolo 34 della convenzione europea dei diritti dell'uomo prevede che «[l]a Corte può essere investita di un ricorso da parte di una persona fisica, un'organizzazione non governativa o un gruppo di privati che sostenga d'essere vittima di una violazione da parte di una delle Alte Parti contraenti dei diritti riconosciuti nella Convenzione o nei suoi protocolli. Le Alte Parti contraenti si impegnano a non ostacolare con alcuna misura l'esercizio effettivo di tale diritto».

3.3 **Accesso e uso da parte delle autorità pubbliche del Regno Unito per motivi di sicurezza nazionale**

(175) Nell'ordine giuridico del Regno Unito, i servizi di intelligence autorizzati a raccogliere informazioni elettroniche detenute da titolari del trattamento o responsabili del trattamento per motivi di sicurezza nazionale, in situazioni pertinenti per uno scenario di adeguatezza, sono il *Security Service* ([258]) (MI5), il *Secret Intelligence Service* ([259]) (SIS) e il *Government Communications Headquarters* ([260]) (GCHQ) ([261]).

3.3.1 *Basi giuridiche, limitazioni e garanzie*

(176) Nel Regno Unito i poteri delle agenzie di intelligence sono stabiliti dalla legge del 2016 sui poteri di indagine e dalla RIPA 2000, che, unitamente alla legge del 2018 sulla protezione dei dati, definiscono l'ambito di applicazione materiale e personale di tali poteri e le limitazioni e garanzie per il loro esercizio. Tali poteri nonché i limiti e le garanzie ed essi applicabili sono valutati in dettaglio nelle sezioni che seguono.

3.3.1.1 Poteri di indagine esercitati nel contesto della sicurezza nazionale

(177) La legge del 2016 sui poteri di indagine definisce il quadro giuridico per l'utilizzo dei poteri di indagine, ossia il potere di intercettare, accedere ai dati relativi alle comunicazioni e attuare ingerenze nelle apparecchiature. La legge del 2016 sui poteri di indagine vieta, sotto forma di divieto generale, e qualifica come reato l'utilizzo di tecniche che consentono l'accesso a contenuti di comunicazioni, l'accesso a dati relativi alle comunicazioni o ingerenze nelle apparecchiature senza autorizzazione legittima ([262]). Ciò si riflette nel fatto che l'esercizio di tali poteri di indagine è lecito soltanto se effettuato sulla base di un mandato o di un'autorizzazione ([263]).

(178) La legge del 2016 sui poteri di indagine stabilisce norme dettagliate che disciplinano l'ambito di applicazione e l'applicazione di ciascun potere di indagine, e le relative limitazioni e garanzie specifiche. Si applicano norme diverse a seconda del tipo di potere di indagine (intercettazione di comunicazioni, acquisizione e

([258]) L'MI5 è soggetto all'autorità del segretario di Stato per gli Affari interni. La legge del 1989 sul servizio di sicurezza stabilisce le funzioni dell'MI5: protezione della sicurezza nazionale (compresa la protezione nei confronti di minacce di spionaggio, terrorismo e sabotaggio, nei confronti di attività di agenti di potenze straniere e di azioni destinate a rovesciare o minare la democrazia parlamentare ricorrendo a mezzi politici, industriali o violenti), salvaguardia del benessere economico del Regno Unito contro minacce esterne e attività di sostegno a favore delle forze di polizia e delle altre agenzie di contrasto nella prevenzione e nell'accertamento di reati gravi.

([259]) Il SIS è soggetto all'autorità del *Foreign Secretary* (segretario di Stato per gli affari esteri) e le sue funzioni sono stabilite nella legge del 1994 sui servizi di intelligence. Le sue funzioni consistono nell'ottenere e nel fornire informazioni in merito ad azioni o intenzioni di persone al di fuori delle isole britanniche nonché nello svolgere altri compiti relativi alle azioni o alle intenzioni di tali persone. Tali funzioni possono essere esercitate soltanto nell'interesse della sicurezza nazionale, nell'interesse del benessere economico del Regno Unito o a sostegno della prevenzione o dell'accertamento di reati gravi.

([260]) Il GCHQ è soggetto all'autorità del segretario di Stato per gli affari esteri e le sue funzioni sono stabilite nella legge del 1994 sui servizi di intelligence. Tali funzioni sono: a) monitorare, utilizzare o interferire con emissioni elettromagnetiche e di altro tipo nonché con apparecchiature che producono tali emissioni, ottenere e fornire informazioni derivanti da o relative a tali emissioni o apparecchiature e da materiale crittografato; b) fornire consulenza e assistenza in ambito linguistico, compresa la terminologia utilizzata per questioni tecniche e di crittografia e altre questioni relative alla protezione delle informazioni a favore delle forze armate, del governo o di altre organizzazioni o persone ritenute appropriate. Tali funzioni possono essere esercitate soltanto nell'interesse della sicurezza nazionale, nell'interesse del benessere economico del Regno Unito in relazione ad azioni o intenzioni di persone al di fuori delle isole britanniche o a sostegno della prevenzione o dell'accertamento di reati gravi.

([261]) Altri organismi pubblici che esercitano funzioni pertinenti per la sicurezza nazionale sono la *Defence Intelligence* (DI), il *National Security Council and Secretariat*, la *Joint Intelligence Organisation* e il *Joint Intelligence Committee*. Tuttavia né il JIC né il JIO sono in grado di utilizzare poteri di indagine ai sensi della legge del 2016 sui poteri di indagine, mentre la DI dispone di un ambito limitato di applicazione dei propri poteri.

([262]) Il divieto si applica alle reti di comunicazione tanto pubbliche quanto private, nonché al servizio postale pubblico quando l'intercettazione viene effettuata nel Regno Unito. Il divieto non si applica al titolare del trattamento di una rete privata se quest'ultimo ha prestato il proprio consenso espresso o implicito allo svolgimento dell'intercettazione (articolo 3 della legge del 2016 sui poteri di indagine).

([263]) In specifici limitati casi, un'intercettazione lecita in assenza di mandato è possibile, ossia quando si effettua l'intercettazione con il consenso del mittente o del destinatario (articolo 44 della legge del 2016 sui poteri di indagine), in caso di finalità limitate amministrative o di contrasto (articoli da 45 a 48 della medesima legge), presso determinate istituzioni speciali (articoli da 49 a 51 della medesima legge) nonché in conformità con richieste provenienti dall'estero (articolo 52 della medesima legge).

conservazione di dati relativi alle comunicazioni e ingerenza in apparecchiature) ([264]), nonché della possibilità che tale potere sia esercitato in relazione a un obiettivo specifico o in maniera massiva. I dettagli sull'ambito di applicazione, le garanzie e le limitazioni di ciascuna misura previsti dalla legge del 2016 sui poteri di indagine sono descritti nella sezione specifica che segue.

(179) Inoltre la legge del 2016 sui poteri di indagine è integrata da una serie di codici di pratica statutari, emessi dal segretario di Stato, approvati da entrambe le camere del parlamento ([265]) e applicabili in tutto il paese, che forniscono ulteriori orientamenti in merito all'esercizio di tali poteri ([266]). Mentre gli interessati possono avvalersi direttamente delle disposizioni previste dalla legge del 2016 sui poteri di indagine per esercitare i loro diritti, l'allegato 7, paragrafo 5, della medesima legge specifica che i codici di pratica sono ammissibili come prova nel contesto di procedimenti civili e penali e che l'organo giurisdizionale o l'autorità di controllo può tenere conto di qualsiasi non conformità rispetto ai codici quando esamina una questione pertinente nel contesto di un procedimento giudiziario ([267]). Nel contesto della valutazione della «qualità della legge» relativa alla precedente legislazione del Regno Unito nel settore della sorveglianza, ossia la RIPA 2000, la Grande Sezione della Corte europea dei diritti dell'uomo ha espressamente riconosciuto la pertinenza dei codici di condotta del Regno Unito e ha accettato che le sue disposizioni possano essere prese in considerazione nel valutare la prevedibilità della normativa che consente la sorveglianza ([268]).

(180) Occorre poi osservare che le agenzie di sicurezza nazionale e alcune autorità di contrasto ([269]) dispongono di poteri mirati (intercettazione mirata ([270]), acquisizione mirata di dati relativi alle comunicazioni ([271]), conservazione mirata di dati relativi alle comunicazioni ([272]) e ingerenza mirata in apparecchiature ([273])), mentre soltanto i servizi di intelligence possono fare uso di tali poteri in maniera massiva (ossia intercettazione massiva ([274]), acquisizione massiva di dati relativi alle comunicazioni ([275]), ingerenza massiva in apparecchiature ([276]) e serie massive di dati personali ([277])).

(181) Nel decidere quale potere di indagine dovrebbe essere utilizzato, l'agenzia di intelligence deve rispettare gli «obblighi in relazione alla protezione della vita privata» di cui alla sezione 2, paragrafo 2, lettera a), della legge del 2016 sui poteri di indagine, che comprende una verifica della necessità e della proporzionalità. Più specificamente, ai sensi di tale disposizione, un'autorità pubblica che ha intenzione di utilizzare un potere di indagine deve valutare: i) se ciò che si vuole conseguire tramite il mandato, l'autorizzazione o l'avviso possa ragionevolmente essere conseguito con altri

([264]) Per quanto riguarda, ad esempio, l'ambito di applicazione di tali misure, ai sensi delle parti 3 e 4 (conservazione e acquisizione dei dati relativi alle comunicazioni) l'ambito di applicazione della misura è strettamente legato alla definizione di «operatori di telecomunicazioni» i cui dati degli utenti sono soggetti alla misura. Un altro esempio può essere fornito in relazione all'uso dei poteri «massivi». In questo caso, la portata di tali poteri è limitata alle «comunicazioni inviate o ricevute da persone fisiche al di fuori dell'isola britannica».

([265]) L'allegato 7 della legge del 2016 sui poteri di indagine stabilisce l'ambito di applicazione dei codici, la procedura da seguire per la loro emissione, le norme per il riesame e l'effetto dei codici.

([266]) I codici di pratica emessi nel contesto della legge del 2016 sui poteri di indagine sono disponibili al seguente indirizzo: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice.

([267]) Gli organi giurisdizionali fanno ricorso ai codici di pratica per valutare la liceità del comportamento delle autorità. Cfr. ad esempio: *Dias V Cleveland Police*, [2017] UKIPTrib15_586-CH, causa nel contesto della quale l'*Investigatory Powers Tribunal* ha fatto riferimento a passaggi specifici del codice di pratica sui dati relativi alle comunicazioni per comprendere la definizione del motivo di «prevenzione o accertamento di reati o prevenzione di disordini» utilizzato per richiedere l'acquisizione di dati relativi alle comunicazioni. Il codice è stato incluso nel ragionamento per trovare se tale motivo fosse stato utilizzato in modo scorretto. L'organo giurisdizionale ha quindi concluso che i comportamenti contestati erano illeciti. Gli organi giurisdizionali hanno altresì effettuato una valutazione in merito al livello di garanzie disponibili nei codici, cfr. ad esempio *Just for Law Kids v Secretary of State for the Home Department* [2019] EWHC 1772 (Admin) nel contesto della quale l'Alta Corte ha riscontrato che il diritto primario e derivato unitamente agli orientamenti interni fornivano garanzie sufficienti; oppure *R (National Council for Civil Liberties) v Secretary of State for the Home Department & Others* [2019] EWHC 2057 (Admin), causa nel contesto della quale l'organo giurisdizionale ha riscontrato che tanto la legge del 2016 sui poteri di indagine quanto il codice di pratica sull'ingerenza in apparecchiature contenevano disposizioni sufficienti per quanto riguarda la necessità di specificità dei mandati.

([268]) Nella causa *Big Brother Watch*, la Grande Sezione della Corte europea dei diritti dell'uomo ha osservato che «Il codice di pratica sull'intercettazione di comunicazioni è un documento pubblico approvato da entrambe le camere del parlamento, pubblicato dal governo sia online che in versione cartacea, di cui devono tenere conto sia le persone che esercitano funzioni di intercettazione sia gli organi giurisdizionali (v. punti 93-94). Di conseguenza, la Corte ha accettato che le disposizioni di detto codice possano essere prese in considerazione nel valutare la prevedibilità della RIPA (v. sentenza Kennedy, cit., punto 157). Pertanto la Corte accetta che la legislazione interna sia adeguatamente "accessibile"» (cfr.Corte europea dei diritti dell'uomo (grande sezione), *Big Brother Watch e altri contro Regno Unito*, ricorsi n. 58170/13, 62322/14 e 24960/15 del 25 maggio 2021, punto 366).

([269]) Per l'elenco delle autorità di contrasto pertinenti che possono applicare poteri di indagine mirati ai sensi della legge del 2016 sui poteri di indagine, cfr. nota (139).

([270]) Parte 2 della legge del 2016 sui poteri di indagine.

([271]) Parte 3 della legge del 2016 sui poteri di indagine.

([272]) Parte 4 della legge del 2016 sui poteri di indagine.

([273]) Parte 5 della legge del 2016 sui poteri di indagine.

([274]) Sezione 136 della legge del 2016 sui poteri di indagine.

([275]) Sezione 158 della legge del 2016 sui poteri di indagine.

([276]) Sezione 176 della legge del 2016 sui poteri di indagine.

([277]) Sezione 199 della legge del 2016 sui poteri di indagine.

mezzi meno intrusivi; ii) 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; iii) l'interesse pubblico per l'integrità e la sicurezza dei sistemi di telecomunicazione e dei servizi postali; e iv) qualsiasi altro aspetto di interesse pubblico nella protezione della vita privata ([278]).

(182) Le modalità di applicazione di tale criterio, così come il modo in cui la loro conformità è valutata nel contesto dell'autorizzazione dell'utilizzo di tali poteri da parte del segretario di Stato e dei commissari giudiziari indipendenti, sono ulteriormente specificate nei codici di prativa pertinenti. In particolare, l'utilizzo di uno qualsiasi di tali poteri di indagine deve sempre essere «proporzionato a quanto si vuole conseguire [il che] implica un bilanciamento tra la gravità dell'intrusione nella vita privata (e altre considerazioni di cui alla sezione 2, paragrafo 2) rispetto alla necessità dell'attività in termini investigativi, operativi o di capacità». Ciò significa in particolare che «dovrebbe offrire una prospettiva realistica di apportare il beneficio previsto e non dovrebbe essere sproporzionato o arbitrario» così come che «[n]essuna ingerenza nella vita privata dovrebbe essere considerata proporzionata se le informazioni che si cercano potrebbero ragionevolmente essere ottenute ricorrendo a mezzi meno intrusivi» ([279]). Più specificamente, il rispetto del principio di proporzionalità deve essere valutato tenendo conto dei seguenti criteri: «i) la portata dell'ingerenza proposta in relazione alla tutela della vita privata rispetto a ciò che si vuole conseguire; ii) le modalità e i motivi per i quali i metodi da adottare causeranno l'ingerenza minima possibile per la persona ed altri soggetti; iii) l'eventualità o meno che l'attività costituisca un uso adeguato dell'atto e un modo ragionevole, avendo considerato tutte le alternative ragionevoli, per conseguire ciò che si vuole conseguire; iv) quali altri metodi, a seconda dei casi, non sono stati attuati o sono stati impiegati ma sono valutati essere insufficienti per soddisfare gli obiettivi operativi in assenza del ricorso al potere di indagine proposto» ([280]).

(183) Nella pratica, come spiegato dalle autorità del Regno Unito, ciò assicura che un'agenzia di intelligence stabilisca innanzitutto l'obiettivo operativo (delimitando così la raccolta, ad esempio una finalità di antiterrorismo internazionale nel contesto di una specifica zona geografica) e, in secondo luogo, sulla base di tale obiettivo operativo, dovrà considerare quale opzione tecnica (ad esempio intercettazione, ingerenza in apparecchiature, acquisizione di dati relativi alle comunicazioni mirate o massive) sia la più proporzionata (ossia la meno invasiva per la vita privata, cfr. articolo 2, paragrafo 2, della legge sui poteri di indagine) rispetto all'obiettivo perseguito e possa quindi essere autorizzata ai sensi di una delle basi giuridiche disponibili.

(184) È opportuno sottolineare che tale affidamento sulle norme di necessità e proporzionalità è stato osservato e accolto con favore anche dal relatore speciale delle Nazioni Unite sul diritto alla tutela della vita privata, Joseph Cannataci, il quale, a proposito del sistema istituito dalla legge del 2016 sui poteri di indagine, ha dichiarato che «[l]e procedure in atto in seno tanto ai servizi di intelligence quanto alle autorità di contrasto sembrano richiedere sistematicamente la considerazione della necessità e della proporzionalità di una misura o di un'operazione di sorveglianza prima che venga raccomandata per l'autorizzazione, così come un suo riesame secondo le stesse basi» ([281]). Il relatore speciale ha osservato altresì che durante il suo incontro con i rappresentanti delle autorità di contrasto e con le agenzie di sicurezza nazionale «[ha] ricevuto un'espressione condivisa del fatto che il diritto alla tutela della vita privata deve essere una considerazione primaria per qualsiasi decisione concernente le misure di sorveglianza. Tutti hanno compreso e sono consapevoli della necessità e della proporzionalità come principi cardinali da prendere in considerazione».

([278]) Il codice di pratica sull'intercettazione di comunicazioni specifica che ulteriori aspetti della verifica di proporzionalità sono: «i) la portata dell'ingerenza proposta in relazione alla tutela della vita privata rispetto a ciò che si vuole conseguire; ii) le modalità e i motivi per i quali i metodi da adottare causeranno l'ingerenza minima possibile per la persona ed altri soggetti; iii) l'eventualità o meno che l'attività costituisca un uso adeguato dell'atto e un modo ragionevole, avendo considerato tutte le alternative ragionevoli, per conseguire ciò che si vuole conseguire; iv) quali altri metodi, a seconda dei casi, non sono stati attuati o sono stati impiegati ma sono valutati essere insufficienti per soddisfare gli obiettivi operativi in assenza del ricorso al potere di indagine proposto». Codice di pratica sull'intercettazione di comunicazioni, punto 4.16, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([279]) Cfr. codice di pratica sull'intercettazione di comunicazioni, punti 4.12 e 4.15, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([280]) Cfr. codice di pratica sull'intercettazione di comunicazioni, punto 4.16.

([281]) Dichiarazione di fine missione del relatore speciale sul diritto alla tutela della vita privata in occasione della conclusione della sua missione nel Regno Unito di Gran Bretagna e Irlanda del Nord, disponibile al seguente indirizzo: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, punto 1, lettera a).

(185) I criteri specifici per l'emissione dei diversi mandati, così come le limitazioni e le garanzie stabilite dalla legge del 2016 sui poteri di indagine per ciascun potere di indagine sono dettagliati nei considerando da 186 a 243.

3.3.1.1.1 Intercettazione ed esame mirati

(186) Esistono tre tipi di mandato per intercettazioni mirate: il mandato di intercettazione mirata ([282]), il mandato di esame mirato e il mandato di assistenza reciproca ([283]). Le condizioni per ottenere tali mandati e le relative garanzie sono stabilite nella parte 2, capo 1, della legge del 2016 sui poteri di indagine.

(187) Un mandato di intercettazione mirata autorizza l'intercettazione delle comunicazioni descritte nel mandato nel corso della loro trasmissione e l'ottenimento di altri dati pertinenti per tali comunicazioni ([284]), compresi i dati secondari ([285]). Un mandato di esame mirato autorizza una persona a svolgere la selezione per l'esame di contenuti intercettati ottenuti ai sensi di un mandato di intercettazione massiva ([286]).

(188) Qualsiasi mandato a norma della parte 2 della legge del 2016 sui poteri di indagine può essere emesso dal segretario di Stato ([287]) e approvato da un commissario giudiziario ([288]). In tutti i casi la durata di qualsiasi tipo di mandato mirato è limitata a 6 mesi ([289]) e si applicano norme specifiche in relazione alla sua modifica ([290]) e al suo rinnovo ([291]).

(189) Prima di emettere il mandato, il segretario di Stato deve effettuare una valutazione della necessità e della proporzionalità ([292]). Nello specifico, per un mandato di intercettazione mirata e un mandato di esame mirato, il segretario di Stato dovrebbe verificare se la misura è necessaria in considerazione di uno dei seguenti motivi: l'interesse della sicurezza nazionale; la prevenzione o l'accertamento di reati gravi; o gli interessi del benessere economico del Regno Unito ([293]) nella misura in cui tali interessi siano pertinenti anche per gli interessi di sicurezza nazionale ([294]). Al contrario, un mandato di assistenza reciproca (cfr. considerando 139) può essere emesso soltanto se il segretario di Stato ritiene che esistano circostanze equivalenti a quelle nelle quali egli avrebbe emesso un mandato al fine di prevenire e accertare reati gravi ([295]).

(190) Il segretario di Stato dovrebbe altresì valutare se la misura sia proporzionata a ciò che si vuole conseguire ([296]). La valutazione della proporzionalità delle misure richieste deve tener conto degli obblighi generali in relazione alla tutela della vita privata stabiliti dalla sezione 2, paragrafo 2, della legge del 2016 sui poteri di indagine, in particolare la necessità di valutare se ciò che si vuole conseguire tramite il mandato, l'autorizzazione o l'avviso

([282]) Sezione 15, paragrafo 2, della legge del 2016 sui poteri di indagine.
([283]) Sezione 15, paragrafo 4, della legge del 2016 sui poteri di indagine.
([284]) Sezione 15, paragrafo 2, della legge del 2016 sui poteri di indagine.
([285]) I dati secondari sono dati collegati o logicamente associati alla comunicazione intercettata, possono essere logicamente distinti dalla comunicazione e se fossero separati, non rivelerebbe nulla di ciò che potrebbe essere ragionevolmente considerato costituire il significato (se presente) della comunicazione. Alcuni esempi di dati secondari comprendono configurazioni del router o del firewall o il periodo di tempo durante il quale un router è stato attivo su una rete quando fanno parte, sono collegati o logicamente associati alla comunicazione intercettata. Per maggiori dettagli cfr. definizione di cui alla sezione 16 della legge del 2016 sui poteri di indagine e al codice di pratica sull'intercettazione di comunicazioni, punto 2.19, cfr. nota 278.
([286]) Tale esame viene effettuato come eccezione di cui alla sezione 152, paragrafo 4, della legge del 2016 sui poteri di indagine che prevede il divieto di cercare di identificare la comunicazione di persone fisiche che si trovano nelle isole britanniche. Cfr. considerando 229.
([287]) Il ministro scozzese autorizza il mandato quando si riferisce a una grave attività criminale in Scozia (cfr. sezioni 21 e 22 della legge del 2016 sui poteri di indagine), mentre un funzionario di alto livello può essere designato dal segretario di Stato affinché emetta un mandato di assistenza reciproca quando sembra che l'intercettazione riguarderà una persona o locali situati al di fuori del Regno Unito (sezione 40 della legge del 2016 sui poteri di indagine).
([288]) Sezioni 19 e 23 della legge del 2016 sui poteri di indagine.
([289]) Sezione 32 della legge del 2016 sui poteri di indagine.
([290]) Sezione 39 della legge del 2016 sui poteri di indagine. Persone prescritte ai sensi delle condizioni di cui alla legge del 2016 sui poteri di indagine possono apportare modifiche limitate ai mandati. La persona che ha emesso il mandato può annullarlo in qualsiasi momento ed è tenuta a farlo qualora il mandato non sia più necessario in ragione di alcuno dei motivi pertinenti o se la condotta autorizzata dal mandato non è più proporzionata a ciò che si vuole conseguire.
([291]) Sezione 33 della legge del 2016 sui poteri di indagine. La decisione di rinnovare il mandato deve essere approvata da un commissario giudiziario.
([292]) Sezione 19 della legge del 2016 sui poteri di indagine.
([293]) per quanto riguarda il concetto di «interesse del benessere economico del Regno Unito, nella misura in cui questo sia pertinente anche per la sicurezza nazionale», la Grande Sezione della Corte europea dei diritti dell'uomo, nella causa *Big Brother Watch and others v United Kingdom* (cfr. nota 268), punto 371, ha riconosciuto che tale concetto era sufficientemente incentrato sulla sicurezza nazionale. Sebbene la constatazione della Corte in questa causa riguardasse l'uso di tale concetto nella RIPA 2000, lo stesso concetto è utilizzato nella legge del 2016 sui poteri di indagine.
([294]) Sezione 20, paragrafo 2, della legge del 2016 sui poteri di indagine.
([295]) Sezione 20, paragrafo 3, della legge del 2016 sui poteri di indagine.
([296]) Sezione 19, paragrafo 1, lettera b), sezione 19, paragrafo 2, lettera b) e sezione 19, paragrafo 3, lettera b), della legge del 2016 sui poteri di indagine.

potrebbe essere ragionevolmente conseguito tramite altri mezzi meno intrusivi e se il livello di protezione da applicare in relazione a qualsiasi ottenimento di informazioni in virtù del mandato sia più elevato in ragione della sensibilità particolare di tali informazioni (cfr. considerando 181).

(191) A tal fine il segretario di Stato dovrà tenere conto di tutti gli aspetti della domanda specificati dall'autorità che presenta la richiesta, in particolare quelli relativi alle persone da sottoporre a intercettazione e la rilevanza della misura per l'indagine. Tali aspetti sono illustrati nel codice di pratica sull'intercettazione di comunicazioni e devono essere descritti con un certo livello di specificità ([297]). Inoltre la sezione 17 della legge del 2016 sui poteri di indagine richiede che qualsiasi mandato emesso ai sensi del suo capo 2 debba indicare il nome o descrivere la persona specifica o un gruppo specifico di persone, un'organizzazione o i locali da sottoporre a intercettazione («l'obiettivo»). In caso di mandato di intercettazione mirata o di mandato di esame mirato, un tale mandato può riguardare anche un gruppo di persone, più di una persona o un'organizzazione oppure più di una serie di locali (anche denominato «mandato tematico») ([298]). In tali casi il mandato dovrebbe descrivere la finalità o l'attività comune condivisa dal gruppo di persone o dall'operazione/dalle indagini e indicare il nome oppure descrivere il maggior numero di persone/organizzazioni o una serie di locali, laddove ciò sia ragionevolmente fattibile ([299]). Infine tutti i mandati emessi ai sensi della parte 2 della legge del 2016 sui poteri di indagine devono specificare gli indirizzi, i numeri, l'apparecchio, i fattori o la combinazione di fattori che devono essere utilizzati per individuare le comunicazioni ([300]). A tale riguardo il codice di pratica sull'intercettazione di comunicazioni specifica che, in caso di un mandato di intercettazione mirata e mandato di esame mirato «il mandato deve specificare (o descrivere) i fattori o la combinazione di fattori che devono essere utilizzati per individuare le comunicazioni. Se le comunicazioni devono essere individuate in riferimento, ad esempio, a un numero di telefono il numero deve essere specificato nella sua interezza. Tuttavia nei casi in cui è necessario utilizzare selettori di internet molto complessi o che variano continuamente per individuare le comunicazioni, occorre descrivere tali selettori per quanto possibile» ([301]).

(192) Una garanzia importante in questo contesto consiste nel fatto che la valutazione effettuata dal segretario di Stato per decidere se emettere un mandato deve essere approvata da un commissario giudiziario indipendente ([302]) che verificherà in particolare se la decisione di emettere il mandato sia conforme ai principi di necessità e proporzionalità ([303]) (per informazioni in merito allo status e al ruolo dei commissari giudiziari cfr. considerando da 251 a 256). La legge del 2016 sui poteri di indagine chiarisce anche che, quando si effettua tale controllo, il commissario giudiziario deve applicare i medesimi principi che sarebbero stati applicati da un organo giurisdizionale in relazione a una domanda di controllo giurisdizionale ([304]). Ciò assicura che in ciascun caso, e prima che avvenga l'accesso ai dati, il rispetto del principio di necessità e proporzionalità sia sistematicamente oggetto di controllo da parte di un organismo indipendente.

(193) La legge del 2016 sui poteri di indagine prevede poche eccezioni specifiche e limitate per effettuare intercettazioni mirate senza mandato. I casi limitati sono specificati nella legge ([305]) e, ad eccezione di quello basato sul «consenso» del mittente/destinatario, sono svolti da persone (enti pubblici o privati) diverse dalle agenzie di sicurezza nazionale. Inoltre, questo tipo di intercettazioni è effettuato a fini diversi dalla raccolta di «intelligence» ([306]) e per alcuni di essi è molto improbabile che la raccolta possa avvenire nel contesto di uno scenario di «trasferimento» (ad esempio in caso

([297]) Tra le informazioni richieste figurano dettagli in merito al contesto (descrizione delle persone/delle organizzazioni/della serie di locali, della comunicazione da intercettare) nonché un'indicazione del modo in cui l'ottenimento di tali informazioni apporterà benefici all'indagine, unitamente a una descrizione della condotta da autorizzare. Nel caso in cui non sia possibile descrivere le persone/l'organizzazione/i locali occorre includere una spiegazione del perché non è stato possibile o del motivo per cui è stata fornita soltanto una descrizione generale (codice di pratica sull'intercettazione di comunicazioni, punti 5.32 e 5.34, cfr. nota 278).

([298]) Sezione 17, paragrafo 2, della legge del 2016 sui poteri di indagine. Cfr. anche il codice di pratica sull'intercettazione di comunicazioni, punti 5.11 e seguenti, cfr. nota 278.

([299]) Sezione 31, paragrafi 4 e 5, della legge del 2016 sui poteri di indagine.

([300]) Sezione 31, paragrafo 8, della legge del 2016 sui poteri di indagine.

([301]) Codice di pratica sull'intercettazione di comunicazioni, punti 5.37 e 5.38, cfr. nota 278.

([302]) L'approvazione da parte di un commissario giudiziario non è richiesta quando il segretario di Stato ritiene che vi sia un'urgente necessità di emettere il mandato (articolo 19, paragrafo 1, della legge sui poteri di indagine). Tuttavia il commissario giudiziario deve essere informato in un breve periodo di tempo e deve decidere se approvare o meno il mandato. Se non lo fa, il mandato cessa di avere effetto (articoli 24 e 25 della legge del 2016 sui poteri di indagine).

([303]) Sezione 23, paragrafo 1, della legge del 2016 sui poteri di indagine.

([304]) Sezione 23, paragrafo 2, della legge del 2016 sui poteri di indagine.

([305]) Cfr. le sezioni da 44 a 51 della legge del 2016 sui poteri di indagine e la sezione 12 del codice di pratica sull'intercettazione di comunicazioni (cfr. nota278).

([306]) È il caso, ad esempio, quando un'intercettazione deve essere effettuata in carcere o in un ospedale psichiatrico (per controllare la condotta della persona incarcerata o di un paziente) o da parte di un operatore postale o di telecomunicazioni, ad esempio per individuare contenuti abusivi.

di intercettazione effettuata in un ospedale psichiatrico o in carcere). Considerata la natura dell'organo cui si applicano questi casi specifici (diverso dalle agenzie di sicurezza nazionale), si applicheranno tutte le garanzie previste dalla parte 2 della legge del 2018 sulla protezione dei dati e dal GDPR del Regno Unito, compresi la vigilanza dell'ICO e i meccanismi di ricorso disponibili. Inoltre, in aggiunta alle garanzie previste dalla legge del 2018 sulla protezione dei dati, in alcuni casi la legge del 2016 sui poteri di indagine prevede anche la vigilanza ex post dell'IPCO ([307]).

(194) Quando viene effettuata l'intercettazione, sono applicabili ulteriori limitazioni e garanzie alla luce dello status specifico della persona o delle persone le cui comunicazioni sono oggetto di intercettazione ([308]). Ad esempio, l'intercettazione di materiale coperto da segreto professionale è autorizzata soltanto in presenza di circostanze eccezionali e cogenti, la persona che emette il mandato deve considerare l'interesse pubblico alla riservatezza del materiale coperto da segreto professionale e il fatto che siano previsti requisiti specifici per la gestione, la conservazione e la comunicazione di tale materiale ([309]).

(195) Inoltre la legge del 2016 sui poteri di indagine prevede garanzie specifiche relative alla sicurezza, alla conservazione e alla comunicazione che il segretario di Stato dovrebbe tenere in considerazione prima di emettere un mandato mirato ([310]). In particolare la sezione 53, paragrafo 5, della legge del 2016 sui poteri di indagine richiede che ogni copia fatta di uno qualsiasi di tali materiali raccolti nel quadro del mandato sia conservata in maniera sicura e venga distrutta non appena non sussistano più i motivi pertinenti per la sua conservazione, mentre la sezione 53, paragrafo 2, della legge del 2016 sui poteri di indagine richiede che il numero di persone destinatarie della comunicazione, della messa a disposizione o della copia di qualsiasi materiale debba essere limitato al minimo necessario per le finalità di legge.

(196) Infine quando il materiale che è stato intercettato mediante un mandato di intercettazione mirata o un mandato di assistenza reciproca deve essere consegnato a un paese terzo («comunicazione all'estero»), la legge del 2016 sui poteri di indagine prevede che il segretario di Stato debba garantire che siano in atto dispositivi adeguati per assicurare che esistano garanzie analoghe in termini di sicurezza, conservazione e comunicazione in tale paese terzo ([311]). Inoltre, la sezione 109, paragrafo 2, della legge del 2018 sulla protezione dei dati prevede che i servizi di intelligence possano trasferire dati personali al di fuori del territorio del Regno Unito solo se il trasferimento costituisce una misura necessaria e proporzionata per l'esercizio delle funzioni statutarie del titolare del trattamento o per altre finalità previste dalla sezione 2, paragrafo 2, lettera a), della legge del 1989 sul servizio di sicurezza o dalla sezione 2, paragrafo 2, lettera a), e dalla sezione 4, paragrafo 2, lettera a), della legge del 1994 sui servizi di intelligence ([312]). È importante sottolineare che tali requisiti si applicano anche nei casi in cui è invocata l'esenzione per motivi di sicurezza nazionale a norma della sezione 110 della legge del 2018 sulla protezione dei dati, in quanto detta sezione non elenca la sezione 109 della medesima legge come una delle disposizioni che possono essere disapplicate se è richiesta un'esenzione rispetto a determinate disposizioni al fine di salvaguardare la sicurezza nazionale.

3.3.1.1.2 Acquisizione e conservazione mirate di dati relativi alle comunicazioni

(197) La legge del 2016 sui poteri di indagine consente al segretario di Stato di richiedere agli operatori di telecomunicazioni di conservare dati relativi alle comunicazioni per finalità di accesso mirato da parte di una serie di autorità pubbliche, comprese 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.

([307]) Cfr. a contrario la sezione 229, paragrafo 4, della legge sui poteri di indagine.

([308]) Le sezioni da 26 a 29 della legge del 2016 sui poteri di indagine introducono limitazioni all'ottenimento di mandati di intercettazione mirata ed esame mirato in relazione all'intercettazione di comunicazioni inviate da, o destinate a, una persona che è un membro del parlamento (qualsiasi parlamento del Regno Unito), l'intercettazione di materiale coperto da segreto professionale, l'intercettazione di comunicazioni che l'autorità che effettua l'intercettazione ritiene saranno comunicazioni contenenti materiale giornalistico riservato, nonché quando la finalità del mandato è quella di individuare o confermare una fonte di informazioni giornalistiche.

([309]) Sezione 26 della legge del 2016 sui poteri di indagine.

([310]) Sezione 19, paragrafo 1, della legge del 2016 sui poteri di indagine.

([311]) Sezione 54 della legge del 2016 sui poteri di indagine. Le garanzie relative alla comunicazione di materiale ad autorità straniere sono ulteriormente specificate nei codici di pratica: cfr., in particolare, punti 9.26 e segg. e 9.87 del codice di pratica sull'intercettazione di comunicazioni e punti 9.33 e segg. e 9.41 del codice di pratica sull'ingerenza in apparecchiature (cfr. nota 278).

([312]) Tali finalità sono: per il *Security Service*, la prevenzione o l'accertamento di reati gravi o qualsiasi procedimento penale (articolo 2, paragrafo 2, lettera a), della legge del 1989 sul servizio di sicurezza); per l'*Intelligence Service*, gli interessi di sicurezza nazionale, la prevenzione o l'accertamento di reati gravi o qualsiasi procedimento penale (articolo 2, paragrafo 2, lettera a), della legge del 1994 sui servizi di intelligence); mentre per il GCHQ, qualsiasi procedimento penale (articolo 4, paragrafo 2, lettera a), della legge del 1994 sui servizi di intelligence). Si vedano anche le note esplicative sulla legge del 2018 sui poteri di indagine disponibili al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(198) 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. A differenza dell'intercettazione, l'acquisizione e la conservazione di dati relativi alle comunicazioni non sono finalizzate all'ottenimento dei contenuti delle comunicazioni, bensì ad ottenere informazioni quali l'abbonato a un servizio telefonico o una fattura dettagliata. Potrebbe rientrare in tale contesto il tempo e la durata della comunicazione, il numero o l'indirizzo e-mail del mittente e del destinatario e, talvolta, l'ubicazione dei dispositivi dai quali è stata effettuata la telecomunicazione ([313]).

(199) Occorre osservare che la conservazione e l'acquisizione dei dati relativi alle comunicazioni non riguarderà di norma dati personali di interessati dell'UE trasferiti ai sensi della presente decisione verso il Regno Unito. L'obbligo di conservare o comunicare dati relativi alle comunicazioni ai sensi della parte 3 e della parte 4 della legge del 2016 sui poteri di indagine riguarda i dati raccolti da operatori di telecomunicazioni nel Regno Unito direttamente da utenti di un servizio di telecomunicazioni ([314]). In genere tale tipo di trattamento «rivolto al cliente» non comporta un trasferimento sulla base della presente decisione, ossia un trasferimento da un titolare del trattamento/responsabile del trattamento nell'UE verso un titolare del trattamento/responsabile del trattamento nel Regno Unito.

(200) Tuttavia, per ragioni di completezza, le condizioni e le garanzie che disciplinano tali regimi di acquisizione e di conservazione sono analizzate nei considerando che seguono.

(201) Come premessa, va osservato che la conservazione e l'acquisizione mirata dei dati relativi alle comunicazioni sono a disposizione sia delle agenzie di sicurezza nazionale che di talune autorità di contrasto ([315]). Le condizioni per richiedere la conservazione e/o l'acquisizione dei dati relativi alle comunicazioni possono variare a seconda del motivo per cui è richiesta la misura, ossia una finalità di sicurezza nazionale o di contrasto.

(202) In particolare, mentre il nuovo regime ha introdotto il requisito generale di un'autorizzazione ex ante da parte di un organismo indipendente che si applicherà in tutti i casi in cui i dati relativi alle comunicazioni sono conservati e/o acquisiti (a fini di contrasto o di sicurezza nazionale), a seguito della sentenza *Tele2/Watson* della Corte di giustizia dell'Unione europea ([316]) sono state introdotte garanzie specifiche quando la misura è richiesta a fini di contrasto. In particolare, quando la conservazione o l'acquisizione dei dati relativi alle comunicazioni è richiesta a fini di contrasto, l'autorizzazione ex ante deve sempre essere rilasciata dall'*Investigatory Power Commissioner*. Non è invece sempre così quando la misura è richiesta a fini di sicurezza nazionale, poiché, come descritto di seguito, in alcuni casi tale tipo di misure può essere autorizzato da una diversa «persona autorizzante». Inoltre, il nuovo regime ha innalzato ai «reati gravi» la soglia per la quale possono essere consentite la conservazione e l'acquisizione dei dati relativi alle comunicazioni ([317]).

([313]) I dati relativi alle comunicazioni sono definiti nella sezione 261, paragrafo 5, della legge del 2016 sui poteri di indagine. I dati relativi alle comunicazioni si dividono in «dati relativi ad eventi» (qualsiasi dato che individui o descriva un evento, con o senza riferimento alla sua ubicazione, nel contesto di o tramite un sistema di telecomunicazioni nel quale l'evento è costituito da una o più entità impegnate in un'attività specifica in un momento specifico) e in «dati relativi ad entità» (qualsiasi dato che: a) riguarda i) un'entità; ii) un'associazione tra un servizio di telecomunicazioni e un'entità; o iii) un'associazione tra qualsiasi parte di un sistema di telecomunicazioni e un'entità; b) è costituito da, o comprende, dati che individuano o descrivono l'entità (facendo riferimento o meno all'ubicazione dell'entità); e c) non sono dati relativi ad eventi).

([314]) Ciò deriva dalla definizione di dati relativi alle comunicazioni fornita dalla sezione 261, paragrafo 5, della legge del 2016 sui poteri di indagine, secondo la quale i dati relativi alle comunicazioni vengono detenuti od ottenuti da un operatore di telecomunicazioni e riguardano l'utente di un servizio di telecomunicazioni e concernono la fornitura di tale servizio oppure sono compresi in, inclusi come parte di, allegati a o logicamente associati a una comunicazione (cfr. anche codice di pratica sui dati relativi alle comunicazioni, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, punti da 2.22 a 2.33). Inoltre la definizione di operatore di telecomunicazioni fornita dalla sezione 261, paragrafo 10, della legge del 2016 sui poteri di indagine richiede che un operatore di telecomunicazioni sia una persona che offre o fornisce un servizio di telecomunicazioni a persone nel Regno Unito o che controlla o fornisce un sistema di telecomunicazioni (interamente o parzialmente) ubicato nel Regno Unito o controllato dal Regno Unito. Tali definizioni chiariscono che gli obblighi ai sensi della legge del 2016 sui poteri di indagine non possono essere imposti ad operatori di telecomunicazioni le cui apparecchiature non si trovano o non sono controllate dal Regno Unito e che non offrono o forniscono servizi a persone nel Regno Unito (cfr. anche il codice di pratica sui dati relativi alle comunicazioni, punto 2.1). Se abbonati dell'UE (ubicati nell'UE o nel Regno Unito) hanno fatto uso di servizi nel Regno Unito, tutte le comunicazioni in relazione alla fornitura di tale servizio verrebbero raccolte direttamente dal fornitore di servizi nel Regno Unito piuttosto che nel contesto di un trasferimento dall'Unione Europea.

([315]) Le autorità pertinenti sono elencate nell'allegato 4 della legge del 2016 sui poteri di indagine e comprendono le forze di polizia, i servizi di intelligence, alcuni ministeri e dipartimenti governativi, la *National Crime Agency*, l'*Her Majesty's Revenue and Customs*, la *Competition and Markets Authority*, l'*Information Commissioner*, servizi di ambulanza, antincendio e soccorso, nonché autorità che operano ad esempio nel settore della sanità e della sicurezza alimentare.

([316]) Sentenza della Corte del 21 dicembre 2016, Tele2/Watson, cause riunite C-203/15 e C-698/15, ECLI:EU:C:2016:970.

([317]) Cfr. la sezione 61.7, lettera b), per l'acquisizione dei dati relativi alle comunicazioni e la sezione 87.10A per la conservazione dei dati relativi alle comunicazioni.

i) *Autorizzazione all'ottenimento di dati relativi alle comunicazioni*

(203) Ai sensi della parte 3 della legge del 2016 sui poteri di indagine, le autorità pubbliche pertinenti sono autorizzate ad ottenere dati relativi alle comunicazioni da un operatore di telecomunicazioni o qualsiasi persona in grado di ottenere e comunicare tali dati. L'autorizzazione può non consentire l'intercettazione dei contenuti delle comunicazioni ([318]) e cessa di avere effetto dopo un termine di un mese ([319]) con possibilità di rinnovo previa un'autorizzazione aggiuntiva ([320]). L'acquisizione dei dati relativi alle comunicazioni richiede l'autorizzazione dell'*Investigatory Powers Commissioner* (IPC) ([321]) (per quanto riguarda lo status e i poteri dell'IPC cfr. considerando da 250 a 251). È sempre il caso quando l'acquisizione dei dati relativi alle comunicazioni è richiesta da un'autorità di contrasto competente. Tuttavia, conformemente alla sezione 61 della legge del 2016 sui poteri di indagine, qualora i dati vengano acquisiti per interessi di sicurezza nazionale o per il benessere economico del Regno Unito nella misura in cui sia pertinente per la sicurezza nazionale, oppure laddove un membro di un'agenzia di intelligence presenti una domanda ai sensi della sezione 61, paragrafo 7, lettera b) ([322]), l'acquisizione può essere in alternativa ([323]) autorizzata dall'*Investigatory Powers Commissioner* oppure da un funzionario di grado elevato designato ([324]). Il funzionario designato deve essere indipendente dall'indagine o dall'operazione in questione e deve disporre di conoscenze professionali in materia di principi e legislazione concernenti i diritti umani, in particolare per quanto riguarda la necessità e la proporzionalità ([325]). La decisione adottata dal funzionario designato sarà soggetta a vigilanza ex post da parte dell'*Investigatory Powers Commissioner* (cfr. considerando 254 per ulteriori dettagli sulle funzioni di vigilanza ex post dell'*Investigatory Powers Commissioner*).

(204) L'autorizzazione all'acquisizione di dati relativi alle comunicazioni si basa su una valutazione della necessità e della proporzionalità della misura. Più specificamente la necessità della misura è valutata alla luce dei motivi elencati nella legislazione ([326]). Considerando la natura mirata di tale misura, essa deve essere altresì necessaria per un'indagine o un'operazione specifica ([327]). Ulteriori requisiti sulla valutazione della necessità delle misure sono stabiliti nel codice di pratica sui dati relativi alle comunicazioni ([328]). Tale codice prevede in particolare che la domanda presentata dall'autorità richiedente debba individuare tre elementi minimi per giustificare la necessità di tale richiesta: i) l'evento oggetto di indagine, come un reato o l'ubicazione di una persona scomparsa vulnerabile; ii) la persona i cui dati sono oggetto di ricerca, come un indiziato, un testimone o una persona scomparsa e come sono collegati all'evento; e iii) i dati relativi alle comunicazioni oggetto di richiesta, come un numero di telefono o un indirizzo IP, e il modo in cui questi dati siano collegati alla persona e all'evento ([329]).

(205) Inoltre l'acquisizione di dati relativi alle comunicazioni deve essere proporzionata a ciò che si cerca di conseguire ([330]). Il codice di pratica sui dati relativi alle comunicazioni chiarisce che, nel condurre tale valutazione, la persona che rilascia l'autorizzazione dovrebbe effettuare un bilanciamento tra «la portata dell'ingerenza nei diritti e nelle libertà di una persona fisica rispetto a un beneficio specifico per l'indagine o l'operazione intrapresa da un'autorità pubblica competente nell'interesse pubblico» e che tenendo conto di tutte le considerazioni di un caso

([318]) Sezione 60A, paragrafo 6, della legge del 2016 sui poteri di indagine.

([319]) Tale termine è ridotto a tre giorni laddove l'autorizzazione venga concessa per ragioni di urgenza (articolo 65, paragrafo 3, lettera a), della legge del 2016 sui poteri di indagine).

([320]) Ai sensi della sezione 65 della legge del 2016 sui poteri di indagine, l'autorizzazione rinnovata durerà per un periodo di un mese dalla data di scadenza dell'autorizzazione in corso. La persona che ha concesso l'autorizzazione può annullarla in qualsiasi momento laddove ritenga che i requisiti non siano più soddisfatti.

([321]) Sezione 60A, paragrafo 1, della legge del 2016 sui poteri di indagine. L'*Office for Communications Data Authorisations* (OCDA) svolge tale funzione per conto dell'IPC (cfr. codici di pratica sui dati relativi alle comunicazioni, punto 5.6).

([322]) La domanda ai sensi della sezione 61, paragrafo 7, lettera b), della legge del 2016 sui poteri di indagine è effettuata per «una finalità di contrasto penale applicabile», il che, ai sensi della sezione 61, paragrafo 7, lettera a), della legge del 2016 sui poteri di indagine, significa: «laddove i dati relativi alle comunicazioni siano interamente o parzialmente dati relativi ad eventi, la finalità di prevenzione o accertamento di reati gravi; in qualsiasi altro caso, la finalità di prevenzione o accertamento di reati o la prevenzione di disordini».

([323]) Il codice di pratica sui dati relativi alle comunicazioni specifica che «laddove una domanda relativa alla sicurezza nazionale possa essere presentata ai sensi della sezione 60A o della sezione 61, la decisione in merito al percorso di autorizzazione più appropriato in ogni caso è una questione spettante alle singole autorità pubbliche. Le autorità pubbliche che desiderano sfruttare la possibilità del funzionario di grado elevato designato dovrebbero disporre di linee guida chiare nei casi in cui tale possibilità di autorizzazione sia adeguata» (codice di pratica sui dati relativi alle comunicazioni, punto 5.19, consultabile all'indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

([324]) L'articolo 70, paragrafo 3, della legge del 2016 sulla protezione dei dati fornisce la definizione di un «funzionario designato» che varia a seconda dell'autorità pubblica pertinente (come stabilito nell'allegato 4 della legge del 2016 sui poteri di indagine).

([325]) Ulteriori dettagli sull'indipendenza del funzionario di grado elevato designato sono forniti nel codice di pratica sui dati relativi alle comunicazioni (punti 4.12-4.17, cfr. nota 323).

([326]) I motivi sono: i) la sicurezza nazionale; ii) la prevenzione o l'accertamento di un reato o la prevenzione di disordini (in caso di «dati relativi a eventi» soltanto reato grave); iii) gli interessi di benessere economico del Regno Unito nella misura in cui tali interessi siano pertinenti anche per quelli di sicurezza nazionale; iv) gli interessi di sicurezza pubblica; v) al fine di prevenire la morte o lesioni o danni alla salute fisica o mentale di una persona oppure di attenuare qualsiasi pregiudizio o danno alla salute fisica o mentale di una persona; vi) la fornitura di assistenza a indagini in merito a presunti errori giudiziari; o vii) l'identificazione di una persona morta o di una persona incapace di identificarsi da sola in ragione di una determinata condizione (articolo 61, paragrafo 7, della legge del 2016 sui poteri di indagine).

([327]) Sezione 60A, paragrafo 1, lettera b), della legge del 2016 sui poteri di indagine.

([328]) Il codice di pratica sui dati relativi alle comunicazioni, punti 3.3 e seguenti, cfr. nota 323.

([329]) Il codice di pratica sui dati relativi alle comunicazioni, punto 3.13, cfr. nota 323.

([330]) Sezione 60, paragrafo 1, della legge del 2016 sui poteri di indagine.

particolare, «un'ingerenza nei diritti di una persona fisica può comunque non essere giustificata perché l'impatto negativo sui diritti di un'altra persona fisica o di un gruppo di persone fisiche è troppo grave». Inoltre, al fine di valutare specificamente la proporzionalità della misura, detto codice elenca una serie di elementi che dovrebbero essere inclusi nella domanda presentata dall'autorità richiedente ([331]). Occorre altresì prestare particolare attenzione al tipo di dati relativi alle comunicazioni (dati relativi ad «entità» o ad «eventi» ([332])) da acquisire e si deve dare preferenza all'uso di categorie di dati meno intrusive ([333]). Il codice di pratica sui dati relativi alle comunicazioni contiene altresì istruzioni specifiche per le autorizzazioni concernenti dati relativi alle comunicazioni di persone che svolgono professioni particolari (quali medici, avvocati, giornalisti, parlamentari o ministri del culto) ([334]) che sono soggette a garanzie supplementari ([335]).

ii) *Avviso che richiede la conservazione di dati relativi alle comunicazioni*

(206) La parte 4 della legge del 2016 sui poteri di indagine stabilisce le norme sulla conservazione di dati relativi alle comunicazioni e in particolare i criteri che consentono al segretario di Stato di rilasciare un avviso di conservazione ([336]). Le garanzie introdotte dalla legge sui poteri di indagine sono le stesse sia per i dati conservati per una finalità di conservazione sia per i dati conservati nell'interesse della sicurezza nazionale.

(207) L'emissione di tali avvisi di conservazione 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 necessario per finalità commerciali ([337]). 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 e descritta nei considerando da 203 a 205.

(208) L'esercizio del potere di richiedere la conservazione di determinati dati è soggetto a una serie di limitazioni e garanzie. Il segretario di Stato può rivolgere un avviso di conservazione a uno o più operatori ([338]) soltanto quando ritiene che il requisito della conservazione dei dati sia necessario per una delle finalità stabilite dalla legge ([339]) e sia proporzionato a ciò che si intende conseguire ([340]). Come chiarito dalla stessa legge del 2016 sui poteri di

([331]) Le informazioni da includere devono comprendere: i) una descrizione del beneficio apportato dall'ottenimento dei dati all'indagine o all'operazione il funzionamento; ii) una spiegazione della rilevanza dei periodi di tempo richiesti, indicando altresì in che modo tali periodi sono proporzionati all'evento oggetto di indagine; iii) una spiegazione di come il livello di intrusione sia giustificato prendendo in considerazione il beneficio che i dati conferiranno all'indagine (tale giustificazione dovrebbe comprendere la considerazione dell'eventualità di intraprendere indagini meno intrusive per raggiungere l'obiettivo); iv) una considerazione dei diritti (in particolare in termini di tutela della vita privata e, nei casi rilevanti, di libertà di espressione) della persona fisica e di un bilanciamento di tali diritti rispetto al beneficio per l'indagine; v) dettagli in merito a quale intrusione collaterale possa verificarsi e in che modo i periodi di tempo richiesti incidano sull'intrusione collaterale (codice di pratica sui dati relativi alle comunicazioni, punti da 3.22 a 3.26, cfr. nota 323).

([332]) Cfr. nota 313.

([333]) Quando si cerca di ottenere dati relativi alle comunicazioni più intrusivi (ossia i dati relativi agli eventi), detto codice specifica che è più appropriato acquisire innanzitutto i dati relativi alle entità o acquisire direttamente i dati relativi ad eventi in casi limitati di urgenza specifica (codice di pratica sui dati relativi alle comunicazioni, punti da 6.10 a 6.14, cfr. nota 323).

([334]) Codice di pratica sui dati relativi alle comunicazioni, punti da 8.8 a 8.44, cfr. nota 323.

([335]) Il codice di pratica specifica che «la persona che rilascia l'autorizzazione deve prestare particolare attenzione quando valuta tali domande, anche considerando altresì se potrebbero esserci conseguenze non intenzionali derivanti da tali domande e se l'interesse pubblico sia meglio servito dalla domanda» (codice di pratica sui dati relativi alle comunicazioni, punto 8.8). Inoltre occorre conservare registrazioni in merito a questo tipo di domande e all'ispezione che segue e tali domande dovrebbero essere contrassegnate per essere sottoposte all'attenzione dell'*Investigatory Powers Commissioner* (codice di pratica sui dati relativi alle comunicazioni, punto 8.10, cfr. nota 323).

([336]) Sezioni da 87 a 89 della legge del 2016 sui poteri di indagine.

([337]) Ai sensi della sezione 90 della legge del 2016 sui poteri di indagine, un operatore di telecomunicazioni al quale viene notificato un avviso di conservazione può chiedere un riesame da parte del segretario di Stato che lo ha emesso.

([338]) Ai sensi della sezione 87, paragrafo 2, lettera a) della legge del 2016 sui poteri di indagine, un avviso di conservazione può riguardare «un particolare operatore o qualsiasi descrizione di operatori».

([339]) Le finalità sono: i) gli interessi di sicurezza nazionale; ii) la finalità di contrasto penale applicabile (come definita dalla sezione 87.10A della legge del 2016 sui poteri di indagine); iii) gli interessi di benessere economico del Regno Unito nella misura in cui tali interessi siano pertinenti anche per quelli di sicurezza nazionale; iv) gli interessi di sicurezza pubblica; v) la finalità di prevenire la morte o lesioni o danni alla salute fisica o mentale di una persona oppure di attenuare qualsiasi pregiudizio o danno alla salute fisica o mentale di una persona; o vi) la fornitura di assistenza ad indagini in merito a presunti errori giudiziari (articolo 87 della legge sui poteri di indagine).

([340]) Sezione 87 della legge del 2016 sui poteri di indagine. Inoltre, conformemente al codice di pratica pertinente, al fine di valutare la proporzionalità dell'avviso di conservazione, si applicano i criteri di cui alla sezione 2, paragrafo 2, della legge del 2016 sui poteri di indagine, in particolare il requisito che prevede la valutazione dell'eventualità che ciò che si vuole conseguire possa essere ragionevolmente conseguito ricorrendo a mezzi meno intrusivi. Analogamente alla valutazione della proporzionalità in relazione all'acquisizione dei dati relativi alle comunicazioni, il codice di pratica sui dati relativi alle comunicazioni chiarisce che tale valutazione implica il «bilanciamento tra la portata dell'ingerenza nel diritto della persona fisica al rispetto della sua vita privata e un vantaggio specifico per l'indagine (codice di pratica sui dati relativi alle comunicazioni, punto 16.3, cfr. nota 323).

indagine ([341]), prima di emettere un avviso di conservazione, il segretario di Stato deve prendere in considerazione: i probabili benefici dell'avviso ([342]); una descrizione dei servizi di telecomunicazione; l'opportunità di limitare i dati da conservare con riferimento all'ubicazione o a descrizioni di persone alle quali sono forniti i servizi di telecomunicazione ([343]); il numero probabile di utenti (se noto) di qualsiasi servizio di telecomunicazioni ai quali l'avviso si riferisce ([344]); la fattibilità tecnica del rispetto dell'avviso; il costo probabile del rispetto dell'avviso e qualsiasi altro effetto dell'avviso sull'operatore di telecomunicazioni (o sulla descrizione degli operatori) a cui si riferisce ([345]). Come dettagliato ulteriormente nel capitolo 17 del codice di pratica sui dati relativi alle comunicazioni, tutti gli avvisi di conservazione devono specificare ciascun tipo di dati che deve essere conservato e in che modo tale tipo di dati soddisfa le verifiche necessarie per la conservazione.

(209) In tutti i casi (a fini sia di sicurezza nazionale che di contrasto) la decisione del segretario di Stato di emettere l'avviso di conservazione deve essere approvata da un commissario giudiziario indipendente, secondo la cosiddetta «procedura a doppia verifica», che deve verificare in particolare se l'avviso di conservazione dei dati relativi alle comunicazioni sia necessario e proporzionato per uno o più dei fini previsti dalla legge ([346]).

3.3.1.1.3 Ingerenza in apparecchiature

(210) L'ingerenza in apparecchiature è costituita da una serie di tecniche utilizzate per ottenere una varietà di dati da apparecchiature ([347]), che comprendono computer, tablet e smartphone, nonché cavi, fili e dispositivi di conservazione ([348]). L'ingerenza in apparecchiature consente di ottenere tanto il contenuto delle comunicazioni quanto i dati sulle apparecchiature ([349]).

(211) Conformemente alla sezione 13, paragrafo 1, della legge del 2016 sui poteri di indagine, l'utilizzo dell'ingerenza in apparecchiature da parte di un servizio di intelligence richiede un'autorizzazione mediante un mandato nel contesto della procedura «a doppia verifica» stabilita dalla legge del 2016 sui poteri di indagine, a condizione che vi sia «un collegamento con le isole britanniche» ([350]). Secondo le spiegazioni fornite dalle autorità del Regno Unito, in situazioni nelle quali i dati vengono trasferiti dall'Unione europea verso il Regno Unito nell'ambito di applicazione

([341]) Sezione 88 della legge del 2016 sui poteri di indagine.

([342]) I benefici possono essere esistenti o previsti e devono essere correlati alle finalità stabilite dalla legge per le quali i dati possono essere conservati (codice di pratica sui dati relativi alle comunicazioni, punto 17.17, cfr. nota 323).

([343]) Tali considerazioni comprenderanno una determinazione dell'eventualità che l'intera portata geografica dell'avviso di conservazione sia necessaria e proporzionata nonché se sia necessario e proporzionato comprendere o escludere qualsiasi descrizione particolare delle persone (codice di pratica sui dati relativi alle comunicazioni, punto 17.17, cfr. nota 323).

([344]) Ciò aiuterà il segretario di Stato a considerare il livello di intrusione rispetto ai clienti, ma anche i probabili vantaggi derivanti dai dati da conservare (codice di pratica sui dati relativi alle comunicazioni, punto 17.17, cfr. nota 323).

([345]) Sezione 88 della legge del 2016 sui poteri di indagine.

([346]) Sezione 89 della legge del 2016 sui poteri di indagine.

([347]) Ai sensi della sezione 135, paragrafo 1, e della sezione 198, paragrafo 1, della legge del 2016 sui poteri di indagine, il concetto di «apparecchiature» comprende le apparecchiature che producono emissioni elettromagnetiche, acustiche o altre emissioni così come qualsiasi dispositivo che possa essere utilizzato in relazione a tali apparecchiature.

([348]) Codice di pratica sull'ingerenza in apparecchiature, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf , punto 2.2.

([349]) I dati relativi alle apparecchiature sono definiti nella sezione 100 della legge del 2016 sui poteri di indagine come dati di sistema e dati che: a) sono compresi in, inclusi come parte di, allegati a o logicamente associati a una comunicazione (da parte del mittente o altrimenti) o da qualsiasi altra informazione; b) possono essere logicamente separati dal resto della comunicazione o dall'informazione; e c) laddove separati, non rivelerebbero nulla di ciò che potrebbe essere ragionevolmente considerato essere il significato (se presente) della comunicazione o dell'informazione.

([350]) Affinché il requisito del mandato sia obbligatorio, la sezione 13, paragrafo 1, della legge del 2016 sui poteri di indagine richiede inoltre che la condotta del servizio di intelligence costituisca uno o più reati ai sensi degli articoli da 1 a 3A della *Computer Misuse Act 1990* (legge del 1990 sull'uso improprio di computer), circostanza che si verificherebbe nella maggior parte dei casi (cfr. codice di pratica sull'ingerenza in apparecchiature, punti 3.32 e da 3.6 a 3.9). Ai sensi della sezione 13, paragrafo 2, della legge del 2016 sui poteri di indagine, si ha un «collegamento con le isole britanniche» se: a) una qualsiasi condotta avverrebbe nelle isole britanniche (indipendentemente dall'ubicazione dell'apparecchiatura con la quale verrebbe attuata, o potrebbe essere attuata, l'ingerenza); b) il servizio di intelligence ritiene che una qualsiasi apparecchiatura con la quale verrebbe attuata, o potrebbe essere attuata, l'ingerenza si troverebbe o potrebbe trovarsi nelle isole britanniche in un certo momento durante lo svolgimento dell'ingerenza; oppure c) l'ingerenza mira a ottenere: i) comunicazioni inviate da o a una persona che si trova o che il servizio di intelligence ritiene si trovi attualmente nelle isole britanniche; ii) informazioni private relative a una persona fisica che si trova o che il servizio di intelligence ritiene si trovi attualmente nelle isole britanniche; oppure iii) dati relativi ad apparecchiature che fanno parte di, o sono collegate a, comunicazioni o informazioni private di cui ai punti i) o ii).

della presente decisione, ci sarebbe sempre un «collegamento con le isole britanniche» e qualsiasi ingerenza in apparecchiature concernente tali dati sarebbe pertanto soggetta al requisito obbligatorio di disporre di un mandato di cui alla sezione 13, paragrafo 1, della legge del 2016 sui poteri di indagine ([351]).

(212) Le norme in materia di mandati di ingerenza mirata in apparecchiature sono stabilite nella parte 5 della legge del 2016 sui poteri di indagine. Analogamente a quanto avviene per l'intercettazione mirata, l'ingerenza mirata in apparecchiature deve riguardare un «obiettivo» specifico, che deve essere definito nel mandato ([352]). I dettagli in merito alle modalità di individuazione dell'«obiettivo» dipendono dalla questione e dal tipo di apparecchiature da sottoporre a ingerenza. In particolare la sezione 115, paragrafo 3, della legge sui poteri di indagine specifica gli elementi che dovrebbero essere inclusi nel mandato (ad esempio nome della persona o dell'organizzazione, descrizione della posizione), a seconda dell'esempio sull'eventualità che l'ingerenza riguardi un'apparecchiatura che appartiene a o è in possesso di una persona in particolare o un'organizzazione o di un gruppo di persone in particolare, si trova presso un'ubicazione specifica, ecc. ([353]). Le finalità per le quali è possibile emettere mandati di ingerenza mirata in apparecchiature dipendono dall'autorità pubblica che ne fa domanda ([354]).

(213) Analogamente a quanto avviene per l'intercettazione mirata, l'autorità emittente deve considerare se la misura è necessaria per il conseguimento di una finalità specifica e se è proporzionata a ciò che si intende conseguire ([355]). Inoltre dovrebbe considerare altresì se esistono garanzie in relazione alla sicurezza, alla conservazione e alla comunicazione, anche in relazione alla «comunicazione all'estero» ([356]) (cfr. considerando 196).

(214) Il mandato deve essere approvato da un commissario giudiziario, fatta eccezione per i casi di urgenza ([357]). In quest'ultimo caso occorre informare un commissario giudiziario che è stato emesso un mandato e che deve approvarlo entro tre giorni lavorativi. Nel caso in cui il commissario giudiziario si rifiuti di approvarlo, il mandato cessa di avere effetto e non può essere rinnovato ([358]). Inoltre, il commissario giudiziario ha il potere di esigere la cancellazione di tutti i dati ottenuti in virtù del mandato ([359]). Il fatto che un mandato sia stato emesso d'urgenza non incide sulla vigilanza ex post (cfr. considerando da 244 a 255) o sulla possibilità per le persone fisiche di avvalersi dei mezzi di ricorso (cfr. considerando da 260 a 270). Le persone fisiche possono presentare reclamo presso l'ICO o contestare qualsiasi presunto comportamento dinanzi l'*Investigatory Powers Tribunal* secondo le modalità abituali. In tutti i casi la verifica applicata dal commissario giudiziario nel decidere se approvare o meno un mandato è la verifica della necessità e della proporzionalità applicabile alle richieste di intercettazione mirata ([360]) (cfr. considerando 192).

([351]) Per ragioni di completezza occorre osservare che anche in situazioni nelle quali non vi è un «collegamento con le isole britanniche» e l'uso dell'ingerenza in apparecchiature non è quindi soggetto al requisito del mandato obbligatorio di cui alla sezione 13, paragrafo 1, della legge del 2016 sui poteri di indagine, un servizio di intelligence che prevede di impegnarsi in attività per le quali è in grado di ottenere un mandato di ingerenza massiva in apparecchiature dovrebbe ottenere tale mandato per una questione di politica (cfr. codice di pratica sull'ingerenza in apparecchiature, punto 3.24). Anche se un mandato per ingerenza in apparecchiature ai sensi della legge del 2016 sui poteri di indagine non è né richiesto né ottenuto ai sensi della legge come questione di politica, le azioni dei servizi di intelligence sono soggette a una serie di condizioni e limitazioni ai sensi della sezione 7 della legge del 1994 sui servizi di intelligence. Rientra in tale contesto in particolare il requisito di un'autorizzazione da parte del segretario di Stato, che deve essere convinto del fatto che qualsiasi azione non vada oltre ciò che è necessario per il corretto adempimento delle funzioni del servizio di intelligence.

([352]) L'articolo 115 della legge del 2016 sui poteri di indagine regolamenta il contenuto del mandato, specificando che deve includere il nome o la descrizione di persone, organizzazioni, posizione o gruppo di persone che costituiscono l'«obiettivo», una descrizione della natura dell'indagine e una descrizione delle attività per le quali viene utilizzata l'apparecchiatura. Deve inoltre descrivere il tipo di apparecchiatura e la condotta che la persona a favore della quale viene rilasciato il mandato è autorizzata ad adottare.

([353]) Cfr. anche il codice di pratica sull'ingerenza in apparecchiature, punto 5.7, cfr. nota 348.

([354]) Le agenzie di sicurezza nazionale possono richiedere un mandato di ingerenza in apparecchiature quando è necessario per finalità di sicurezza nazionali, per finalità di accertamento di reati gravi e/o nell'interesse del benessere economico del Regno Unito nella misura in cui tali interessi sono pertinenti anche per interessi di sicurezza nazionale (articoli 102 e 103 della legge del 2016 sui poteri di indagine). A seconda dell'agenzia, un mandato di ingerenza in apparecchiature può essere richiesto per una finalità di contrasto quando è necessario per accertare o prevenire un reato grave oppure per la finalità di prevenire la morte o qualsiasi infortunio o danni alla salute fisica o mentale di una persona oppure di attenuare qualsiasi infortunio o danno alla salute fisica o mentale di una persona (cfr. articolo 106 paragrafi 1 e 3, della legge del 2016 sui poteri di indagine).

([355]) Sezione 102, paragrafo 1, della legge del 2016 sui poteri di indagine.

([356]) Articoli da 129 a 131 della legge del 2016 sui poteri di indagine.

([357]) Sezione 109 della legge del 2016 sui poteri di indagine.

([358]) Sezione 109, paragrafo 4, della legge del 2016 sui poteri di indagine.

([359]) Sezione 110, paragrafo 3, lettera b), della legge del 2016 sui poteri di indagine. Ai sensi del codice di pratica sull'ingerenza in apparecchiature, punto 5.67, l'urgenza è determinata in base al criterio della ragionevole possibilità di chiedere l'autorizzazione del commissario giudiziario ad emettere il mandato entro il tempo a disposizione per soddisfare un'esigenza operativa o investigativa. I mandati d'urgenza dovrebbero rientrare in una o in entrambe le seguenti categorie: i) una minaccia imminente per la vita o danni gravi, ad esempio se una persona è stata rapita e si ritiene che la sua vita sia in pericolo imminente; o ii) un'opportunità investigativa o un'opportunità di raccolta di intelligence con un tempo limitato per agire — ad esempio, una spedizione di droga di classe A sta per entrare nel Regno Unito e le autorità di contrasto vogliono avere la copertura degli autori dei reati gravi al fine di effettuare arresti. Cfr. nota 348.

([360]) Sezione 108 della legge del 2016 sui poteri di indagine.

(215) Infine le garanzie specifiche applicabili all'intercettazione mirata si applicano anche all'ingerenza in apparecchiature per quanto concerne la durata, il rinnovo e la modifica del mandato nonché l'intercettazione di membri del parlamento, di materiale coperto da segreto professionale e di materiale giornalistico (cfr. ulteriori dettagli di cui al considerando 193).

3.3.1.1.4 Esercizio di poteri massivi

(216) I poteri massivi sono regolamentati nella parte 6 della legge del 2016 sui poteri di indagine. Inoltre i codici di pratica prevedono maggiori dettagli sull'uso di poteri massivi. Sebbene nel diritto del Regno Unito non vi sia alcuna definizione del termine «*bulk power*» (potere massivo), nel contesto della legge del 2016 sui poteri di indagine tale concetto è stato descritto come la raccolta e la conservazione di grandi quantitativi di dati acquisiti dal governo attraverso vari mezzi (ossia i poteri di intercettazione massiva, di acquisizione massiva, di ingerenza massiva in apparecchiature e di serie massive di dati personali), ai quali le autorità possono successivamente accedere. Tale descrizione è chiarita mediante confronto con ciò che non si intende per «*bulk power*»: non equivale alla cosiddetta «sorveglianza di massa» senza limitazioni o garanzie. Al contrario, come spiegato di seguito, integra le limitazioni e le garanzie progettate per assicurare che l'accesso ai dati non venga fornito in maniera indiscriminata o ingiustificata ([361]). In particolare è possibile esercitare i poteri massivi soltanto se si stabilisce un collegamento tra la misura tecnica che un'organizzazione di intelligence nazionale intende utilizzare e l'obiettivo operativo per il quale tale misura viene richiesta.

(217) Inoltre i poteri massivi sono disponibili soltanto alle agenzie di intelligence e sono sempre soggetti a un mandato rilasciato dal segretario di Stato e approvato da un commissario giudiziario. Nella scelta dei mezzi per raccogliere intelligence, occorre valutare se l'obiettivo in questione possa essere perseguito ricorrendo a «mezzi meno intrusivi» ([362]). Tale approccio deriva dal quadro della legislazione che si fonda sul principio di proporzionalità e dà quindi priorità alla raccolta mirata piuttosto che a quella massiva.

3.3.1.1.4.1 Intercettazione massiva e ingerenza massiva in apparecchiature

(218) Il regime per l'intercettazione massiva è definito nella parte 6, capo 1, della legge del 2016 sui poteri di indagine, mentre il capo 3 della medesima parte regolamenta l'ingerenza massiva in apparecchiature. Poiché tali regimi sono sostanzialmente uguali, le condizioni e le garanzie supplementari applicabili a tali mandati vengono analizzate congiuntamente.

i) *Condizioni e criteri per l'emissione del mandato*

(219) Il mandato di intercettazione massiva è limitato all'intercettazione di comunicazioni nel corso della loro trasmissione da o verso persone fisiche al di fuori delle isole britanniche ([363]), le cosiddette «comunicazioni relative all'estero» ([364]), e di altri dati pertinenti e alla successiva selezione per esame del materiale

([361]) Secondo la relazione dei poteri massivi presentata da Lord David Anderson, revisore indipendente della legislazione in materia di terrorismo prima dell'approvazione della legge del 2016 sui poteri di indagine, «*dovrebbe essere specificato che la raccolta e la conservazione di dati in massa non equivale alla cosiddetta 'sorveglianza di massa'. Qualsiasi ordinamento giuridico degno di tale nome integrerà limitazioni e garanzie progettate specificamente per assicurare che l'accesso ad archivi di dati sensibili [...] non venga concesso in maniera indiscriminata o ingiustificata. Tali limitazioni e garanzie esistono sicuramente nell'atto in questione*». Lord David Anderson, *Report of the bulk power review,* agosto 2016, punto 1.9 (sottolineatura aggiunta), disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF.

([362]) Sezione 2.2 della legge del 2016 sui poteri di indagine. Cfr. ad esempio il codice di pratica sull'acquisizione massiva di dati relativi alle comunicazioni, punto 4.11, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf.

([363]) Per «isole britanniche» si intendono il Regno Unito, le isole del Canale e l'Isola di Man; tali territori sono definiti nell'allegato 1 della *Interpretation Act 1978* (legge del 1978 sull'interpretazione), disponibile al seguente indirizzo: https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

([364]) Ai sensi della sezione 136 della legge del 2016 sui poteri di indagine, «comunicazioni relative all'estero» significa: i) comunicazioni inviate da persone fisiche che si trovano al di fuori delle isole britanniche; o ii) comunicazioni ricevute da persone fisiche che si trovano fuori delle isole britanniche. Tale regime, come confermato dalle autorità del Regno Unito, copre anche le comunicazioni tra due persone che si trovano entrambe al di fuori delle isole britanniche. La Grande Sezione della Corte europea dei diritti dell'uomo, nella causa *Big Brother Watch and others v United Kingdom* (cfr. nota 279), punto 376, ha riconosciuto, per quanto riguarda una limitazione analoga (relativa alle «comunicazioni esterne») delle comunicazioni che possono essere acquisite mediante intercettazione massiva ai sensi della RIPA 2000, che essa era sufficientemente circoscritta e prevedibile.

intercettato ([365]). Il mandato di ingerenza massiva in apparecchiature ([366]) autorizza il destinatario ad effettuare ingerenze in qualsiasi apparecchiatura al fine di ottenere comunicazioni relative all'estero (in qualsiasi loro aspetto: parlato, musica, suoni, immagini visive o dati di qualsiasi descrizione), dati relativi alle apparecchiature (dati che abilitano o facilitano il funzionamento di un servizio postale; di un sistema di telecomunicazioni; di un servizio di telecomunicazioni) o qualsiasi altra informazione ([367]).

(220) Il segretario di Stato può emettere un mandato massivo soltanto a fronte di una domanda presentata da un capo di un servizio di intelligence ([368]). Un mandato che autorizza un'intercettazione massiva o un'ingerenza massiva in apparecchiature deve essere rilasciato soltanto se necessario nell'interesse della sicurezza nazionale e per l'ulteriore finalità di prevenire o accertare reati gravi oppure nell'interesse del benessere economico del Regno Unito laddove pertinente per la sicurezza nazionale ([369]). L'articolo 142, paragrafo 7, della legge del 2016 sui poteri di indagine richiede inoltre che un mandato di intercettazione massiva sia specificato in modo più preciso rispetto a un semplice riferimento agli «interessi di sicurezza nazionale», al «benessere economico del Regno Unito» e alla «prevenzione e al contrasto di reati gravi»; deve infatti essere stabilito un collegamento tra la misura richiesta e una o più finalità operative che devono essere incluse nel mandato.

(221) La scelta della finalità operativa è il risultato di un processo a più livelli. L'articolo 142, paragrafo 4, prevede che le finalità operative indicate nel mandato debbano essere specificate in un elenco gestito dai capi dei servizi di intelligence ed essere considerate da questi ultimi finalità operative per le quali i contenuti intercettati o i dati secondari ottenuti in forza di mandati di intercettazione massiva possono essere selezionati per l'esame. L'elenco delle finalità operative deve essere approvato dal segretario di Stato. Il segretario di Stato può fornire tale approvazione soltanto se si è accertato del fatto che la finalità operativa è specificata con un maggiore livello di dettaglio rispetto ai motivi generali per l'autorizzazione del mandato (sicurezza nazionale o sicurezza nazionale e benessere economico o prevenzione di reati gravi) ([370]). Al termine di ciascun periodo di tre mesi pertinente, il segretario di Stato deve fornire una copia dell'elenco delle finalità operative all'*Intelligence and Security Committee* (ISC, commissione sui servizi di intelligence e sicurezza) del parlamento. Infine il primo ministro deve riesaminare l'elenco delle finalità operative almeno una volta l'anno ([371]). Come osservato dall'Alta Corte, «[n]on devono essere sminuite come garanzie insignificanti, dato che congiuntamente costituiscono un insieme complesso di modalità di responsabilizzazione, che coinvolge il parlamento e membri del governo di livello più elevato» ([372]).

(222) Tali finalità operative limitano altresì l'ambito di applicazione della selezione del materiale di intercettazione per la fase di esame. La selezione per l'esame del materiale raccolto ai sensi di un mandato massivo deve essere giustificata alla luce della o delle finalità operative. Come spiegato dalle autorità del Regno Unito, ciò significa che le modalità pratiche concernenti l'esame devono essere valutate dal segretario di Stato già nella fase di rilascio del mandato, fornendo dettagli sufficienti per il soddisfacimento degli obblighi stabiliti dalla legge ai sensi degli articoli 152 e 193 della legge del 2016 sui poteri di indagine ([373]). I dettagli forniti al segretario di Stato in relazione a tali modalità pratiche dovrebbero comprendere ad esempio, informazioni (se applicabili) sulle modalità di filtraggio che potrebbero variare nel corso della durata dell'efficacia di un mandato ([374]). Per ulteriori dettagli sul processo e sulle garanzie applicati alle fasi di filtraggio ed esame, cfr. considerando 229 .

([365]) Sezione 136, paragrafo 4, della legge del 2016 sui poteri di indagine. Secondo le spiegazioni ricevute dal governo del Regno Unito, si può ricorrere all'intercettazione massiva ad esempio per individuare minacce precedentemente sconosciute per la sicurezza nazionale del Regno Unito, filtrando e analizzando il materiale intercettato al fine di individuare le comunicazioni aventi valore di intelligence (Regno Unito, *Explanatory Framework section H: National security*, pag. 27 e 28, cfr. nota 29). Come spiegato dalle autorità del Regno Unito, tali strumenti possono essere utilizzati per stabilire legami tra soggetti di interesse noti nonché per cercare tracce di attività da parte di persone fisiche che potrebbero non essere ancora note ma che vengono rilevate nel corso di un'indagine nonché per individuare modelli di attività che possono indicare una minaccia per il Regno Unito.

([366]) Conformemente alla sezione 13, paragrafo 1, della legge del 2016 sui poteri di indagine, l'utilizzo dell'ingerenza in apparecchiature da parte di un servizio di intelligence richiede un'autorizzazione mediante un mandato ai sensi della legge del 2016 sui poteri di indagine, a condizione che vi sia «un collegamento con le isole britanniche» (cfr. considerando 211).

([367]) Sezione 176 della legge del 2016 sui poteri di indagine. Un mandato di ingerenza massiva in apparecchiature potrebbe non autorizzare una condotta che (se attuata senza un'autorità legittima) costituirebbe un'intercettazione illecita (fatta eccezione in relazione a una comunicazione conservata). Secondo il quadro esplicativo del Regno Unito, le informazioni ottenute potrebbero essere necessarie per l'identificazione di soggetti di interesse e di norma si tratterà di operazioni adeguate su larga scala (Regno Unito, *Explanatory Framework, section H: National security*, pag. 28, cfr. nota 29).

([368]) Sezione 138, paragrafo 1, e sezione 178, paragrafo 1, della legge del 2016 sui poteri di indagine.

([369]) Sezione 138, paragrafo 2, e sezione 178, paragrafo 2, della legge del 2016 sui poteri di indagine.

([370]) Secondo le spiegazioni fornite dalle autorità del Regno Unito una finalità operativa può ad esempio limitare l'ambito di applicazione della misura all'esistenza di una minaccia in una specifica zona geografica.

([371]) Sezione 142, paragrafi da 4 a 10, della legge del 2016 sui poteri di indagine.

([372]) *High Court of Justice, Liberty*, [2019] EWHC 2057 (Admin), punto 167.

([373]) Le sezioni da 152 a 193 della legge del 2016 sui poteri di indagine richiedono che: a) la selezione per l'esame venga effettuata soltanto per le finalità operative specificate nel mandato; b) la selezione per l'esame sia necessaria e proporzionata in tutte le circostanze; e c) la selezione per l'esame non violi il divieto di selezionare materiale e individui comunicazioni inviate da o destinate a persone fisiche che è noto si trovino nelle isole britanniche in quel momento.

([374]) Cfr. codice di pratica sull'intercettazione di comunicazioni, punto 6.6, cfr. nota 278.

(223) L'esercizio di un potere massivo può essere autorizzato soltanto se è proporzionato a ciò che si vuole conseguire ([375]). Come specificato nel codice di pratica sull'intercettazione, qualsiasi valutazione della proporzionalità implica un «raffronto per definire l'equilibrio tra la gravità dell'intrusione nella vita privata (e altre considerazioni di cui alla sezione 2, paragrafo 2) e la necessità dell'attività in termini investigativi, operativi o di capacità. La condotta autorizzata dovrebbe offrire una prospettiva realistica di apportare il beneficio previsto e non dovrebbe essere sproporzionata o arbitraria» ([376]). Come già menzionato, nella pratica ciò significa che la verifica della proporzionalità si basa su una verifica del bilanciamento tra ciò che si vuole conseguire («finalità operativa/e») e le opzioni tecniche disponibili (ad esempio intercettazione, ingerenza in apparecchiature, acquisizione di dati relativi alle comunicazioni mirate o massive), dando preferenza ai mezzi meno intrusivi (cfr. considerando 181 e 182). Laddove più di una misura sia adeguata per l'obiettivo, occorre preferire i mezzi meno intrusivi.

(224) Un'ulteriore garanzia in merito alla valutazione della proporzionalità della misura richiesta è assicurata dal fatto che il segretario di Stato deve ricevere le informazioni pertinenti necessarie per effettuare correttamente la sua valutazione. In particolare il codice di pratica sull'intercettazione e il codice di pratica sull'ingerenza in apparecchiature richiedono che la domanda presentata dall'autorità competente debba menzionare il contesto della domanda, la descrizione delle comunicazioni da intercettare e gli operatori di telecomunicazioni tenuti a fornire assistenza, la descrizione della condotta da autorizzare, le finalità operative e una spiegazione sul motivo per cui tale condotta è necessaria e proporzionata ([377]).

(225) Infine, e soprattutto, la decisione del segretario di Stato di emettere il mandato deve essere approvata da un commissario giudiziario indipendente che esamina la valutazione della necessità e della proporzionalità della misura proposta, utilizzando gli stessi principi che verrebbero utilizzati da un organo giurisdizionale nel contesto di una domanda di controllo giurisdizionale ([378]). Più specificatamente, il commissario giudiziario riesaminerà le conclusioni del segretario di Stato in merito all'eventualità o meno che il mandato sia necessario e che la condotta sia proporzionata alla luce dei principi di cui alla sezione 2, paragrafo 2, della legge del 2016 sui poteri di indagine (obblighi generali in relazione alla tutela della vita privata). Il commissario giudiziario esaminerà le conclusioni del segretario di Stato anche al fine di stabilire se ciascuna delle finalità operative specificate nel mandato costituisca o meno una finalità per la quale una selezione è, o potrebbe essere, necessaria. Se il commissario giudiziario si rifiuta di approvare la decisione di emettere un mandato, il segretario di Stato può: i) accettare la decisione e quindi non emettere il mandato; o ii) deferire la questione all'*Investigatory Powers Commissioner* affinché si pronunci in merito (fatto salvo il caso in cui sia quest'ultimo ad aver pronunciato la decisione originale) ([379]).

ii) *Garanzie supplementari*

(226) La legge del 2016 sui poteri di indagine ha introdotto ulteriori limiti alla durata, al rinnovo e alla modifica di un mandato massivo. Il mandato deve avere una durata massima di sei mesi e qualsiasi decisione di rinnovo o modifica (fatta eccezione per modifiche minori) del mandato deve essere approvata anche da un commissario giudiziario ([380]). Il codice di pratica sull'intercettazione e il codice di pratica sull'ingerenza in apparecchiature hanno specificato che una variazione delle finalità operative del mandato è considerata una modifica importante del mandato ([381]).

([375]) Sezione 138, paragrafo 1, lettere b) e c) e articolo 178, lettere b) e (c) della legge del 2016 sui poteri di indagine.

([376]) Codice di pratica sull'intercettazione di comunicazioni, punto 4.10, cfr. nota 278.

([377]) Codice di pratica sull'intercettazione di comunicazioni, punto 6.20, cfr. nota 278 e codice di pratica sull'ingerenza in apparecchiature, punto 6.13, cfr. nota 348.

([378]) Sezione 138, paragrafo 1, lettera g), e articolo 178, paragrafo 1, lettera f), della legge del 2016 sui poteri di indagine. L'autorizzazione preventiva da parte di un organismo indipendente è stata in particolare individuata dalla Corte europea dei diritti dell'uomo come un'importante garanzia contro gli abusi nel contesto di intercettazioni massive. Corte europea dei diritti dell'uomo (Grande Sezione), *Big Brother Watch and others v United Kingdom*, (cfr. nota 269), punti 351 e 352. È importante ricordare che tale sentenza riguardava il quadro giuridico precedente (RIPA 2000) che non conteneva alcune delle garanzie (compresa l'autorizzazione preventiva da parte di un commissario giudiziario indipendente) introdotte dalla legge del 2016 sui poteri di indagine.

([379]) Sezione 159, paragrafi 3 e 4, della legge del 2016 sui poteri di indagine.

([380]) Sezioni da 143 a 146 e da 184 a 188 della legge del 2016 sui poteri di indagine. In caso di modifica urgente, il segretario di Stato può effettuare la modifica senza approvazione, tuttavia deve notificarla al commissario giudiziario il quale deve quindi decidere se approvare o rifiutare la modifica (articolo 147 della legge del 2016 sui poteri di indagine). I mandati devono essere annullati laddove non siano più necessari o proporzionati o se l'esame di contenuti intercettati, metadati o altri dati ottenuti ai sensi del mandato non è più necessario per nessuna delle finalità operative specificate nel mandato (articoli 148 e 189 della legge del 2016 sui poteri di indagine).

([381]) Codice di pratica sull'intercettazione di comunicazioni, punti da 6.44 a 6.47, cfr. nota 278 e codice di pratica sull'ingerenza in apparecchiature, punto 6.48, cfr. nota 348.

(227) Analogamente a quanto previsto per l'intercettazione mirata, la parte 6 della legge del 2016 sui poteri di indagine prevede che il segretario di Stato debba assicurare che siano in atto dispositivi destinati a fornire garanzie in merito alla conservazione e alla comunicazione di materiali ottenuti ai sensi del mandato ([382]),così come per la comunicazione all'estero ([383]). In particolare la sezione 150, paragrafo 5 e la sezione 191, paragrafo 5, della legge del 2016 sui poteri di indagine richiedono che ogni copia fatta di uno qualsiasi di tali materiali raccolti nel quadro del mandato sia conservata in maniera sicura e venga distrutta non appena non sussistono più i motivi pertinenti per la sua conservazione; mentre la sezione 150, paragrafo 2, e la sezione 191, paragrafo 2, paragrafo 2, della legge del 2016 sui poteri di indagine richiedono che il numero di persone destinatarie della comunicazione, della messa a disposizione o della copia di qualsiasi materiale debba essere limitato al minimo necessario per le finalità di legge ([384]).

(228) Infine quando il materiale che è stato intercettato mediante un'intercettazione massiva o un'ingerenza massiva in apparecchiature deve essere consegnato a un paese terzo («comunicazioni all'estero»), la legge del 2016 sui poteri di indagine prevede che il segretario di Stato debba garantire che siano in atto dispositivi adeguati per assicurare che esistano garanzie analoghe in termini di sicurezza, conservazione e comunicazione in tale paese terzo ([385]). Inoltre, la sezione 109, della legge del 2018 sulla protezione dei dati prevede requisiti specifici per i trasferimenti internazionali di dati personali da parte dei servizi di intelligence verso paesi terzi o organizzazioni internazionali, e non consente che i dati siano trasferiti verso un paese o territorio al di fuori del Regno Unito o verso un'organizzazione internazionale, fatto salvo il caso in cui il trasferimento sia necessario e proporzionato per l'esercizio delle funzioni statutarie del titolare del trattamento o per altre finalità previste dalla sezione 2, paragrafo 2, lettera a), della legge del 1989 sul servizio di sicurezza o dalla sezione 2, paragrafo 2, lettera a), e dalla sezione 4, paragrafo 2, lettera a), della legge del 1994 sui servizi di intelligence ([386]). È importante sottolineare che tali requisiti si applicano anche nei casi in cui è invocata l'esenzione per motivi di sicurezza nazionale a norma della sezione 110 della legge del 2018 sulla protezione dei dati, in quanto detta sezione non elenca la sezione 109 della medesima legge come una delle disposizioni che possono essere disapplicate se è richiesta un'esenzione rispetto a determinate disposizioni al fine di salvaguardare la sicurezza nazionale.

(229) Una volta che il mandato è stato approvato e i dati sono stati raccolti in massa, i dati saranno soggetti a una selezione prima di essere esaminati. La fase di selezione ed esame è soggetta ad un'ulteriore verifica della proporzionalità effettuata dall'analista che, sulla base delle finalità operative incluse nel mandato (e di modalità di filtraggio eventualmente esistenti), definisce i criteri per la selezione. Come previsto dagli articoli 152 e 193 della legge sui poteri di indagine, al momento del rilascio del mandato, il segretario di Stato deve assicurare che siano in atto dispositivi destinati a garantire che la selezione del materiale sia effettuata soltanto per le finalità operative specificate e che sia necessaria e proporzionata in tutte le circostanze. A tale riguardo le autorità del Regno Unito hanno chiarito che il materiale intercettato in massa viene selezionato, innanzitutto, tramite un filtro automatizzato con l'obiettivo di scartare i dati che è improbabile siano di interesse per la sicurezza nazionale. I filtri variano di volta in volta (come cambiano i modelli, i tipi e i protocolli di traffico internet) e dipenderanno dalla tecnologia e dal contesto operativo. Dopo questa fase i dati possono essere selezionati per l'esame soltanto se pertinenti per le finalità operative specificate nel mandato ([387]). Le garanzie previste dalla legge del 2016 sui poteri di indagine per l'esame del materiale raccolto si applicano a qualsiasi tipo di dati (contenuto intercettato e dati secondari) ([388]). Gli articoli 152 e 193 della legge del 2016 sui poteri di indagine prevedono inoltre un divieto generale di selezionare per l'esame materiale riferibile a conversazioni inviate da o destinate a persone fisiche che si trovano nelle isole britanniche. Se desiderano esaminare tale materiale, le autorità devono presentare una richiesta di mandato di esame mirato ai sensi della parte 2 e della parte 4 della legge del 2016 sui poteri di indagine, rilasciato dal segretario di Stato e approvato da un commissario giudiziario ([389]). Se una persona seleziona deliberatamente il contenuto intercettato per l'esame in violazione dei requisiti stabiliti dalla legge ([390]) commette un reato ([391]).

([382]) Sezione 156 della legge del 2016 sui poteri di indagine.
([383]) Sezioni 150 e 191 della legge del 2016 sui poteri di indagine.
([384]) La Grande Sezione della Corte europea dei diritti dell'uomo, nella causa Big Brother Watch and others v United Kingdom (cfr. nota 268), ha confermato il sistema di garanzie supplementari per la conservazione, l'accesso e la comunicazione previsto dalla RIPA 2000, cfr. punti da 392 a 394 e da 402 a 405. Lo stesso sistema di garanzie è previsto dalla legge del 2016 sui poteri di indagine.
([385]) Sezioni 151 e 192 della legge del 2016 sui poteri di indagine.
([386]) Per maggiori informazioni su tali finalità si veda la nota 312.
([387]) A tale riguardo il codice sull'intercettazione di comunicazioni specifica che «tali sistemi di trattamento trattano i dati dai collegamenti e dai segnali di comunicazione che l'autorità che ha effettuato l'intercettazione ha scelto di intercettare. Un grado di filtraggio viene quindi applicato al traffico su tali collegamenti e segnali, progettato per selezionare i tipi di comunicazioni aventi un potenziale valore di intelligence, scartando allo stesso tempo quelli che è meno probabile abbiano un valore in termini di intelligence. Come conseguenza di tale filtraggio, che varierà in base ai sistemi di trattamento, una percentuale significativa delle comunicazioni su tali collegamenti e segnali verrà automaticamente scartata. In seguito potranno essere quindi effettuate ulteriori ricerche complesse per estrarre ulteriori comunicazioni che hanno la probabilità maggiore di presentare il valore di intelligence più elevato, che fa riferimento alle funzioni statutarie dell'agenzia. Tali comunicazioni possono quindi essere selezionate per l'esame per una o più finalità operative specificate nel mandato laddove siano soddisfatte le condizioni di necessità e proporzionalità. Soltanto i materiali che sono stati filtrati possono essere potenzialmente selezionati per l'esame da parte di persone autorizzate» (codice di pratica sull'intercettazione di comunicazioni, punto 6.6, cfr. nota 278).
([388]) Cfr. la sezione 152, paragrafo 1, lettere a) e b), della legge del 2016 sui poteri di indagine, in base alla quale l'esame di entrambi i tipi di dati (contenuto intercettato e dati secondari) deve essere effettuato solo per lo scopo specificato e deve essere necessario e proporzionato in ogni circostanza.
([389]) Questo tipo di mandato non è richiesto quando i dati relativi alle persone fisiche che si trovano nell'isola britannica sono «dati secondari» (cfr. sezione 152, paragrafo 1, lettera c), della legge del 2016 sui poteri di indagine).
([390]) Sezioni 152 e 193 della legge del 2016 sui poteri di indagine.
([391]) Sezioni 155 e 196 della legge del 2016 sui poteri di indagine.

(230) La valutazione effettuata dall'analista per la selezione del materiale è soggetta a una vigilanza ex post da parte dell'*Investigatory Powers Commissioner*, che valuta la conformità rispetto alle garanzie specifiche stabilite nella legge del 2016 sui poteri di indagine per la fase di esame ([392]) (cfr. anche il considerando 229). L'*Investigatory Powers Commissioner* deve mantenere sotto esame (anche mediante audit, ispezione e indagine) l'esercizio da parte delle autorità pubbliche dei poteri di indagine menzionati nella legge del 2016 sui poteri di indagine ([393]). A tale riguardo il codice di pratica sull'intercettazione e il codice di pratica sull'ingerenza in apparecchiature chiariscono che l'agenzia deve conservare registri ai fini dell'esame e di audit successivi, e che tali registri devono descrivere il motivo per cui l'accesso ai materiali da parte di persone autorizzate è necessario e proporzionato nonché le finalità operative applicabili ([394]). Nella sua relazione annuale del 2018, l'*Investigatory Powers Commissioner Office* (IPCO) ([395]) ha concluso che le giustificazioni registrate dagli analisti per l'esame di taluni materiali raccolti massivamente soddisfacevano il livello richiesto di proporzionalità, fornendo dettagli sufficienti circa le motivazioni delle loro «interrogazioni» in relazione alla finalità da conseguire ([396]). Nella relazione del 2019, l'IPCO, in relazione ai poteri massivi, ha espresso chiaramente la propria intenzione di continuare le ispezioni delle intercettazioni massive, compreso un esame dettagliato dei selettori e dei criteri di ricerca ([397]). Continuerà inoltre a esaminare attentamente, caso per caso, la scelta delle misure di sorveglianza (mirate o massive) sia durante l'esame delle domande di mandato nell'ambito della procedura a doppia verifica sia in occasione delle ispezioni ([398]). Questo ulteriore monitoraggio sarà preso in debita considerazione nel contesto del monitoraggio della presente decisione da parte della Commissione di cui ai considerando da 281 a 284.

3.3.1.1.4.2 Acquisizione massiva di dati relativi alle comunicazioni

(231) La parte 6, capo 2, della legge del 2016 sui poteri di indagine regolamenta i mandati per l'acquisizione massiva che autorizzano il destinatario a richiedere a un operatore di telecomunicazioni di comunicare od ottenere qualsiasi dato relativo alle comunicazioni in suo possesso. Tali mandati autorizzano altresì l'autorità richiedente a selezionare i dati per l'ulteriore fase di esame. Come la conservazione mirata e l'acquisizione mirata di dati relativi alle comunicazioni (cfr. considerando 199), anche l'acquisizione massiva di dati relativi alle comunicazioni non riguarda normalmente i dati personali degli interessati dell'UE trasferiti ai sensi della presente decisione verso il Regno Unito. L'obbligo di comunicare dati relativi alle comunicazioni ai sensi della parte 2, capo 6, della legge del 2016 sui poteri di indagine riguarda i dati raccolti da operatori di telecomunicazioni nel Regno Unito direttamente da utenti di un servizio di telecomunicazioni ([399]). In genere tale tipo di trattamento «rivolto al cliente» non comporta un trasferimento sulla base della presente decisione, ossia un trasferimento da un titolare del trattamento/responsabile del trattamento nell'UE verso un titolare del trattamento/responsabile del trattamento nel Regno Unito.

(232) Tuttavia, per ragioni di completezza, le condizioni e le garanzie che disciplinano l'acquisizione di dati massivi relativi alle comunicazioni sono descritte in appresso.

([392]) Sezioni 152 e 193 della legge del 2016 sui poteri di indagine.

([393]) Sezione 229 della legge del 2016 sui poteri di indagine.

([394]) Codice di pratica sull'intercettazione di comunicazioni, punto 6.74, cfr. nota 278 e codice di pratica sull'ingerenza in apparecchiature, punto 6.78, cfr. nota 348.

([395]) L'IPCO è stato istituito ai sensi della sezione 238 della legge del 2016 sui poteri di indagine per fornire all'IPC il personale, i locali, le apparecchiature necessari, così come altri servizi e strutture necessari per lo svolgimento delle sue funzioni (cfr. considerando 251).

([396]) La relazione annuale dell'IPCO del 2018 ha specificato che le giustificazioni registrate dagli analisti del GCHQ «soddisfacevano il livello richiesto e gli analisti spiegavano con sufficiente dettaglio la proporzionalità delle loro interrogazioni su dati massivi». Relazione annuale del 2018 dell'*Investigatory Powers Commissioner*, punto 6.22, cfr. nota 464.

([397]) Relazione annuale del 2019 dell'*Investigatory Powers Commissioner*, punto 7.6, cfr. nota 463.

([398]) Relazione annuale del 2019 dell'*Investigatory Powers Commissioner*, punto 10.22, cfr. nota 463.

([399]) Ciò deriva dalla definizione di dati relativi alle comunicazioni fornita dalla sezione 261, paragrafo 5, della legge del 2016 sui poteri di indagine, secondo la quale i dati relativi alle comunicazioni vengono detenuti od ottenuti da un operatore di telecomunicazioni e riguardano l'utente di un servizio di telecomunicazioni e concernono la fornitura di tale servizio oppure sono compresi in, inclusi come parte di, allegati a o logicamente associati a una comunicazione (cfr. anche codice di pratica sull'acquisizione massiva di dati relativi alle comunicazioni, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf punti da 2.15 a 2.22). Inoltre la definizione di operatore di telecomunicazioni fornita dalla sezione 261, paragrafo 10, della legge del 2016 sui poteri di indagine richiede che un operatore di telecomunicazioni sia una persona che offre o fornisce un servizio di telecomunicazioni a persone nel Regno Unito o che controlla o fornisce un sistema di telecomunicazioni (interamente o parzialmente) ubicato nel Regno Unito o controllato dal Regno Unito. Tali definizioni chiariscono che gli obblighi ai sensi della legge del 2016 sui poteri di indagine non possono essere imposti ad operatori di telecomunicazioni le cui apparecchiature non si trovano o non sono controllate dal Regno Unito e che non offrono o forniscono servizi a persone nel Regno Unito (cfr. anche il codice di pratica sull'acquisizione massiva di dati relativi alle comunicazioni, punto 2.2). Se abbonati dell'UE (ubicati nell'UE o nel Regno Unito) hanno fatto uso di servizi nel Regno Unito, tutte le comunicazioni in relazione alla fornitura di tale servizio verrebbero raccolte direttamente dal fornitore di servizi nel Regno Unito piuttosto che nel contesto di un trasferimento dall'Unione Europea.

(233) La legge del 2016 sui poteri di indagine sostituisce la legislazione relativa all'acquisizione di dati massivi relativi alle comunicazioni che è stata oggetto della sentenza della Corte di giustizia dell'Unione europea nella causa *Privacy International*. La legislazione in questione in tale causa è stata abrogata e il nuovo regime prevede le condizioni e le garanzie specifiche in base alle quali tale misura può essere autorizzata.

(234) In particolare, a differenza di quanto accadeva ai sensi del regime precedente nel contesto del quale il segretario di Stato aveva piena discrezionalità in merito all'autorizzazione della misura ([400]), la legge del 2016 sui poteri di indagine impone al segretario di Stato di emettere un mandato soltanto se la misura è necessaria e proporzionata. Ciò significa nella pratica che dovrebbe esserci un nesso tra l'accesso ai dati e la finalità perseguita ([401]). Più specificamente il segretario di Stato dovrà valutare l'esistenza di un collegamento tra la misura richiesta e una o più «finalità operative» indicate nel mandato (cfr. considerando 219). In relazione alla valutazione della proporzionalità, il codice di pratica rilevante specifica che «il segretario di Stato deve tenere conto dell'eventualità o meno che ciò che si vuole conseguire tramite il mandato possa ragionevolmente essere conseguito tramite altri mezzi meno intrusivi (sezione 2, paragrafo 2, lettera a), della legge); ad esempio ottenendo le informazioni richieste attraverso un potere meno intrusivo come l'acquisizione mirata di dati relativi alle comunicazioni» ([402]).

(235) Per effettuare tale valutazione il segretario di Stato si baserà sulle informazioni che i capi dei servizi di intelligence ([403]) sono tenuti a presentare nella loro domanda, come le motivazioni per cui la misura è considerata necessaria per uno dei motivi statutari così come le motivazioni per cui ciò che si vuole conseguire non può essere ragionevolmente conseguito tramite altri mezzi meno intrusivi ([404]). Inoltre le finalità operative limitano l'ambito di applicazione per il quale i dati ottenuti ai sensi del mandato possono essere selezionati per l'esame ([405]). Come specificato nel codice di pratica pertinente, le finalità operative devono descrivere un requisito chiaro e contenere un dettaglio sufficiente a convincere il segretario di Stato del fatto che i dati acquisiti possono essere selezionati soltanto per l'esame per motivi specifici ([406]). In effetti, prima di autorizzare il mandato, il segretario di Stato dovrà assicurarsi che siano in atto dispositivi specifici destinati a garantire che soltanto il materiale ritenuto necessario per l'esame per una finalità operativa e una finalità statutaria sia selezionato per l'esame e che tale materiale sia proporzionato e necessario in tutte le circostanze. Questo specifico requisito, rispecchiato dagli articoli 158 e 172 ([407]) della legge del 2016 sui poteri di indagine, relativo alla valutazione preventiva della necessità e della proporzionalità dei criteri utilizzati ai fini della selezione rappresenta un'ulteriore importante novità del regime introdotto da tale legge rispetto al regime precedente.

(236) La legge del 2016 sui poteri di indagine ha inoltre introdotto l'obbligo per il segretario di Stato di assicurarsi, prima dell'emissione del mandato per l'acquisizione massiva di dati relativi alle comunicazioni, che siano in atto limitazioni specifiche concernenti la sicurezza, la conservazione e la comunicazione dei dati personali raccolti ([408]). In caso di comunicazione all'estero, le garanzie, di cui al considerando 227, per l'intercettazione massiva e l'ingerenza massiva in apparecchiature si applicano anche in questo contesto ([409]). Ulteriori limitazioni sono fissate nella legislazione in relazione alla durata ([410]), al rinnovo ([411]) e alla modifica dei mandati massivi ([412]).

(237) È importante sottolineare che, come per gli altri poteri massivi, prima di emettere il mandato il segretario di Stato necessita dell'approvazione da parte di un commissario giudiziario ([413]). Questa è una caratteristica fondamentale del regime messo in atto dalla legge del 2016 sui poteri di indagine.

([400]) L'articolo 94, paragrafo 1, della *Telecommunication Act 1984* (legge del 1984 sulle telecomunicazioni) prevedeva che il segretario di Stato poteva emettere «istruzioni di carattere generale che il segretario di Stato riteneva essere necessarie od opportune nell'interesse della sicurezza nazionale [...]» (cfr. nota 451).

([401]) Cfr. *Privacy International*, punto 78.

([402]) Cfr. codice di pratica sull'acquisizione massiva di dati relativi alle comunicazioni, punto 4.11 (cfr. nota 399).

([403]) Un mandato di acquisizione massiva può essere richiesto soltanto dai capi dei servizi di intelligence, ossia: i) il direttore generale del *Security Service*; ii) il capo del *Secret Intelligence Service*; o iii) il direttore del GCHQ (cfr. articoli 158 e 263 della legge del 2016 sui poteri di indagine).

([404]) Codice di pratica sull'acquisizione massiva di dati relativi alle comunicazioni, punto 4.5 (cfr. nota 399).

([405]) Ai sensi della sezione 161 della legge del 2016 sui poteri di indagine, le finalità operative specificate nel mandato devono essere quelle specificate in un elenco gestito dai capi dei servizi di intelligence («l'elenco delle finalità operative»), come finalità che essi considerano essere finalità operative per le quali i dati relativi alle comunicazioni ottenuti ai sensi di mandati di acquisizione massiva possono essere selezionati per l'esame.

([406]) Codice di pratica sull'acquisizione massiva di dati relativi alle comunicazioni, punto 6.6 (cfr. nota 399).

([407]) L'articolo 172 della legge del 2016 sui poteri di indagine impone che siano messe in atto garanzie specifiche per la fase di filtraggio e selezione per l'esame di dati relativi alle comunicazioni acquisiti in maniera massiva. Inoltre un esame deliberato in violazione di tali garanzie costituisce altresì un reato (cfr. articolo 173 della legge del 2016 sui poteri di indagine).

([408]) Sezione 171 della legge del 2016 sui poteri di indagine.

([409]) Sezione 171, paragrafo 9, della legge del 2016 sui poteri di indagine.

([410]) Sezione 162 della legge del 2016 sui poteri di indagine.

([411]) Sezione 163 della legge del 2016 sui poteri di indagine.

([412]) Sezioni da 164 a 166 della legge del 2016 sui poteri di indagine.

([413]) Sezione 159 della legge del 2016 sui poteri di indagine.

(238) L'*Investigatory Powers Commissioner* svolge un'attività di vigilanza ex post sulla procedura di esame rispetto ai materiali (dati relativi alle comunicazioni) acquisiti in maniera massiva (cfr. considerando 254). A tale riguardo, la legge del 2016 sui poteri di indagine ha introdotto il requisito che impone all'analista del servizio di intelligence di registrare, prima di selezionare i dati per l'esame, la motivazione per la quale l'esame proposto è necessario e proporzionato per una finalità operativa specificata ([414]). Nella relazione annuale del 2019 dell'IPCO, in relazione alla pratica attuata dal GCHQ e dall'MI5 è stato constatato che «il ruolo critico dei dati massivi relativi alle comunicazioni per la serie di attività svolte presso il GCHQ è risultato essere ben articolato nella casistica oggetto di ispezione. L'ispezione ha preso in considerazione la natura dei dati richiesti e i requisiti di intelligence dichiarati, e gli ispettori hanno potuto accertare che la documentazione dimostrava che il loro approccio era necessario e proporzionato» ([415]). Le giustificazioni registrate dall'MI5 erano di buon livello e soddisfacevano i principi di necessità e proporzionalità« ([416]).

3.3.1.1.4.3 Conservazione ed esame delle serie massive di dati personali

(239) I mandati per serie massive di dati personali (BPD, *Bulk Personal Dataset*) ([417]) autorizzano le agenzie di intelligence a conservare ed esaminare serie di dati che contengono dati personali relativi diverse persone fisiche. Secondo le spiegazioni fornite dalle autorità del Regno Unito, l'analisi di tali serie di dati può essere »l'unico modo per l'UKIC per procedere con le indagini ed individuare terroristi a partire da indizi di intelligence molto limitati oppure quando le loro comunicazioni sono state deliberatamente occultate« ([418]). Esistono due tipi di mandati: i »*class BPD warrants*« ([419]) (mandati BPD di classe) che riguardano una determinata categoria di serie di dati, ossia serie di dati analoghi in termini di contenuto e utilizzo proposto e che sollevano considerazioni analoghe ad esempio in termini di grado di intrusione e sensibilità e di proporzionalità dell'utilizzo dei dati; di conseguenza consentono al segretario di Stato di valutare in un'unica volta la necessità e la proporzionalità dell'acquisizione di tutti i dati rientranti nella classe pertinente. Un mandato BPD di classe può riguardare ad esempio le serie di dati relative ai viaggi concernenti percorsi analoghi ([420]). Gli «*specific BPD warrants*» ([421]) (mandati BPD specifici) riguardano invece una serie di dati specifica, come una serie di dati relativa a un tipo nuovo o insolito di informazioni che non rientrano nell'ambito di applicazione di un mandato BPD di classe esistente o una serie di dati che riguarda tipi specifici di dati personali ([422]) e quindi richiede garanzie supplementari ([423]). Le disposizioni della legge del 2016 sui poteri di indagine relative alle serie massive di dati personali consentono l'esame e la conservazione di tali serie di dati soltanto se è necessario e proporzionato farlo ([424]) e comunque in linea con gli obblighi generali relativi alla tutela della vita privata ([425]).

(240) Il potere di emettere un mandato BPD è soggetto alla procedura »a doppia verifica«: la valutazione della necessità e della proporzionalità della misura viene effettuata innanzitutto dal segretario di Stato e successivamente dal commissario giudiziario ([426]). Il segretario di Stato è tenuto a considerare la natura e l'ambito di applicazione del mandato richiesto, la categoria di dati interessata e il numero di singole serie massive di dati personali che potrebbero rientrare nel tipo specifico di mandato ([427]). Inoltre, come specificato nel codice di pratica sulla conservazione e sull'utilizzo di serie massive di dati personali da parte dei servizi di intelligence, occorre conservare registri dettagliati che sono altresì soggetti ad audit da parte dell'*Investigatory Powers Commissioner* ([428]). La conservazione e l'esame delle serie massive di dati personali al di fuori dei limiti sanciti dalla legge del 2016 sui poteri di indagine è un reato ([429]).

([414]) Relazione annuale del 2019 dell'IPCO, punto 8.6, cfr. nota 463.
([415]) Relazione annuale del 2019 dell'IPCO, punto 10.4, cfr. nota 463.
([416]) Relazione annuale del 2019 dell'IPCO, punto 8.37, cfr. nota 463.
([417]) Sezione 200 della legge del 2016 sui poteri di indagine.
([418]) Regno Unito, *Explanatory Framework for Adequacy Discussions, section H: National Security*, pag. 34, cfr. nota 29.
([419]) Sezione 204 della legge del 2016 sui poteri di indagine.
([420]) Codice di pratica sulla conservazione e sull'utilizzo di serie massive di dati personali da parte dei servizi di intelligence, punto 4.7, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf.
([421]) Sezione 205 della legge del 2016 sui poteri di indagine.
([422]) Come ad esempio dati personali sensibili, cfr. articolo 202 della legge del 2016 sui poteri di indagine e il codice di pratica sulla conservazione e sull'utilizzo di serie massive di dati personali da parte dei servizi di intelligence, punti 4.21 e 4.12, cfr. nota 469.
([423]) Una domanda per un mandato BPD specifico deve essere considerata singolarmente dal segretario di Stato, ossia in relaziona a una serie di dati specifica. Il servizio di intelligence è tenuto in virtù della sezione 205 della legge sui poteri di indagine a includere nella sua domanda di mandato BPD specifico una spiegazione dettagliata della natura e dell'estensione del materiale in questione così come un elenco delle «finalità operative» per le quali il servizio di intelligence pertinente intende esaminare la serie massiva di dati personali (laddove il servizio di intelligence intenda ottenere un mandato per la conservazione e l'esame, piuttosto che soltanto per la conservazione). Quando emette un mandato BPD di classe, il segretario di Stato considera invece l'intera categoria di serie di dati contemporaneamente.
([424]) Sezione 204 e sezione 205 della legge del 2016 sui poteri di indagine.
([425]) Sezione 2 della legge del 2016 sui poteri di indagine.
([426]) Sezioni 204 e 205 della legge del 2016 sui poteri di indagine.
([427]) Codice di pratica sulla conservazione e sull'utilizzo di serie massive di dati personali da parte dei servizi di intelligence, punto 5.2, cfr. nota 420.
([428]) Codice di pratica sulla conservazione e sull'utilizzo di serie massive di dati personali da parte dei servizi di intelligence, punti da 8.1 a 8.15, cfr. nota 420.
([429]) Regno Unito, *Explanatory Framework for Adequacy Discussions, section H: National Security*, pag. 34, cfr. nota 29.

3.3.2 *Ulteriore utilizzo delle informazioni raccolte*

(241) I dati personali trattati ai sensi della parte 4 della legge del 2018 sulla protezione dei dati non devono essere trattati in maniera incompatibile con la finalità per la quale sono stati raccolti ([430]). La legge del 2018 sulla protezione dei dati prevede che il titolare del trattamento possa trattare i dati per un'altra finalità, diversa da quella per la quale i dati sono stati raccolti, quando quest'altra finalità è compatibile con quella originale e a condizione che il titolare del trattamento sia autorizzato dalla legge a trattare tali dati e che il trattamento sia necessario e proporzionato ([431]). Inoltre la legge del 1989 sul servizio di sicurezza e la legge del 1994 sui servizi di intelligence specificano che i capi delle agenzie di intelligence hanno il compito di garantire che non sia ottenuta o comunicata alcuna informazione fatta eccezione per quanto necessario per il corretto adempimento delle funzioni di agenzia o per altre finalità limitate e specifiche elencate nelle disposizioni pertinenti ([432]).

(242) Inoltre la sezione 109 della legge del 2018 sulla protezione dei dati stabilisce requisiti specifici per i trasferimenti internazionali di dati personali da parte dei servizi di intelligence verso paesi terzi od organizzazioni internazionali. Ai sensi di tale disposizione, i dati personali non possono essere trasferiti verso un paese o territorio al di fuori del Regno Unito o verso un'organizzazione internazionale, fatto salvo il caso in cui il trasferimento sia necessario e proporzionato per l'esercizio delle funzioni statutarie del titolare del trattamento o per altre finalità previste dalla sezione 2, paragrafo 2, lettera a), della legge del 1989 sul servizio di sicurezza o dalla sezione 2, paragrafo 2, lettera a), e dalla sezione 4, paragrafo 2, lettera a), della legge del 1994 sui servizi di intelligence ([433]). È importante sottolineare che tali requisiti si applicano anche nei casi in cui è invocata l'esenzione per motivi di sicurezza nazionale a norma della sezione 110 della legge del 2018 sulla protezione dei dati, in quanto detta sezione non elenca la sezione 109 della medesima legge come una delle disposizioni che possono essere disapplicate se è richiesta un'esenzione rispetto a determinate disposizioni al fine di salvaguardare la sicurezza nazionale.

(243) Inoltre, come sottolineato dall'ICO negli orientamenti sul trattamento da parte dei servizi di intelligence, oltre alle garanzie previste dalla parte 4 della legge del 2018 sulla protezione dei dati, un'agenzia di intelligence, quando condivide dati con un organismo di intelligence di un paese terzo, è soggetta anche alle garanzie previste da altre misure legislative loro applicabili per garantire che i dati personali siano ottenuti, condivisi e trattati in modo lecito e responsabile ([434]). Ad esempio, la legge del 2016 sui poteri di indagine stabilisce ulteriori garanzie in relazione ai trasferimenti verso un paese terzo di materiali raccolti attraverso intercettazione mirata ([435]), ingerenza mirata in apparecchiature ([436]), intercettazione massiva ([437]), acquisizione massiva di dati relativi alle comunicazioni ([438]) e ingerenza massiva in apparecchiature ([439]) (cosiddette »comunicazioni all'estero«). In particolare l'autorità che rilascia il mandato deve assicurarsi che siano in atto dispositivi destinati a garantire che il paese terzo che riceve i dati limiti al minimo necessario per le finalità di cui alla legge del 2016 sui poteri di indagine il numero di persone che accedono al materiale, la portata della comunicazione e il numero di copie effettuate di qualsiasi materiale ([440]).

3.3.3 *Vigilanza*

(244) L'accesso da parte delle pubbliche amministrazioni per finalità di sicurezza nazionale è soggetto a vigilanza ad opera di una serie di organismi diversi. L'*Information Commissioner* vigila sul trattamento dei dati personali ai sensi della legge del 2018 sulla protezione dei dati (per ulteriori informazioni sull'indipendenza, sulla nomina, sul ruolo e sui poteri di tale commissario cfr. considerando da 85 a 98); la vigilanza indipendente e giudiziaria sull'utilizzo dei poteri di indagine ai sensi della legge del 2016 sui poteri di indagine spetta invece all'*Investigatory Powers*

([430]) Sezione 87, paragrafo 1, della legge del 2018 sulla protezione dei dati.

([431]) Sezione 87, paragrafo 3, della legge del 2018 sulla protezione dei dati. Sebbene i titolari del trattamento possano essere esentati da tale principio ai sensi della sezione 110 della legge del 2018 sulla protezione dei dati qualora tale misura sia necessaria per salvaguardare la sicurezza nazionale, tale esenzione deve essere valutata caso per caso e può essere invocata soltanto nella misura in cui l'applicazione di una disposizione particolare avrebbe conseguenze negative per la sicurezza nazionale (cfr. considerando 132). I certificati di sicurezza nazionale per i servizi di intelligence del Regno Unito (disponibili al seguente indirizzo: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) non riguardano la sezione 87, paragrafo 3, della legge del 2018 sulla protezione dei dati. Inoltre dato che qualsiasi trattamento per una finalità diversa deve essere autorizzato dalla legge, i servizi di intelligence devono disporre di una base giuridica chiara per procedere al trattamento ulteriore.

([432]) Per ulteriori informazioni su tali finalità si veda la nota312.

([433]) Cfr. nota 312.

([434]) Orientamenti dell' ICO sul trattamento da parte dei servizi di intelligence (cfr. nota 161).

([435]) Sezione 54 della legge del 2016 sui poteri di indagine.

([436]) Sezione 130 della legge del 2016 sui poteri di indagine.

([437]) Sezione 151 della legge del 2016 sui poteri di indagine.

([438]) Sezione 171, paragrafo 9, della legge del 2016 sui poteri di indagine.

([439]) Sezione 192 della legge del 2016 sui poteri di indagine.

([440]) Tali dispositivi devono comprendere misure destinate a garantire che ogni copia effettuata di qualsiasi materiale di tale tipo sia conservata, per tutta la durata della sua conservazione, in maniera sicura. Il materiale ottenuto ai sensi di un mandato e ogni copia effettuata di uno qualsiasi di tali materiali devono essere distrutti non appena non sussistano più i motivi pertinenti per conservarli (cfr. sezione 150, paragrafi 2 e 5, e sezione 151, paragrafo 2, della legge del 2016 sui poteri di indagine). È opportuno notare che garanzie analoghe, previste nell'ambito del precedente quadro giuridico (RIPA 2000), sono state ritenute conformi ai requisiti stabiliti dalla Corte europea dei diritti dell'uomo per la condivisione di materiale ottenuto mediante intercettazione massiva con Stati stranieri o organizzazioni internazionali [Corte europea dei diritti dell'uomo (Grande Sezione), *Big Brother Watch and others v United Kingdom*, (cfr. nota 279), punti 362 e 399).

Commissioner. L'*Investigatory Powers Commissioner* vigila sull'utilizzo dei poteri di indagine di cui alla legge del 2016 sui poteri di indagine da parte delle autorità di contrasto e di sicurezza nazionale. La vigilanza a livello politico è garantita dall'*Intelligence Service Committee* (commissione dei servizi di intelligence) del parlamento.

3.3.3.1 Vigilanza ai sensi della parte 4 della legge sulla protezione dei dati

(245) Il trattamento dei dati personali svolto dai servizi di intelligence ai sensi della parte 4 della legge del 2018 sulla protezione dei dati è oggetto di vigilanza da parte dell'*Information Commissioner* ([441]).

(246) Le funzioni generali dell'*Information Commissioner* in relazione al trattamento dei dati personali da parte di servizi di intelligence ai sensi della parte 4 della legge del 2018 sulla protezione dei dati sono stabilite nell'allegato 13 di tale legge. Tra tali compiti figurano, a titolo esemplificativo ma non esaustivo, il controllo e l'assicurazione del rispetto delle norme di cui alla parte 4 della legge del 2018 sulla protezione dei dati, la promozione della sensibilizzazione del pubblico, attività di consulenza a favore del parlamento, del governo e di altre istituzioni in merito a misure legislative e amministrative, la promozione della consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo ai loro obblighi, l'erogazione di informazioni a un interessato sull'esercizio dei suoi diritti, lo svolgimento di indagini, ecc.

(247) Per quanto concerne la parte 3 della legge del 2018 sulla protezione dei dati, l'*Information Commissioner* ha il potere di notificare ai titolari del trattamento una presunta violazione, emettere avvertimenti in merito al fatto che è probabile che un trattamento violi le norme e emettere ammonimenti quando la violazione è confermata. Può inoltre emettere avvisi di esecuzione e di irrogazione di sanzioni per violazioni di determinate disposizioni della legge ([442]). Tuttavia, contrariamente a quanto previsto per altre parti della legge del 2018 sulla protezione dei dati, l'*Information Commissioner* non può rivolgere un avviso di valutazione a un organismo di sicurezza nazionale ([443]).

(248) Inoltre la sezione 110 della legge del 2018 sulla protezione dei dati prevede un'eccezione all'utilizzo di determinati poteri da parte dell'*Information Commissioner* quando ciò è necessario al fine di proteggere la sicurezza nazionale. Ciò riguarda tra l'altro il potere dell'*Information Commissioner* di emettere (qualsiasi tipo di) avvisi ai sensi della legge sulla protezione dei dati (avvisi di informazione, di valutazione, di esecuzione e di irrogazione di sanzioni), il potere di effettuare ispezioni in conformità con gli obblighi internazionali, i poteri di accesso e di ispezione e le norme in materia di reati ([444]). Come spiegato al considerando 126, tali eccezioni saranno applicate soltanto se necessario e proporzionato e su base individuale.

(249) L'ICO e i servizi di intelligence del Regno Unito hanno firmato un protocollo d'intesa ([445]) che stabilisce un quadro per la cooperazione su una serie di questioni, comprese le notifiche di violazioni dei dati e la gestione dei reclami degli interessati. In particolare tale protocollo prevede che, quando riceve un reclamo, l'ICO valuti che la domanda di qualsiasi esenzione per motivi di sicurezza nazionale sia stata utilizzata in maniera adeguata. Le risposte alle domande poste dall'ICO nel contesto dell'esame di singoli reclami devono essere fornite entro 20 giorni lavorativi dall'agenzia di sicurezza nazionale interessata, utilizzando canali sicuri adeguati laddove la questione riguardi informazioni classificate. Da aprile 2018 ad oggi l'ICO ha ricevuto 21 reclami da persone fisiche in relazione ai servizi di intelligence. Ogni reclamo è stato valutato e l'esito è stato comunicato all'interessato ([446]).

([441]) Sezione 116 della legge del 2018 sulla protezione dei dati.

([442]) Ai sensi dell'allegato 13, paragrafo 2, della legge del 2018 sulla protezione dei dati, gli avvisi di esecuzione e di irrogazione di sanzioni possono essere emessi nei confronti di un titolare del trattamento o di un responsabile del trattamento in relazione a violazioni della parte 4, capo 2, della legge del 2018 sulla protezione dei dati (principi di trattamento), a una disposizione della parte 4 della legge del 2018 sulla protezione dei dati che conferisce diritti a un interessato, a un requisito che impone la comunicazione di una violazione dei dati personali all'*Information Commissioner* ai sensi della sezione 108 della legge del 2018 sulla protezione dei dati, nonché in relazione ai principi per i trasferimenti di dati personali verso paesi terzi, paesi che non hanno sottoscritto convenzioni e organizzazioni internazionali di cui alla sezione 109 della legge del 2018 sulla protezione dei dati (per ulteriori dettagli in merito all'avviso di esecuzione e di irrogazione di sanzioni cfr. considerando(92)).

([443]) Ai sensi della sezione 147, paragrafo 6. della legge del 2018 sulla protezione dei dati, l'*Information Commissioner* non può emettere un avviso di valutazione nei confronti di un organismo di cui alla sezione 23, paragrafo 3, della legge del 2000 sulla libertà di informazione. Rientrano in tale contesto il *Security Service* (MI5), il *Secret Intelligence Service* (MI6) e il *Government Communications Headquarter*.

([444]) Le disposizioni che possono essere esentate sono: articolo 108 (comunicazione di una violazione dei dati personali all'*Information Commissioner*), articolo 119 (ispezione in conformità con gli obblighi internazionali); articoli da 142 a 154 e allegato 15 (avvisi dell'*Information Commissioner* e poteri di accesso e ispezione); e articoli da 170 a 173 (reati relativi ai dati personali). Inoltre, in relazione al trattamento da parte dei servizi di intelligence di cui all'allegato 13 (altre funzioni generali dell'*Information Commissioner*), il paragrafo 1, lettere a) e g) e il paragrafo 2.

([445]) Protocollo d'intesa tra l'ICO e la *UK Intelligence Community*, cfr. nota 165.

([446]) In sette di questi casi, l'ICO ha consigliato al reclamante di far presente la propria preoccupazione al titolare del trattamento (ciò si verifica quando una persona fisica segnala una sua preoccupazione all'ICO, ma avrebbe dovuto prima comunicarla al titolare del trattamento); in uno di questi casi, l'ICO ha fornito un consiglio generale al titolare del trattamento (tale strumento viene utilizzato quando le azioni del titolare del trattamento non paiono aver violato la legislazione, ma un miglioramento delle pratiche avrebbe potuto evitare che la preoccupazione venisse segnalata all'ICO); mentre negli altri 13 casi, non è stata richiesta alcuna azione da parte del titolare del trattamento (ciò avviene quando le preoccupazioni sollevate dalla persona fisica non rientrano nell'ambito di applicazione della legge del 2018 sulla protezione dei dati perché riguardano il trattamento di informazioni personali, ma sulla base delle informazioni fornite il titolare del trattamento non sembra aver violato la legislazione).

3.3.3.2 Vigilanza sull'utilizzo dei poteri di indagine ai sensi della legge del 2016 sui poteri di indagine

(250) Ai sensi della parte 8 della legge del 2016 sui poteri di indagine, la vigilanza sull'utilizzo dei poteri di indagine è esercitata dall'*Investigatory Powers Commissioner* (IPC). L'*Investigatory Powers Commissioner* è assistito da altri commissari giudiziari, che sono collettivamente denominati commissari giudiziari ([447]). La legge del 2016 sui poteri di indagine fissa le garanzie per la tutela dell'indipendenza dei commissari giudiziari. I commissari giudiziari devono rivestire, o aver rivestito, un incarico giudiziario di alto livello (ossia devono essere, o essere stati, membri delle più alte corti) ([448]), e, come ogni membro della magistratura, godono di uno status indipendente dal governo ([449]). Ai sensi della sezione 227 della legge del 2016 sui poteri di indagine, è il primo ministro a nominare l'*Investigatory Powers Commissioner* e il numero di commissari giudiziari che ritiene necessario. Tutti i commissari, siano essi membri attuali o ex membri della magistratura, possono essere nominati solo sulla base di una raccomandazione comune dei tre Giudici capo di Inghilterra e Galles, Scozia e Irlanda del Nord e del Lord Cancelliere ([450]). Il segretario di Stato deve fornire all'*Investigatory Powers Commissioner* personale, locali, apparecchiature e altre strutture e servizi ([451]). Il mandato dei commissari ha una durata di tre anni e i commissari possono essere rinominati ([452]). Ad ulteriore garanzia della loro indipendenza, la nomina a commissario giudiziario può essere revocata soltanto a condizioni rigorose che impongono una soglia elevata: dal primo ministro in circostanze specifiche elencate in maniera esaustiva alla sezione 228, paragrafo 5, della legge del 2016 sui poteri di indagine (quali il fallimento o l'incarcerazione) oppure qualora sia emessa una risoluzione che approva tale revoca da ciascuna camera del parlamento ([453]).

(251) L'*Investigatory Powers Commissioner* e i commissari giudiziari sono sostenuti nei loro ruoli dall'*Investigatory Powers Commissioner's Office* (IPCO). Il personale dell'IPCO comprende un gruppo di ispettori, esperti giuridici e tecnici interni e un comitato consultivo sulle tecnologie incaricato di fornire consulenza di esperti. Come per i singoli commissari giudiziari, l'indipendenza dell'IPCO è tutelata. L'IPCO è un »organismo indipendente« del ministero dell'Interno, ossia riceve finanziamenti da quest'ultimo ma svolge le proprie funzioni in maniera indipendente ([454]).

(252) Le principali funzioni dei commissari giudiziari sono definite dalla sezione 229 della legge del 2016 sui poteri di indagine ([455]). In particolare i commissari giudiziari dispongono di un ampio potere di approvazione preventiva, che rientra nel contesto delle garanzie introdotte nel quadro giuridico del Regno Unito con la legge del 2016 sui poteri di indagine. I mandati in relazione all'intercettazione mirata, all'ingerenza in apparecchiature, alle serie massive di dati personali, all'acquisizione massiva di dati relativi alle comunicazioni così come gli avvisi di conservazione per i dati relativi alle comunicazioni devono tutti essere approvati da commissari giudiziari ([456]). L'*Investigatory Powers Commissioner* deve inoltre preautorizzare l'acquisizione di dati relativi alle comunicazioni per finalità di contrasto ([457]). Se un commissario rifiuta di approvare un mandato, il segretario di Stato può presentare ricorso presso l'*Investigatory Powers Commissioner*, la cui decisione è definitiva.

([447]) Conformemente alla sezione 227, paragrafi 7 e 8, della legge del 2016 sui poteri di indagine, l'*Investigatory Powers Commissioner* è un commissario giudiziario e l'*Investigatory Powers Commissioner* e gli altri commissari giudiziari sono collettivamente denominati commissari giudiziari. Attualmente vi sono 15 commissari giudiziari.

([448]) Ai sensi della sezione 60, paragrafo 2, della parte 3 della *Constitutional Reform Act 2005* (legge del 2005 sulla riforma costituzionale), con «incarico giudiziario di alto livello» si intende un incarico in veste di giudice di uno dei seguenti organi giurisdizionali: i) la Corte suprema; ii) la Corte d'appello in Inghilterra e Galles; iii) l'Alta Corte in Inghilterra e Galles; iv) la *Court of Session*; v) la Corte d'appello in Irlanda del Nord; vi) l'Alta Corte in Irlanda del Nord; oppure l'aver agito in veste di *Lord of Appeal in Ordinary*.

([449]) L'indipendenza del potere giudiziario si basa sulla convenzione ed è stata ampiamente riconosciuta sin dal *1701 Act of Settlement* (atto di disposizione 1701).

([450]) Sezione 227, paragrafo 3, della legge del 2016 sui poteri di indagine. I commissari giudiziari devono essere raccomandati anche dall'*Investigatory Powers Commissioner* (articolo 227, paragrafo 4, della legge del 2016 sui poteri di indagine).

([451]) Sezione 238 della legge del 2016 sui poteri di indagine.

([452]) Sezione 227, paragrafo 2, della legge del 2016 sui poteri di indagine.

([453]) Il processo di rimozione dall'incarico è identico a quello per la rimozione di altri giudici nel Regno Unito (cfr. ad esempio articolo 11, paragrafo 3 della *Senior Courts Act 1981* (legge del 1981 sugli organi giurisdizionali di grado superiore) e la sezione 33 della legge del 2005 sulla riforma costituzionale, che richiede altresì che sia emessa una risoluzione in seguito a un'approvazione da parte di entrambe le camere del parlamento). Ad oggi nessun commissario giudiziario è stato rimosso dal proprio incarico.

([454]) Un organismo indipendente è un'organizzazione o un'agenzia che riceve finanziamenti da un governo, ma è in grado di agire in maniera indipendente (per una definizione e ulteriori informazioni in merito, cfr. manuale del Cabinet Office «*Classification Of Public Bodies: Guidance For Departments*», disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf così come la prima relazione della sessione 2014-2015 della commissione ad hoc sulla pubblica amministrazione della Camera dei Comuni, disponibile al seguente indirizzo: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf).

([455]) Ai sensi della sezione 229 della legge del 2016 sui poteri di indagine, il commissario giudiziario dispone di ampi poteri di vigilanza, che comprendono anche la vigilanza sulla conservazione e sulla comunicazione dei dati raccolti dalle agenzie di intelligence.

([456]) Le decisioni in merito all'approvazione o meno di una decisione del segretario di Stato di rilasciare un mandato spettano ai commissari giudiziari. Se un commissario rifiuta di approvare un mandato, il segretario di Stato può presentare ricorso presso l'*Investigatory Powers Commissioner*, la cui decisione è definitiva.

([457]) L'autorizzazione dell'*Investigatory Powers Commissioner* è sempre richiesta laddove i dati relativi alle comunicazioni vengano acquisiti per finalità di contrasto (articolo 60A della legge del 2016 sui poteri di indagine). Laddove i dati relativi alle comunicazioni vengano acquisiti per finalità di sicurezza nazionale, l'autorizzazione può essere concessa dall'*Investigatory Powers Commissioner* o, in alternativa, da un funzionario di grado elevato designato dell'autorità pubblica pertinente (cfr. articoli 61 e 61A della legge del 2016 sui poteri di indagine e considerando 203).

(253) Il relatore speciale delle Nazioni Unite sul diritto alla tutela della vita privata ha accolto con molto favore l'istituzione dei commissari giudiziari da parte della legge del 2016 sui poteri di indagine, in quanto »tutte le richieste più sensibili o intrusive di svolgere attività di sorveglianza devono essere autorizzate tanto da un ministro del gabinetto quanto dall'IPCO«. In particolare il relatore speciale ha sottolineato che »tale aspetto di controllo giurisdizionale [attraverso il ruolo dell'*Investigatory Powers Commissioner*] assistito da un gruppo di ispettori esperti ed esperti tecnologici, dotato di risorse migliori, costituisce una delle nuove garanzie più significative introdotte dalla legge sui poteri di indagine«, che ha sostituito un sistema precedentemente frammentato di autorità di vigilanza e che integra il ruolo dell'*Intelligence and Security Committee* (ISC, commissione per l'intelligence e la sicurezza) del parlamento e dell'*Investigatory Powers Tribunal*» ([458]).

(254) Inoltre l'*Investigatory Powers Commissioner* dispone di poteri per effettuare una vigilanza ex post (anche mediante audit, ispezione e indagine) dell'utilizzo dei poteri di indagine ai sensi della legge del 2016 sui poteri di indagine ([459]) e di alcuni altri poteri e di alcune altre funzioni previste nella legislazione pertinente ([460]). I risultati di tale vigilanza ex post sono compresi nella relazione che l'*Investigatory Powers Commissioner* deve preparare annualmente e presentare al primo ministro ([461]) e che deve essere pubblicata e presentata al parlamento ([462]). La relazione contiene statistiche e informazioni pertinenti sull'utilizzo dei poteri di indagine da parte delle agenzie di intelligence e delle autorità di contrasto nonché dell'impiego di garanzie in relazione a materiale coperto da segreto professionale, materiale giornalistico riservato e fonti di informazione giornalistica riservate, informazioni sugli accordi presi e sulle finalità operative utilizzate nel contesto dei mandati massivi. Infine, nella relazione annuale dell'IPCO, è specificato in quale settore sono state formulate raccomandazioni indirizzate alle autorità pubbliche e in che modo tali raccomandazioni sono state affrontate ([463]).

(255) Conformemente alla sezione 231 della legge del 2016 sui poteri di indagine, se l'*Investigatory Powers Commissioner* viene a conoscenza di qualsiasi errore pertinente commesso da autorità pubbliche nell'utilizzo dei loro poteri di indagine, deve informare la persona interessata laddove ritenga che l'errore sia grave e sia nell'interesse pubblico informare tale persona ([464]). In particolare la sezione 231 della legge del 2016 sui poteri di indagine specifica che, quando informa una persona di un errore, l'*Investigatory Powers Commissioner* deve fornire informazioni in merito a qualsiasi diritto spettante a tale persona di adire l'*Investigatory Powers Tribunal*, nonché fornire i dettagli che ritenga necessari per l'esercizio di tali diritti e indicare l'esistenza di un interesse pubblico per la comunicazione ([465]).

([458]) Dichiarazione di fine missione del relatore speciale sul diritto alla tutela della vita privata in occasione della conclusione della sua missione nel Regno Unito di Gran Bretagna e Irlanda del Nord (cfr. nota 281).

([459]) Sezione 229 della legge del 2016 sui poteri di indagine. I poteri di indagine e informazione del commissario giudiziario sono stabiliti nella sezione 235 della legge del 2016 sui poteri di indagine.

([460]) Rientrano in tale contesto misure di sorveglianza ai sensi della RIPA 2000, l'esercizio di funzioni ai sensi della parte 3 della *Police Act 1997* (legge del 1997 sulla polizia) (autorizzazione all'azione in relazione alla proprietà) e l'esercizio da parte del segretario di Stato delle funzioni ai sensi degli articoli da 5 a 7 della legge del 1994 sui servizi di intelligence (mandato per ingerenza con telegrafia wireless, accesso e ingerenza nella proprietà (articolo 229 della legge del 2016 sui poteri di indagine)).

([461]) Sezione 230 della legge del 2016 sui poteri di indagine. L'*Investigatory Powers Commissioner* può altresì riferire al primo ministro di propria iniziativa in merito a qualsiasi questione relativa alle proprie funzioni. L'*Investigatory Powers Commissioner* deve altresì riferire al primo ministro su richiesta di quest'ultimo e il primo ministro può fornire istruzioni all'*Investigatory Powers Commissioner* affinché riesamini qualsiasi funzione dei servizi di intelligence.

([462]) Talune parti possono essere escluse laddove la pubblicazione sarebbe contraria alla sicurezza nazionale.

([463]) Ad esempio, nella relazione annuale del 2019 dell'IPCO (punto 6.38) è menzionato che all'MI5 è stato raccomandato di modificare la sua politica di conservazione per le serie massive di dati personali in quanto avrebbe dovuto adottare un approccio che tenesse conto della proporzionalità della conservazione per tutti i campi nei casi di detenzioni di tali serie di dati e per ciascuna di tali serie detenuta. Alla fine del 2018, l'IPCO ha affermato di non essere convinto del fatto che fosse stato dato seguito a tale raccomandazione e la relazione del 2019 ha spiegato che l'MI5 sta ora introducendo un nuovo processo per il soddisfacimento di tale requisito. La relazione annuale del 2019 (punto 8.22) menziona altresì che il GHCQ ha ricevuto una serie di raccomandazioni riguardanti la tenuta di registri in merito alla proporzionalità delle loro interrogazioni su dati massivi. La relazione conferma che alla fine del 2018 risultavano essere stati compiuti miglioramenti in questo settore. Relazione annuale del 2019 dell'*Investigatory Powers Commissioner Office*, disponibile al seguente indirizzo: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Inoltre, ogni ispezione di un'autorità pubblica da parte dell'IPCO si conclude con una relazione che viene trasmessa all'autorità e che comprende tutte le raccomandazioni risultanti dall'ispezione. L'IPCO inizia quindi ogni ispezione successiva con un riesame delle eventuali raccomandazioni precedenti, e nella nuova relazione di ispezione indica se le raccomandazioni precedenti sono state attuate o se sono state riportate.

([464]) Un errore è considerato «grave» quando il Commissario ritiene che abbia causato pregiudizi o danni significativi alla persona interessata (articolo 231, paragrafo 2, della legge del 2016 sui poteri di indagine). Nel 2018 sono stati segnalati 22 errori di cui otto sono stati considerati gravi e hanno portato all'informazione della persona interessata. Cfr. relazione annuale del 2018 dell'*Investigatory Powers Commissioner Office*, allegato C (cfr. https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). Nel 2019 sono stati 14 gli errori considerati essere gravi. Cfr. relazione annuale del 2019 dell'apporto annuale dell'*Investigatory Powers Commissioner Office*, allegato C, cfr. nota 463.

([465]) L'articolo 231 della legge del 2016 sui poteri di indagine specifica che quando informa una persona in merito a un errore, l'*Investigatory Powers Commissioner* deve fornirle i dettagli che ritiene necessari per l'esercizio dei diritti in questione, in considerazione in particolare della misura in cui rivelare dettagli sarebbe contrario all'interesse pubblico o pregiudizievole per la prevenzione o l'accertamento di reati gravi, del benessere economico del Regno Unito o dell'adempimento continuo delle funzioni di uno qualsiasi dei servizi di intelligence.

3.3.3.3 Vigilanza parlamentare sui servizi di intelligence

(256) La vigilanza parlamentare da parte della commissione per l'intelligence e la sicurezza (ISC) ha le sue basi giuridiche nella *Justice and Security Act 2013* (JSA 2013, legge del 2013 sulla giustizia e sulla sicurezza) ([466]). Tale legge istituisce l'ISC come commissione del parlamento del Regno Unito. Dal 2013 all'ISC sono stati conferiti maggiori poteri, compresa la vigilanza sulle attività operative dei servizi di sicurezza. Conformemente alla sezione 2 della legge del 2013 sulla giustizia e sulla sicurezza, l'ISC ha il compito di vigilare sulla spesa, sull'amministrazione, sulla politica e sulle operazioni delle agenzie di sicurezza nazionale. Tale legge specifica che l'ISC può condurre indagini in merito a questioni operative quando queste non si riferiscono ad operazioni in corso ([467]). Il protocollo d'intesa concordato tra il primo ministro e l'ISC ([468]) specifica in maniera dettagliata gli elementi da prendere in considerazione quando si valuta se un'attività non fa parte di alcuna operazione in corso ([469]). L'ISC può inoltre essere invitato a indagare in merito a operazioni in corso da parte del primo ministro e può esaminare le informazioni fornite volontariamente dalle agenzie.

(257) Ai sensi dell'allegato 1 della legge del 2013 sulla giustizia e sulla sicurezza l'ISC può chiedere ai capi di uno qualsiasi dei tre servizi di intelligence di rivelare qualsiasi informazione. L'agenzia deve rendere disponibili tali informazioni, fatto salvo il caso in cui il segretario di Stato ponga un veto ([470]). Secondo le spiegazioni fornite dalle autorità del Regno Unito, nella pratica sono rarissime le informazioni che non vengono divulgate dall'ISC ([471]).

(258) L'ISC è costituita da membri appartenenti a una camera del parlamento e nominati dal primo ministro in seguito a consultazione del leader dell'opposizione ([472]). L'ISC è tenuto a presentare una relazione annuale al parlamento in merito all'adempimento delle sue funzioni così come altre relazioni che ritiene adeguate ([473]). Inoltre l'ISC ha il diritto di ricevere ogni tre mesi l'elenco delle finalità operative utilizzate per esaminare il materiale ottenuto da attività massive ([474]). Copie di indagini, ispezioni o audit dell'*Investigatory Powers Commissioner* sono condivise con l'ISC dal primo ministro laddove la questione trattata nelle relazioni sia pertinente per le competenze statutarie della commissione ([475]). Infine la commissione può chiedere all'*Investigatory Powers Commissioner* di svolgere un'indagine e quest'ultimo deve informare l'ISC della decisione in merito all'eventualità o meno di svolgere tale indagine ([476]).

(259) L'ISC ha inoltre fornito contributi al progetto di legge del 2016 sui poteri di indagine, che ha portato a una serie di modifiche attualmente rispecchiate in tale legge ([477]). In particolare l'ISC ha raccomandato il rafforzamento delle protezioni in materia di tutela della vita privata introducendo una serie di protezioni a tale riguardo che si applicano

([466]) Come spiegato dalle autorità del Regno Unito, tale legge ha ampliato il mandato dell'ISC in maniera da includere un ruolo nella vigilanza sulla comunità di intelligence al di là delle tre agenzie e da consentire una vigilanza retrospettiva sulle attività operative delle agenzie in merito a questioni di interesse nazionale significativo.

([467]) Sezione 2 della legge del 2013 sulla giustizia e sulla sicurezza.

([468]) Protocollo d'intesa tra il primo ministro e l'ISC, disponibile al seguente indirizzo: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.

([469]) Protocollo d'intesa tra il primo ministro e l'ISC, punto 14, cfr. nota 468.

([470]) Il segretario di Stato può porre un veto sulla divulgazione di informazioni soltanto sulla base di due motivi: le informazioni sono sensibili e non dovrebbero essere divulgate all'ISC nell'interesse della sicurezza nazionale; oppure si tratta di informazioni aventi una natura tale che qualora fosse invitato a produrle dinanzi una commissione dipartimentale ad hoc della Camera dei Comuni, il segretario di Stato riterrebbe opportuno (per motivi non limitati alla sicurezza nazionale) non farlo (allegato 1, paragrafo 4, punto 2, della legge del 2013 sulla giustizia e sulla sicurezza).

([471]) Regno Unito, *Explanatory Framework for Adequacy Discussions, section H: National Security*, pag. 43, cfr. nota 31.

([472]) Sezione 1 della legge del 2013 sulla giustizia e sulla sicurezza. I ministri non sono ammissibili a divenire membri. I membri detengono la loro posizione in seno all'ISC per la durata del parlamento durante il quale sono stati nominati. Possono essere rimossi dall'incarico mediante una risoluzione della camera dalla quale sono stati nominati oppure se cessano di essere membri del parlamento o se diventano un ministro. Un membro può inoltre dimettersi.

([473]) Le relazioni e le dichiarazioni della commissione sono disponibili online al seguente indirizzo: https://isc.independent.gov.uk/publications/. Nel 2015 l'ISC ha pubblicato una relazione dal titolo «*Privacy and Security: A modern and transparent legal framework*» (cfr.: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf) nell'ambito della quale ha preso in considerazione il quadro giuridico per le tecniche di sorveglianza utilizzate dalle agenzie di intelligence e ha emesso una serie di raccomandazioni che sono state successivamente considerate e integrate nel progetto di *Investigatory Powers Bill* (disegno di legge sui poteri di indagine) che è stato convertito in legge, ossia nella legge del 2016 sui poteri di indagine. La risposta del governo alla relazione sulla tutela della vita privata e sulla sicurezza è disponibile al seguente indirizzo: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

([474]) Sezioni 142, 161 e 183 della legge del 2016 sui poteri di indagine.

([475]) Sezione 234 della legge del 2016 sui poteri di indagine.

([476]) Sezione 236 della legge del 2016 sui poteri di indagine.

([477]) *Intelligence and Security Committee of Parliament, Report on the draft Investigatory Powers Bill*, disponibile al seguente indirizzo: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

all'insieme dei poteri di indagine ([478]). Ha inoltre suggerito modifiche delle capacità proposte per quanto riguarda l'ingerenza in apparecchiature, le serie massive di dati personali e i dati relativi alle comunicazioni, e ha richiesto altre modifiche specifiche per rafforzare le limitazioni e le garanzie per l'utilizzo di poteri di indagine ([479]).

3.3.4 *Mezzi di ricorso*

(260) Nel settore dell'accesso da parte delle pubbliche amministrazioni per finalità di sicurezza nazionale, l'interessato deve disporre della possibilità di esperire mezzi di ricorso dinanzi a un giudice indipendente e imparziale al fine di avere accesso ai dati personali che lo riguardano o di ottenerne la rettifica o la soppressione ([480]). Tale organo giudiziario deve in particolare disporre del potere per adottare decisioni vincolanti sul servizio di intelligence ([481]). Nel Regno Unito, come spiegato nei considerando da 261 a 271, diversi mezzi di ricorso giurisdizionale offrono agli interessati la possibilità di perseguire e ottenere tali rimedi.

3.3.4.1 Meccanismi di ricorso disponibili ai sensi della parte 4 della legge sulla protezione dei dati

(261) Ai sensi della sezione 165 della legge del 2018 sulla protezione dei dati, l'interessato ha il diritto di proporre reclamo presso l'*Information Commissioner* qualora ritenga che, in relazione ai dati personali che lo riguardano, sia stata commessa una violazione della parte 4 della legge del 2018 sulla protezione dei dati. L'*Information Commissioner* ha il potere di valutare il rispetto della legge del 2018 sulla protezione dei dati da parte del titolare del trattamento e del responsabile del trattamento, e di richiedere loro di adottare le misure necessarie. Ai sensi della parte 4 della legge del 2018 sulla protezione dei dati, le persone fisiche hanno altresì il diritto di adire l'Alta Corte (o la *Court of Session* in Scozia) per ottenere l'emissione di un'ordinanza che imponga al titolare del trattamento di rispettare i diritti di accesso ai dati ([482]), di opposizione al trattamento ([483]) e di rettifica o cancellazione ([484]).

(262) Le persone fisiche hanno altresì il diritto di richiedere un risarcimento dei danni subiti a causa di una violazione in relazione a un requisito di cui alla parte 4 della legge del 2018 sulla protezione dei dati da parte del titolare del trattamento o di un responsabile del trattamento ([485]). Tali danni comprendono tanto la perdita finanziaria quanto danni che non contemplano una perdita finanziaria, quali ad esempio la sofferenza ([486]).

3.3.4.2 Meccanismi di ricorso disponibili ai sensi della legge del 2016 sui poteri di indagine

(263) Le persone fisiche possono ottenere riparazione per violazioni della legge del 2016 sui poteri di indagine adendo l'*Investigatory Powers Tribunal* (organo giurisdizionale competente per i poteri di indagine).

(264) L'*Investigatory Powers Tribunal* è stato istituito dalla RIPA 2000 ed è indipendente dal potere esecutivo ([487]). Conformemente alla sezione 65 della RIPA 2000, i membri di tale organo giurisdizionale sono nominati dalla Regina per un mandato di cinque anni. L'incarico di un membro di detto organo giurisdizionale può essere revocato dalla Regina su raccomandazione ([488]) presentata da entrambe le camere del parlamento ([489]).

([478]) Tali doveri generali in relazione alla tutela della vita privata sono ora sanciti dalla sezione 2, paragrafo 2, della legge del 2016 sui poteri di indagine, che prevede che un'autorità pubblica che agisce ai sensi di tale legge debba considerare se ciò che si intende conseguite tramite il mandato, l'autorizzazione o l'avviso potrebbe essere ragionevolmente conseguito con altri mezzi meno invasivi, 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, l'interesse pubblico per l'integrità e la sicurezza dei sistemi di telecomunicazione e dei servizi postali, nonché qualsiasi altro aspetto di interesse pubblico legato alla tutela della vita privata.

([479]) Ad esempio, su richiesta dell'ISC, il numero di giorni per i quali un mandato «d'urgenza» può rimanere in atto prima che il commissario giudiziario debba approvarlo è stato ridotto da cinque a tre giorni lavorativi ed è stato conferito all'ISC il potere di rinviare determinate questioni all'*Investigatory Powers Commissioner* per una sua indagine.

([480]) *Schrems II*, punto 194.

([481]) *Schrems II*, punto 197.

([482]) Sezione 94, paragrafo 11, della legge del 2018 sulla protezione dei dati.

([483]) Sezione 99, paragrafo 4, della legge del 2018 sulla protezione dei dati.

([484]) Sezione 100, paragrafo 1, della legge del 2018 sulla protezione dei dati.

([485]) Sezione 169 della legge del 2018 sulla protezione dei dati, che consente la presentazione di istanze da parte di «una persona che subisca danni in ragione di una violazione di un requisito della legislazione in materia di protezione dei dati». Secondo le informazioni fornite dalle autorità del Regno Unito nella pratica è probabile che una domanda o un reclamo nei confronti dei servizi di intelligence debba essere presentata o promosso adendo l'*Investigatory Powers Tribunal* il quale gode di un'ampia competenza giurisdizionale e ha la facoltà di riconoscere un indennizzo/un risarcimento dei danni. Promuovere un'azione dinanzi tale organo giurisdizionale non comporta alcun costo.

([486]) Sezione 169, paragrafo 5, della legge del 2018 sulla protezione dei dati.

([487]) Ai sensi dell'allegato 3 della RIPA 2000, i membri devono disporre di un'esperienza giudiziaria specificata ed essere ammissibili a beneficiare di una eventuale rinnovabilità del mandato.

([488]) Una raccomandazione, in inglese «*address*», è una mozione presentata dinanzi al parlamento che intende rendere il monarca consapevole dei pareri del parlamento in merito a una questione specifica.

([489]) Allegato 3, paragrafo 1, punto 5, della RIPA 2000.

(265) Ai sensi della sezione 65 della legge della RIPA 2000, tale organo giurisdizionale è competente a pronunciarsi sui reclami promossi da chiunque si ritenga leso da un comportamento nell'ambito della legge del 2016 sui poteri di indagine o della RIPA 2000 o da una condotta dei servizi di intelligence ([490]).

(266) Al fine di promuovere un'azione dinanzi l'*Investigatory Powers Tribunal* («requisito sulla legittimazione»), a norma della sezione 65 della RIPA 2000, una persona fisica deve ritenere ([491]) che la condotta di un servizio di intelligence sia stata adottata in relazione alla sua persona, ai suoi beni, alle comunicazioni che essa ha inviato o ricevuto, o al suo utilizzo di un servizio postale, di un servizio di telecomunicazioni o di un sistema di telecomunicazioni ([492]). Inoltre il reclamante deve ritenere che la condotta abbia avuto luogo in «circostanze impugnabili» ([493]) o «sia stata adottata da o per conto dei servizi di intelligence» ([494]). Dato che tale livello di «convinzione» è stato interpretato in maniera alquanto ampia ([495]), promuovere un'azione dinanzi a detto organo giurisdizionale richiede il soddisfacimento di requisiti di legittimazione bassi.

(267) Quando valuta un reclamo che gli è stato sottoposto, l'*Investigatory Powers Tribunal* è tenuto a determinare se le persone nei confronti delle quali è stata mossa un'accusa abbiano svolto attività in relazione al reclamante, indagare in merito all'autorità presumibilmente coinvolta nelle violazioni e stabilire se l'asserita condotta abbia avuto luogo o meno ([496]). Quando esamina un procedimento, l'*Investigatory Powers Tribunal* deve applicare i medesimi principi decisionali che verrebbero applicati da un organo giurisdizionale per un'istanza di controllo giurisdizionale ([497]). Inoltre, i destinatari di mandati e avvisi ai sensi della legge del 2016 sui poteri di indagine e ogni altra persona che eserciti funzioni di Stato, sia impiegata dalle forze di polizia o dal *Police Investigations and Review Commissioner* sono tenuti a divulgare o a fornire a detto organo giurisdizionale tutti i documenti e tutte le informazioni che detto organo giurisdizionale possa richiedere per poter esercitare la sua competenza giurisdizionale ([498]).

(268) L'*Investigatory Powers Tribunal* deve notificare al reclamante se è stata presa una decisione a suo favore o meno ([499]). Conformemente alla sezione 67, paragrafi 6 e 7, della RIPA 2000, l'*Investigatory Powers Tribunal* ha il potere di emettere provvedimenti provvisori e riconoscere risarcimenti o rendere qualsiasi altra ordinanza ritenuta opportuna. Può trattarsi di un'ordinanza di annullamento o cancellazione di un mandato o un'autorizzazione o di un'ordinanza che richieda la distruzione di qualunque registrazione di informazioni ottenute nell'esercizio di un potere conferito da un mandato, da un'autorizzazione o da un avviso, o altrimenti detenute da un'autorità pubblica

([490]) Sezione 65, paragrafo 5, della RIPA 2000.

([491]) Sulla verifica del livello di «convinzione» cfr. causa *Human Rights Watch v Secretary of State* [2016] UKIPTrib15_165-CH, punto 41. Nel contesto di tale causa l'*Investigatory Powers Tribunal*, facendo riferimento alla giurisprudenza della Corte europea dei diritti dell'uomo, ha ritenuto che la verifica adeguata riguardi la possibilità o meno che in relazione alla convinzione asserita secondo la quale una qualsiasi condotta che rientra nell'ambito di applicazione di cui alla sezione 68, paragrafo 5, della RIPA 2000 sia stata attuata da o per conto di uno dei servizi di intelligence vi sia una base fondata per tale convinzione tale per cui detta persona fisica possa sostenere di essere vittima di una violazione dovuta alla mera esistenza di misure segrete o di una legislazione che consente misure segrete soltanto se detta persona fisica è in grado di dimostrare, in base alla propria situazione personale, di essere potenzialmente a rischio di essere sottoposta a tali misure.

([492]) Sezione 65, paragrafo 4, lettera a), della RIPA 2000.

([493]) Tali circostanze fanno riferimento alla condotta di autorità pubbliche che si svolgono a fronte di un nulla osta (ad esempio un mandato, un'autorizzazione/un avviso per l'acquisizione di comunicazioni, ecc.) oppure laddove le circostanze siano tali (indipendentemente dal fatto che vi sia o meno tale autorità) da rendere inadeguata tale condotta in assenza di detto nulla osta o quanto meno senza aver valutato adeguatamente se fosse opportuno tentare di ottenere tale nulla osta. La condotta autorizzata da un commissario giudiziario è considerata aver avuto luogo in circostanze impugnabili (sezione 65, paragrafo 7ZA, della RIPA 2000) mentre altre condotte che avvengono con il permesso di un funzionario dell'autorità giudiziaria sono considerate non avere avuto luogo in circostanze impugnabili (sezione 65, paragrafi 7 e 8, della RIPA 2000).

([494]) Secondo le informazioni fornite dalle autorità del Regno Unito, la bassa soglia fissata per promuovere reclamo fa sì che non sia inusuale che l'indagine dell'organo giurisdizionale stabilisca che il reclamante non è mai stato in effetti soggetto a indagine da parte di un'autorità pubblica. L'ultima relazione statistica dell'*Investigatory Powers Tribunal* specifica che nel 2016 detto organo giurisdizionale ha ricevuto 209 reclami, il 52 % dei quali sono stati considerati futili o vessatori, mentre il 25 % ha dato come esito «nessuna constatazione». Le autorità del Regno Unito hanno spiegato che ciò significa che non vi è stato alcun ricorso a poteri/attività sotto copertura in relazione al reclamante o che vi è stato un ricorso a tecniche di copertura e l'organo giurisdizionale ha stabilito che tali attività erano lecite. Inoltre l'11 % dei reclami è stato dichiarato non rientrare nella competenza giurisdizionale, è stato ritirato o considerato non valido, il 5 % è stato chiuso per superamento dei termini, mentre nel 7 % dei casi è stata emessa una pronuncia a favore del reclamante. Relazione statistica del 2016 dell'*Investigatory Powers Tribunal*, disponibile al seguente indirizzo: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([495]) Cfr. la causa *Human Rights Watch v Secretary of State* [2016] UKIPTrib15_165-CH. Nel contesto di tale causa l'*Investigatory Powers Tribunal*, facendo riferimento alla giurisprudenza della Corte europea dei diritti dell'uomo, ha ritenuto che la verifica adeguata in relazione alla convinzione che una qualsiasi condotta che rientra nell'ambito di applicazione di cui alla sezione 68, paragrafo 5, della RIPA 2000 sia stata attuata da o per conto di uno dei servizi di intelligence consista nel valutare se la convinzione del reclamante sia fondata, anche in considerazione del fatto che una persona fisica può sostenere di essere vittima di una violazione dovuta alla mera esistenza di misure segrete o di una legislazione che consente misure segrete soltanto se detta persona fisica è in grado di dimostrare, in base alla propria situazione personale, di essere potenzialmente a rischio di essere sottoposta a tali misure (cfr. *Human Rights Watch v Secretary of State*, punto 41).

([496]) Sezione 67, paragrafo 3, della RIPA 2000.

([497]) Sezione 67, paragrafo 2, della RIPA 2000.

([498]) Sezione 68, paragrafi da 6 a 7, della RIPA 2000.

([499]) Sezione 68, paragrafo 4, della RIPA 2000.

in relazione a una persona ([500]). Conformemente alla sezione 67A della RIPA 2000, una decisione dell'*Investigatory Powers Tribunal* può essere impugnata, a condizione che il *Tribunal* o l'organo giurisdizionale di appello competente dia la propria autorizzazione.

(269) È infine opportuno sottolineare che il ruolo dell'*Investigatory Powers Tribunal* è stato discusso nel contesto di azioni giudiziarie promosse dinanzi la Corte europea dei diritti dell'uomo in diverse occasioni, in particolare nella causa *Kennedy contro Regno Unito* ([501]) e più recentemente nella causa *Big Brother Watch e altri contro Regno Unito* ([502]), in cui l'organo giurisdizionale ha dichiarato che «l'*Investigatory Powers Tribunal* si è dimostrato un solido ricorso giurisdizionale per chiunque sospetti che le proprie comunicazioni siano state intercettate dai servizi di intelligence» ([503]).

3.3.4.3 Altri meccanismi di ricorso disponibili

(270) Come spiegato ai considerando da 109 a 111, i mezzi di ricorso ai sensi della legge del 1998 sui diritti umani e la possibilità di adire la Corte europea dei diritti dell'uomo ([504]) sono disponibili anche nel settore della sicurezza nazionale. La sezione 65, paragrafo 2, della RIPA 2000 conferisce all'*Investigatory Powers Tribunal* la competenza giurisdizionale esclusiva per tutte le domande concernenti la legge sui diritti umani in relazione alle agenzie di intelligence ([505]). Ciò significa che, come osservato dall'Alta Corte, «la questione della sussistenza o meno, in un caso particolare, di una violazione della legge sui diritti umani può essere in linea di principio sollevata e decisa da un organo giurisdizionale indipendente che può avere accesso a tutto il materiale pertinente, compreso il materiale segreto. [...] Ricordiamo altresì in questo contesto che l'*Investigatory Powers Tribunal* stesso può ormai formare oggetto di un ricorso dinanzi l'organo giurisdizionale di secondo grado competente (in Inghilterra e Galles si tratterebbe della Corte d'appello); e che la Corte suprema ha recentemente deciso che l'*Investigatory Powers Tribunal* è in linea di principio assoggettabile a controllo giurisdizionale: cfr. *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219» ([506]).

(271) Ne consegue che quando le autorità del Regno Unito preposte all'attività di contrasto o alla sicurezza nazionale accedono a dati personali che rientrano nel campo di applicazione della presente decisione, tale accesso è disciplinato da leggi che stabiliscono le condizioni alle quali può avvenire l'accesso e assicurano che l'accesso e l'ulteriore uso dei dati siano limitati a quanto necessario e proporzionati all'obiettivo di contrasto o di sicurezza nazionale perseguito. Inoltre tale accesso è soggetto nella maggior parte dei casi alla previa autorizzazione da parte di un organo giudiziario, attraverso l'approvazione di un mandato o di un'ordinanza per la consegna di prove, e in ogni caso a una vigilanza indipendente. Dopo che le autorità pubbliche hanno avuto accesso ai dati, il loro trattamento, compresi la condivisione successiva e il trasferimento successivo, è soggetto a garanzie specifiche in materia di protezione dei dati ai sensi della parte 3 della legge del 2018 sulla protezione dei dati, che rispecchiano quelle di cui alla direttiva (UE) 2016/680, per il trattamento da parte di autorità di contrasto e della parte 4 della medesima legge per il trattamento da parte di agenzie di intelligence. Infine gli interessati godono in questo settore di diritti a mezzi di ricorso effettivi in sede amministrativa e giudiziale, e hanno in particolare il diritto di accedere ai loro dati e di ottenerne la rettifica o la cancellazione.

(272) Data l'importanza di tali condizioni, limitazioni e garanzie ai fini della presente decisione, la Commissione seguirà da vicino l'applicazione e l'interpretazione delle norme del Regno Unito che disciplinano l'accesso ai dati da parte delle pubbliche amministrazioni. Ciò comprenderà gli sviluppi legislativi, normativi e giurisprudenziali pertinenti, nonché le attività dell'ICO e di altre autorità di vigilanza in questo settore. Si presterà inoltre particolare attenzione

([500]) Un esempio dell'applicazione di tali poteri è dato dalla causa *Liberty & Others vs. the Security Service, SIS, GCHQ*, [2015] UKIP Trib 13_77-H_2. L'*Investigatory Powers Tribunal* si è pronunciato a favore di due reclamanti dato che, in un caso, la comunicazione del reclamante è stata conservata oltre i limiti stabiliti e, nell'altro, la procedura sull'esame non è stata seguita come stabilito nelle norme interne di GCHQ. Nel primo caso l'organo giurisdizionale ha ordinato ai servizi di intelligence di distruggere le comunicazioni conservate oltre il termine pertinente. Nel secondo caso non è stato emesso un ordine di distruzione perché la comunicazione non era stata conservata.

([501]) *Kennedy*, cfr. nota 129.

([502]) Corte europea dei diritti dell'uomo (Grande Sezione), *Big Brother Watch and others v United Kingdom*, (cfr. nota 268), punti da 413 a 415.

([503]) Corte europea dei diritti dell'uomo, *Big Brother Watch*, punto 425

([504]) Come illustrato, ad esempio, dalla recente sentenza della Grande Sezione della Corte europea dei diritti dell'uomo nella causa *Big Brother Watch and others v United Kingdom* (cfr. nota 279), ciò consente un controllo giurisdizionale effettivo — analogo a quello cui sono soggetti gli Stati membri dell'UE — da parte di un organo giurisdizionale internazionale sul rispetto dei diritti fondamentali da parte delle autorità pubbliche quando accedono ai dati personali. Inoltre, l'esecuzione delle sentenze della Corte europea dei diritti dell'uomo è soggetta a un controllo specifico da parte del Consiglio d'Europa.

([505]) Nella causa *Belhaj & others [2017] UKSC 3* la constatazione della non liceità dell'intercettazione di materiale coperto da segreto professionale si è basata direttamente sull'articolo 8 della CEDU (cfr. constatazione 11).

([506]) *High Court of Justice, Liberty*, [2019] EWHC 2057 (Admin), punto 170.

all'esecuzione da parte del Regno Unito delle sentenze pertinenti della Corte europea dei diritti dell'uomo, comprese le misure individuate nei «piani d'azione» e nelle «relazioni d'azione» presentate al Comitato dei ministri nel contesto del controllo del rispetto delle sentenze della Corte.

4. **CONCLUSIONI**

(273) La Commissione ritiene che il GDPR del Regno Unito e la legge del 2018 sulla protezione dei dati assicurino un livello di protezione dei dati personali trasferiti dall'Unione europea che è essenzialmente equivalente a quello garantito dal regolamento (UE) 2016/679.

(274) Inoltre la Commissione ritiene che, nel complesso, i meccanismi di vigilanza e i mezzi di ricorso previsti dal diritto del Regno Unito consentano 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, in ultima analisi, di ottenerne la rettifica o la cancellazione.

(275) 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, sarà limitata a quanto strettamente necessario per conseguire l'obiettivo legittimo in questione; la Commissione ritiene inoltre che esista una protezione giuridica efficace contro tale ingerenza.

(276) Di conseguenza, in considerazione delle risultanze di cui alla presente decisione, è opportuno decidere che il Regno Unito assicura 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.

(277) Questa conclusione si basa tanto sul regime interno pertinente del Regno Unito quanto sugli impegni assunti dal Regno Unito a livello internazionale, in particolare l'adesione alla convenzione europea dei diritti dell'uomo e l'assoggettamento alla competenza giurisdizionale della Corte europea dei diritti dell'uomo. Il costante adempimento di tali obblighi internazionali costituisce pertanto un aspetto particolarmente importante della valutazione sulla quale si basa la presente decisione.

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

(278) Gli Stati membri e i loro organi sono tenuti ad adottare le misure necessarie per conformarsi agli atti delle istituzioni dell'Unione, poiché 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.

(279) 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 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.

(280) 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* ([507]), 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 per l'affermazione di tali obiezioni dinanzi un organo giurisdizionale nazionale, che può essere tenuto a effettuare un rinvio pregiudiziale alla Corte di giustizia ([508]).

([507]) *Schrems*, punto 65.

([508]) *Schrems*, 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».

6. MONITORAGGIO, SOSPENSIONE, ABROGAZIONE O MODIFICA DELLA PRESENTE DECISIONE

(281) 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 in seguito all'adozione della presente decisione al fine di valutare se sia sempre assicurato un livello essenzialmente equivalente di protezione. Tale monitoraggio è particolarmente importante in questo caso, in quanto il Regno Unito gestirà, applicherà e farà rispettare un nuovo regime di protezione dei dati non più soggetto al diritto dell'Unione europea, che potrebbe essere suscettibile di evoluzioni. A tale riguardo, si presterà particolare attenzione all'applicazione pratica delle norme del Regno Unito sul trasferimento di dati personali verso paesi terzi e all'impatto che ciò può avere sul livello di protezione offerto ai dati trasferiti a norma della presente decisione; 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'ICO e di altri organismi indipendenti contribuiranno al monitoraggio della Commissione.

(282) 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 presente decisione, nonché di qualsiasi evoluzione delle pratiche relative al trattamento dei dati personali oggetto della 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 281.

(283) 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.

(284) Se dalle informazioni disponibili, in particolare da quelle risultanti dal monitoraggio della 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.

(285) 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.

(286) 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.

(287) 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. DURATA E RINNOVO DELLA PRESENTE DECISIONE

(288) La Commissione deve tenere conto del fatto che, alla fine del periodo di transizione previsto dall'accordo di recesso e non appena la disposizione provvisoria di cui all'articolo 782 dell'accordo sugli scambi e la cooperazione UE-Regno Unito cesserà di applicarsi, il Regno Unito gestirà, applicherà e farà rispettare un nuovo regime di protezione dei dati che sostituirà quello in vigore quando era vincolato dal diritto dell'Unione europea. Ciò può comportare in particolare modifiche o cambiamenti del quadro di protezione dei dati valutato nella presente decisione, nonché altri sviluppi pertinenti.

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

(290) 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**

(291) Il comitato europeo per la protezione dei dati ha pubblicato il proprio parere ([509]), del quale si è tenuto conto nell'elaborazione della presente decisione.

(292) Le misure di cui alla presente decisione sono conformi al parere del comitato istituito a norma dell'articolo 93 del regolamento (UE) 2016/679,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

1. 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 del regolamento (UE) 2016/679 dall'Unione europea verso il Regno Unito.

2. La presente 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 sulla protezione dei dati.

Articolo 2

Quando, al fine di proteggere le persone con riguardo al trattamento dei loro dati personali, le autorità di controllo competenti degli Stati membri esercitano i poteri di cui all'articolo 58 del regolamento (UE) 2016/679 in relazione ai trasferimenti di dati che rientrano nell'ambito di applicazione di cui all'articolo 1, lo Stato membro interessato ne informa senza indugio la Commissione.

Articolo 3

1. La Commissione monitora costantemente l'applicazione del quadro giuridico su cui si basa la presente decisione, comprese le condizioni in cui sono effettuati i trasferimenti successivi, sono esercitati i diritti individuali e le autorità pubbliche del Regno Unito hanno accesso ai dati trasferiti sulla base della presente decisione, al fine di valutare se il Regno Unito continui a garantire un livello di protezione adeguato ai sensi dell'articolo 1.

2. Gli Stati membri e la Commissione si informano reciprocamente dei casi in cui l'*Information Commissioner* o qualsiasi altra autorità competente del Regno Unito non garantisca il rispetto del quadro giuridico su cui si basa la presente decisione.

3. Gli Stati membri e la Commissione si informano reciprocamente di qualsiasi indicazione del fatto che le ingerenze delle autorità pubbliche del Regno Unito nel diritto delle persone alla protezione dei loro dati personali vanno oltre quanto strettamente necessario o che contro tali ingerenze non esiste una tutela giuridica efficace.

4. Laddove disponga di indicazioni secondo le quali non è più garantito un livello di protezione adeguato, la Commissione informa le autorità competenti del Regno Unito e può sospendere, abrogare o modificare la presente decisione.

([509]) Parere 14/2021 relativo al progetto di decisione di esecuzione della Commissione europea a norma del regolamento (UE) 2016/679 sull'adeguata protezione dei dati personali nel Regno Unito, disponibile al seguente indirizzo: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

5. La Commissione può sospendere, abrogare o modificare la presente decisione se la mancanza di collaborazione da parte del governo del Regno Unito le impedisce di stabilire se la constatazione di cui all'articolo 1, paragrafo 1, risulti compromessa.

Articolo 4

La presente decisione scade il 27 giugno 2025, a meno che non sia prorogata secondo la procedura di cui all'articolo 93, paragrafo 2, del regolamento (UE) 2016/679.

Articolo 5

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 28 giugno 2021

Per la Commissione
Didier REYNDERS
Membro della Commissione