

DECISIONE DI ESECUZIONE (UE) 2021/1773 DELLA COMMISSIONE

del 28 giugno 2021

a norma della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito*[notificata con il numero C(2021) 4801]*

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

vista la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio ⁽¹⁾, in particolare l'articolo 36, paragrafo 3,

considerando quanto segue:

1. INTRODUZIONE

- (1) La direttiva (UE) 2016/680 definisce le norme per il trasferimento di dati dalle autorità competenti nell'Unione verso paesi terzi od organizzazioni internazionali nella misura in cui tale trasferimento rientri nel suo ambito di applicazione. Le norme sui trasferimenti internazionali di dati da parte delle autorità competenti sono stabilite nel capo V della direttiva (UE) 2016/680, in particolare negli articoli da 35 a 40. Sebbene la circolazione di dati personali verso e da paesi al di fuori dell'Unione europea sia essenziale per un'efficiente cooperazione in materia di contrasto, occorre garantire che il livello di protezione dei dati personali nell'Unione europea non sia compromesso da tali trasferimenti ⁽²⁾.
- (2) Ai sensi dell'articolo 36, paragrafo 3, della direttiva (UE) 2016/680 la Commissione può decidere, mediante un atto 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 (fatto salvo il caso in cui un altro Stato membro dal quale sono stati ottenuti i dati debba fornire la propria autorizzazione a tale trasferimento), come previsto dall'articolo 35, paragrafo 1, e dal considerando 66 della direttiva (UE) 2016/680.
- (3) Come specificato all'articolo 36, paragrafo 2, della direttiva (UE) 2016/680, l'adozione di una decisione di adeguatezza deve essere basata su un'analisi completa dell'ordinamento giuridico del paese terzo. 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 67 della direttiva (UE) 2016/680]. Il criterio rispetto al quale viene valutata l'«equivalenza sostanziale» è quello stabilito dalla legislazione dell'UE, in particolare dalla direttiva (UE) 2016/680, 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 sono rilevanti a questo proposito ⁽⁴⁾.
- (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 riservatezza e rendendone l'attuazione, l'azionabilità e il controllo effettivi, il sistema estero, nel suo insieme, offra il necessario livello di protezione ⁽⁷⁾.

⁽¹⁾ GU L 119 del 4.5.2016, pag. 89.

⁽²⁾ Cfr. considerando 64 della direttiva (UE) 2016/680.

⁽³⁾ Cfr., più di recente, la sentenza della Corte di giustizia del 16 luglio 2020, *Maximilian Schrems/Data Protection Commissioner* («*Schrems II*»), C-311/18, ECLI:EU:C:2020:559.

⁽⁴⁾ Cfr. *Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive*, adottate nel febbraio 2021, disponibili al seguente indirizzo: https://edpb.europa.eu/our-work-tools/our-documents/publication-type/recommendations_it

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

⁽⁶⁾ *Schrems*, punto 74.

⁽⁷⁾ 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, punto 3.1, pag. 7, disponibile al seguente indirizzo: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017DC0007&from=IT>.

- (5) La Commissione ha analizzato attentamente la normativa e la prassi del Regno Unito in materia. Sulla base delle risultanze illustrate in appresso, la Commissione conclude che il Regno Unito garantisce un livello di protezione adeguato per i dati personali trasferiti dalle autorità competenti nell'Unione che rientrano nell'ambito di applicazione della direttiva (UE) 2016/680, alle autorità competenti nel Regno Unito che rientrano nell'ambito di applicazione della parte 3 della legge del 2018 sulla protezione dei dati (*Data Protection Act 2018*) del Regno Unito ⁽⁸⁾.
- (6) Per effetto della presente decisione tali trasferimenti possono avvenire senza la necessità di ottenere ulteriori autorizzazioni per un periodo di quattro anni, rinnovabile, fatte salve le condizioni di cui all'articolo 35 della direttiva (UE) 2016/680.

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

2.1. Il quadro costituzionale

- (7) Il Regno Unito è una democrazia parlamentare. 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 (Camera dei Comuni e *House of Lords*, Camera dei Lord), che sono competenti per l'esame dell'operato del governo nonché per la discussione e l'emanazione delle leggi. Il parlamento del Regno Unito ha delegato al parlamento scozzese, al parlamento gallese (*Senedd Cymru*) e all'assemblea dell'Irlanda del Nord la competenza per legiferare rispettivamente in Scozia, in Galles e in Irlanda del Nord in determinate materie interne. Sebbene la protezione dei dati sia di competenza esclusiva del parlamento del Regno Unito, 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 (le attività esercitate dalle forze di polizia), di Scozia e Irlanda del Nord sono soggetti rispettivamente alla competenza del parlamento scozzese e dell'assemblea dell'Irlanda del Nord ⁽⁹⁾.
- (8) Il Regno Unito non dispone di una costituzione codificata nel senso di un documento costitutivo consolidato: i suoi 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. I diritti fondamentali delle persone fisiche sono stati sviluppati, come parte della costituzione, attraverso la «*common law*» (diritto giurisprudenziale), gli statuti e i trattati internazionali, in particolare la convenzione europea dei diritti dell'uomo (CEDU), 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⁾.
- (9) La legge del 1998 sui diritti umani integra nel diritto del Regno Unito i diritti sanciti dalla 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 da 1 a 3 del suo primo protocollo e all'articolo 1 del suo tredicesimo protocollo, in combinato disposto con gli articoli da 16 a 18 CEDU. Tra di essi è compreso il diritto al rispetto della vita privata e familiare, che a sua volta comprende il diritto alla protezione dei dati, e il diritto a un equo processo ⁽¹¹⁾. In particolare, conformemente all'articolo 8 CEDU, può esservi ingerenza 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.

⁽⁸⁾ Legge del 2018 sulla protezione dei dati, disponibile al seguente indirizzo: <https://www.legislation.gov.uk/ukpga/2018/12/contents>.

⁽⁹⁾ Regno Unito, *Explanatory Framework for Adequacy Discussion, section F: Law enforcement*, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

⁽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 successivamente è stata a sua volta sostituita dalla legge del 2018 sulla protezione dei dati (letta in combinato disposto con il regolamento generale sulla protezione dei dati 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 («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).

- (10) Conformemente alla legge del 1998 sui diritti umani, qualsiasi azione delle autorità pubbliche deve essere compatibile con un diritto sancito dalla CEDU ⁽¹²⁾. Inoltre la legislazione primaria e quella subordinata vanno lette e attuate in maniera compatibile con tali diritti ⁽¹³⁾. Nella misura in cui una persona fisica ritenga che i suoi diritti, compresi quelli relativi alla tutela della vita privata e alla protezione dei dati, siano stati violati dalle autorità pubbliche, può presentare ricorso dinanzi gli organi giurisdizionali del Regno Unito ai sensi della legge del 1998 sui diritti umani e, se del caso, una volta esperiti i mezzi di ricorso nazionali, può presentare ricorso dinanzi alla Corte europea dei diritti dell'uomo per violazione dei diritti sanciti dalla CEDU.

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

- (11) Il Regno Unito ha receduto dall'Unione 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 che disciplinava il trattamento di dati personali da parte delle autorità competenti per fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, compresa la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, era costituito dalle parti pertinenti della legge del 2018 sulla protezione dei dati, che recepisce la direttiva (UE) 2016/680.
- (12) In preparazione al recesso dall'Unione europea, il governo del Regno Unito ha emanato la *European Union (Withdrawal) Act 2018* ⁽¹⁵⁾ (legge del 2018 relativa al recesso dall'Unione europea), che ha incorporato la legislazione dell'Unione direttamente applicabile nel diritto del Regno Unito e ha previsto che la cosiddetta «legislazione interna derivata da quella dell'Unione» continuasse ad avere efficacia dopo la fine del periodo di transizione. La parte 3 della legge del 2018 sulla protezione dei dati ⁽¹⁶⁾ che recepisce la direttiva (UE) 2016/680 costituisce «legislazione interna derivata da quella dell'Unione» nel contesto della legge del 2018 relativa al recesso dall'Unione europea. Conformemente alla legge del 2018 relativa al recesso dall'Unione europea, la «legislazione interna derivata da quella dell'Unione» non modificata deve essere interpretata dagli organi giurisdizionali del Regno Unito in conformità con la relativa giurisprudenza della Corte di giustizia dell'Unione europea (Corte di giustizia) e con i principi generali del diritto dell'Unione così come efficaci immediatamente prima della fine del periodo di transizione (denominati rispettivamente «giurisprudenza dell'UE mantenuta» e «principi generali del diritto dell'UE mantenuti») ⁽¹⁷⁾.
- (13) 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 adottare le modifiche necessarie al diritto dell'Unione mantenuto in conseguenza del recesso del Regno Unito dall'Unione. Essi hanno esercitato tale potere adottando i *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019* (regolamenti DPPEC) ⁽¹⁸⁾, che modificano la legislazione del Regno Unito in materia di protezione dei dati, inclusa la legge del 2018 sulla protezione dei dati, per adattarla al contesto nazionale ⁽¹⁹⁾.

⁽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 384 I del 12.11.2019, pag. 1) («accordo sul recesso»), disponibile al seguente indirizzo: [https://eur-lex.europa.eu/legal-content/ITN/TXT/PDF/?uri=CELEX:12019W/TXT\(02\)&from=IT](https://eur-lex.europa.eu/legal-content/ITN/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=IT).

⁽¹⁵⁾ *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>.

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

⁽¹⁷⁾ Sezione 6 della legge del 2018 relativa al recesso dall'Unione europea.

⁽¹⁸⁾ *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>.

⁽¹⁹⁾ I regolamenti sull'uscita introducono una serie di modifiche alla parte 3 della legge del 2018 sulla protezione dei dati, molte delle quali sono modifiche tecniche quali l'eliminazione dei riferimenti a «Stato membro» o alla «direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie» (cfr. ad esempio sezione 48, paragrafo 8, o sezione 73, paragrafo 5, lettera a), della legge del 2018 sulla protezione dei dati sostituiti con riferimenti al «diritto nazionale»), che rendono la parte 3 funzionante in modo efficace come diritto nazionale dopo la fine del periodo di transizione. In alcuni punti si sono resi necessari altri tipi di modifiche, ad esempio, in relazione al «soggetto» che adotta le «decisioni di adeguatezza» ai fini del quadro normativo del Regno Unito in materia di protezione dei dati (cfr. sezione 74 A della legge del 2018 sulla protezione dei dati), ossia il segretario di Stato anziché la Commissione europea.

- (14) Di conseguenza il quadro giuridico in materia di trattamento dei dati personali da parte delle autorità competenti 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 pubblica nel Regno Unito, dopo il periodo di transizione in virtù dell'accordo di recesso continueranno ad essere stabilite nelle parti pertinenti della legge del 2018 sulla protezione dei dati, ma quale modificata dai regolamenti DPPEC, in particolare nella parte 3 di tale legge. Il regolamento generale sulla protezione dei dati del Regno Unito (GDPR del Regno Unito) non si applica a questo tipo di trattamento.
- (15) La parte 3 della legge del 2018 sulla protezione dei dati definisce le norme per il trattamento di dati personali per finalità di contrasto in materia penale, nonché i principi di protezione dei dati, le basi giuridiche del trattamento (liceità), i diritti degli interessati, gli obblighi delle autorità competenti in qualità di titolari del trattamento e le limitazioni ai trasferimenti successivi. Le norme applicabili in materia di vigilanza, applicazione e ricorso nel settore delle attività di contrasto sono definite nelle parti 5 e 6 della legge del 2018 sulla protezione dei dati.
- (16) Inoltre, alla luce del ruolo pertinente svolto dalle forze di polizia nel settore delle attività di contrasto, è opportuno prendere in considerazione le norme che disciplinano le attività di polizia. Queste ultime, essendo oggetto di delega, sono disciplinate in a) Inghilterra e Galles, b) Scozia e c) Irlanda del Nord da atti legislativi diversi, che tuttavia sono spesso analoghi in termini di contenuti ⁽²⁰⁾. Ulteriori chiarimenti sulle modalità di utilizzo dei poteri della polizia sono forniti da vari tipi di documenti di orientamento, che assumono tre forme principali: 1) gli orientamenti normativi emessi ai sensi della legislazione, quali il Codice etico ⁽²¹⁾ e il *Code of Practice on the Management of Police Information* ⁽²²⁾ («codice di pratica MoPI» adottato in virtù della *Police Act 1996* ⁽²³⁾ (legge del 1996 sulla polizia) o i codici PACE ⁽²⁴⁾ adottati in virtù della *Police and Criminal Evidence Act* ⁽²⁵⁾; 2) *Authorised Professional Practice on the Management of Police Information* (orientamenti APP sulla gestione delle informazioni di polizia) ⁽²⁶⁾, emessi dal *College of Policing*; e 3) gli orientamenti operativi (pubblicati dalla polizia stessa). Il Consiglio nazionale dei capi di polizia (*National Police Chiefs Council*), un organismo di coordinamento per tutte le forze di polizia del Regno Unito, pubblica orientamenti operativi approvati da tutte le forze di polizia e che si applicano pertanto a livello nazionale ⁽²⁷⁾, destinati ad assicurare la coerenza tra le forze di polizia in merito alle modalità di gestione delle informazioni ⁽²⁸⁾.
- (17) Il codice di pratica MoPI è stato pubblicato dal segretario di Stato nel 2005, nell'esercizio dei poteri previsti dalla sezione 39 A della legge del 1996 sulla polizia ⁽²⁹⁾. Ogni codice di pratica emesso ai sensi della legge sulla polizia deve ottenere l'approvazione del segretario di Stato ed è oggetto di consultazione con la *National Crime Agency* prima di essere presentato al parlamento. La sezione 39 A, paragrafo 7, della legge sulla polizia impone alle forze di polizia di tenere in debito conto i codici emessi ai sensi di tale legge, che di conseguenza devono essere rispettati dalla

⁽²⁰⁾ Per una spiegazione più dettagliata sulle forze della polizia e sui loro poteri nel Regno Unito cfr.: *Explanatory Framework for Adequacy Discussion*, section F: *Law enforcement* (cfr. nota 9).

⁽²¹⁾ *The Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales*, disponibile al seguente indirizzo: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; il *Code of Ethics for policing in Scotland*, <https://www.nipolicingboard.org.uk/psni-code-ethics>; il *Police Service Northern Ireland Code of Ethics*, disponibile al seguente indirizzo: <https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/>.

⁽²²⁾ *Code of Practice on the Management of Police Information*, disponibile al seguente indirizzo: <http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf>.

⁽²³⁾ *Police Act 1996*, disponibile al seguente indirizzo: <https://www.legislation.gov.uk/ukpga/1996/16/contents>.

⁽²⁴⁾ Codici PACE (codici relativi alla *Police and Criminal Evidence Act 1984* - legge del 1984 sulle prove nelle attività di polizia e di azione penale — in appresso «legge del 1984 sulle prove»), disponibili al seguente indirizzo: <https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice>.

⁽²⁵⁾ *Police and Criminal Evidence Act 1984*, disponibile al seguente indirizzo: <https://www.legislation.gov.uk/ukpga/1984/60/contents>.

⁽²⁶⁾ *Authorised Professional Practice on the Management of Police Information*, disponibile al seguente indirizzo: <https://www.app.college.police.uk/app-content/information-management/management-of-police-information/>.

⁽²⁷⁾ *Data Protection Manual for Police Data Protection Professionals*, disponibile al seguente indirizzo: <https://www.npcc.police.uk/2019%20FOI/MORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf>.

⁽²⁸⁾ Ad esempio il codice di pratica MoPI (cfr. nota 22) si applica alla conservazione delle informazioni sulle attività operative di polizia (cfr. considerando 47 della presente decisione).

⁽²⁹⁾ Secondo le informazioni fornite dalle autorità del Regno Unito, durante il periodo dei colloqui sull'adeguatezza, il *College of Policing* era in procinto di redigere un codice di pratica sulla gestione di informazioni e registrazioni destinato a sostituire il codice di pratica MoPI. Il progetto di codice è stato pubblicato per la consultazione pubblica il 25 gennaio 2021 ed è disponibile al seguente indirizzo: <https://www.college.police.uk/article/information-records-management-consultation>

polizia⁽³⁰⁾. Inoltre gli orientamenti non normativi (come gli orientamenti sulle pratiche professionali autorizzate in materia di gestione delle informazioni di polizia) devono essere sempre coerenti con il codice di pratica MoPI, che prevale rispetto a essi⁽³¹⁾. Sebbene gli operatori di polizia debbano discostarsi da tali orientamenti in determinate situazioni operative, essi sono comunque tenuti a rispettare le prescrizioni di cui alla parte 3 della legge del 2018 sulla protezione dei dati⁽³²⁾.

- (18) Ulteriori orientamenti sulla legislazione del Regno Unito in materia di protezione dei dati per il trattamento nel settore delle attività di contrasto sono forniti dall'*Information Commissioner* («ICO») ⁽³³⁾, su cui si vedano i considerando da 93 a 109. Sebbene tali orientamenti non siano giuridicamente vincolanti, in una causa giudiziaria gli organi giurisdizionali sarebbero tenuti a prendere in considerazione eventuali loro violazioni, dato che hanno valenza interpretativa e dimostrano come l'ICO interpreti e applichi nella pratica la legislazione in materia di protezione dei dati⁽³⁴⁾.
- (19) Infine, come menzionato nei considerando da 8 a 10, le autorità di contrasto del Regno Unito devono garantire il rispetto della CEDU e della convenzione 108.
- (20) In termini di struttura e componenti principali, il quadro giuridico che disciplina il trattamento dei dati da parte delle autorità di contrasto in materia penale del Regno Unito 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

- (21) L'ambito di applicazione materiale della parte 3 della legge del 2018 sulla protezione dei dati coincide con l'ambito di applicazione della direttiva (UE) 2016/680 quale specificato nell'articolo 2, paragrafo 2, di quest'ultima. La parte 3 si applica al trattamento interamente o parzialmente automatizzato dei dati personali da parte di un'autorità competente, così come al trattamento da parte di un'autorità competente di dati personali che sono contenuti, o destinati a essere contenuti, in un archivio, con mezzi diversi da quelli automatizzati.
- (22) Inoltre, per rientrare nell'ambito di applicazione della parte 3 il titolare del trattamento deve essere un'«autorità competente» e il trattamento deve essere svolto per una «finalità di contrasto». Di conseguenza, il regime di protezione dei dati valutato nella presente decisione si applica a tutte le attività di contrasto svolte da tali autorità competenti.
- (23) A norma 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 qualsiasi finalità di contrasto. 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*, *Welsh Revenue Authority*, *Competition and Markets Authority*, *Her Majesty's Land Register* o *National Crime Agency*), le procure, altri organi di giustizia penale e altri titolari od organizzazioni che svolgono attività di

⁽³⁰⁾ Nella causa *R v the Commission of Police of the Metropolis* [2014], EWCA (England and Wales Court of Appeal, Corte d'appello di Inghilterra e Galles) Civ 585, è stato confermato lo status giuridico del codice di pratica MoPI e il giudice Laws ha dichiarato che la *Commission of Police of the Metropolis* era tenuta a prendere in considerazione tale codice e gli orientamenti sulle pratiche professionali autorizzate in materia di gestione delle informazioni di polizia ai sensi della sezione 39 A della legge del 1996 sulla polizia.

⁽³¹⁾ Le forze di polizia sono soggette a ispezioni da parte dell'*Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services* (HMICFRS) in merito al rispetto da parte loro del codice di pratica MoPI.

⁽³²⁾ A tale riguardo cfr. la posizione del *College of Policing* in merito al rispetto degli orientamenti sulle pratiche professionali autorizzate in relazione a tutti gli elementi delle attività di polizia, che spiega che tali «orientamenti sono autorizzati dall'organo professionale per le attività di polizia (il *College of Policing*) come fonte ufficiale di pratiche professionali in materia di attività di polizia. I funzionari e il personale di polizia devono tener conto di tali orientamenti nello svolgimento delle attività di loro competenza. In talune circostanze, tuttavia, le forze di polizia possono deviare dalle pratiche professionali autorizzate per una motivazione operativa legittima, purché vi sia una logica evidente per procedere in tal senso. Spetta alla forza di polizia in questione farsi carico della responsabilità di qualsiasi rischio locale e nazionale legato all'operare al di fuori degli orientamenti concordati a livello nazionale e, qualora si verifichi un incidente o sia svolta un'indagine a seguito di tale scostamento (ad esempio da parte dell'*Independent Office of Police Conduct*), detta forza di polizia è responsabile per qualsiasi rischio. Informazioni disponibili al seguente indirizzo: <https://www.app.college.police.uk/faq-page/>.

⁽³³⁾ *Guide to Law Enforcement Processing*, disponibile al seguente indirizzo: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/>.

⁽³⁴⁾ Cfr. causa *Bridges v the Chief Constable of South Wales Police* [2019] EWHC (England and Wales High Court, Alta Corte di Inghilterra e Galles) 2341 (Admin), nel contesto della quale, pur rilevando la natura non legislativa degli orientamenti dell'ICO, l'Alta Corte ha dichiarato che «[n]el valutare se un titolare del trattamento abbia o meno rispettato l'obbligo di cui alla sezione 64 [effettuare una valutazione d'impatto sulla protezione dei dati in relazione a un trattamento soggetto a rischio elevato], un organo giurisdizionale dovrà prendere in considerazione gli orientamenti emessi dall'ICO in relazione alle valutazioni d'impatto sulla protezione dei dati».

contrasto⁽³⁵⁾. La parte 3 della legge del 2018 sulla protezione dei dati si applica anche agli organi giurisdizionali quando esercitano le loro funzioni giudiziarie, fatta eccezione per la parte relativa ai diritti degli interessati e alla vigilanza da parte dell'ICO⁽³⁶⁾. L'elenco delle autorità competenti fornito dall'allegato 7 non è definitivo e può essere aggiornato dal segretario di Stato mediante regolamenti tenendo conto delle modifiche dell'organizzazione degli uffici pubblici⁽³⁷⁾.

- (24) Il trattamento in questione deve inoltre avvenire per una «finalità di contrasto», definita come la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, compresa la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica⁽³⁸⁾. Il trattamento da parte di un'autorità competente non è regolamentato dalla parte 3 della legge del 2018 sulla protezione dei dati laddove non sia svolto per finalità di contrasto. Ciò si verifica ad esempio quando la *Competition and Markets Authority*, l'autorità del Regno Unito per la concorrenza e i mercati, indaga in merito a casi che non si qualificano come reato (ad esempio fusioni tra imprese). In tal caso si applicherà il GDPR del Regno Unito, unitamente alla parte 2 della legge del 2018 sulla protezione dei dati, dato che il trattamento dei dati personali da parte delle autorità competenti è svolto per finalità diverse da quelle di contrasto. Ai fini della determinazione del regime di protezione applicabile (parte 3 o parte 2 della legge del 2018 sulla protezione dei dati) al trattamento dei dati personali in questione, l'autorità competente, ossia il titolare del trattamento, deve considerare se la «finalità primaria» di tale trattamento sia una delle finalità di contrasto previste dalla legge del 2018 sulla protezione dei dati.
- (25) Per quanto concerne l'ambito di applicazione territoriale della parte 3 della legge del 2018 sulla protezione dei dati, la sezione 207, paragrafo 2, prevede che tale legge si applichi al trattamento dei dati personali nel contesto delle attività di una persona stabilita nel territorio del Regno Unito. Rientrano in tale contesto le autorità pubbliche dei territori di Inghilterra, Galles, Scozia e Irlanda del Nord soggette all'ambito di applicazione materiale della parte 3 della legge del 2018 sulla protezione dei dati⁽³⁹⁾.

2.3.1. Definizione di dati personali e trattamento

- (26) I concetti chiave di «dati personali» e «trattamento» sono definiti dalla sezione 3 della legge del 2018 sulla protezione dei dati e si applicano in tutto il testo di tale legge. Le definizioni seguono da vicino le definizioni corrispondenti di cui all'articolo 3 della direttiva (UE) 2016/680. Ai sensi della legge del 2018 sulla protezione dei dati, per dato personale si intende qualsiasi informazione relativa a una persona fisica vivente identificata o identificabile⁽⁴⁰⁾. Ai sensi della sezione 3, paragrafo 3, della legge del 2018 sulla protezione dei dati, una persona fisica è identificabile se può essere identificata direttamente o indirettamente in base alle informazioni, anche mediante riferimento a un nome o un identificatore o a uno o più fattori specifici del suo aspetto fisico o del suo stato fisiologico, genetico, mentale, economico, culturale oppure della sua identità sociale. Per «trattamento» si intende un'operazione o un insieme di operazioni compiute su informazioni o su serie di informazioni, quali: a) la raccolta, la registrazione, l'organizzazione, la strutturazione o la conservazione; b) l'adattamento o la modifica; c) l'estrazione, la consultazione, l'uso; d) la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione; e) il raffronto o l'interconnessione; o f) la limitazione, la cancellazione o la distruzione. Tale legge definisce inoltre il «trattamento di dati sensibili» come a) il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale; b) il trattamento di dati genetici, o di dati biometrici, al fine di identificare in modo univoco una persona fisica; c) il trattamento di dati relativi alla salute; d) il trattamento di dati relativi alla vita sessuale o all'orientamento sessuale della persona fisica⁽⁴¹⁾. A tale riguardo la sezione 205 della legge del 2018 sulla protezione dei dati fornisce la definizione di «dati biometrici»⁽⁴²⁾, «dati relativi alla salute»⁽⁴³⁾ e «dati genetici»⁽⁴⁴⁾.

⁽³⁵⁾ 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*.

⁽³⁶⁾ Sezione 43, paragrafo 3, della legge del 2018 sulla protezione dei dati.

⁽³⁷⁾ Sezione 30, paragrafo 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 (cfr. sezione 30, paragrafo 2, della legge del 2018 sulla protezione dei dati) e la parte 3 della legge del 2018 sulla protezione dei dati non si applica ad alcuna delle loro attività. Le loro attività rientrano nell'ambito di applicazione della parte 4 della legge del 2018 sulla protezione dei dati.

⁽³⁸⁾ Sezione 31 della legge del 2018 sulla protezione dei dati.

⁽³⁹⁾ Di conseguenza la legge del 2018 sulla protezione dei dati, e pertanto la presente decisione, non si applica alle dipendenze della Corona del Regno Unito e agli altri territori britannici d'oltremare, ad esempio le isole Falkland e il territorio di Gibilterra.

⁽⁴⁰⁾ I dati personali relativi a una persona deceduta non rientrano nell'ambito di applicazione della legge del 2018 sulla protezione dei dati.

⁽⁴¹⁾ Sezione 35, paragrafo 8, della legge del 2018 sulla protezione dei dati.

⁽⁴²⁾ Per «dati biometrici» si intende 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.

⁽⁴³⁾ Per «dati relativi alla salute» si intende 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.

⁽⁴⁴⁾ Per «dati genetici» si intende 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.

- (27) La sezione 32 della legge del 2018 sulla protezione dei dati contiene le definizioni di «titolare del trattamento» e «responsabile del trattamento» nel contesto del trattamento di dati personali per finalità di contrasto, che rispecchiano in larga misura le definizioni equivalenti contenute nella direttiva (UE) 2016/680. Il «titolare del trattamento» è l'autorità competente per stabilire le finalità e i mezzi del trattamento dei dati personali. Se il trattamento è imposto per legge, il titolare del trattamento è l'autorità competente a cui tale obbligo è imposto dalla legge in questione. Il responsabile del trattamento è la persona che tratta dati personali per conto del titolare del trattamento (diversa da un dipendente del titolare del trattamento).

2.4. Garanzie, diritti e obblighi

2.4.1. Liceità e correttezza del trattamento

- (28) La sezione 35 della legge del 2018 sulla protezione dei dati stabilisce che il trattamento dei dati personali deve essere lecito e corretto, in maniera analoga a quanto stabilito dall'articolo 4, paragrafo 1, lettera a), della direttiva (UE) 2016/680. Conformemente alla sezione 35, paragrafo 2, della legge del 2018 sulla protezione dei dati, il trattamento di dati personali per qualsiasi finalità di contrasto è lecito soltanto se si basa sulla legge e se l'interessato ha prestato il proprio consenso al trattamento per tale finalità, oppure se è necessario per lo svolgimento di uno dei compiti esercitati da un'autorità competente per tale finalità.

2.4.1.1. Trattamento sulla base di disposizioni legislative

- (29) Analogamente a quanto stabilito dall'articolo 8 della direttiva (UE) 2016/680, al fine di garantire la liceità di un trattamento che rientra nell'ambito di applicazione della parte 3 della legge del 2018 sulla protezione dei dati, tale trattamento deve essere effettuato «sulla base di disposizioni legislative». Per trattamento «lecito» si intende un trattamento autorizzato da una legge, dalla «common law» o da prerogative reali ⁽⁴⁵⁾.
- (30) I poteri delle autorità competenti sono in generale disciplinati da statuti, il che significa che le loro funzioni e i loro poteri sono definiti chiaramente negli atti legislativi adottati dal parlamento ⁽⁴⁶⁾. In alcuni casi la polizia, così come altre autorità competenti elencate nell'allegato 7 della legge del 2018 sulla protezione dei dati, può basarsi sulla «common law» per il trattamento di dati ⁽⁴⁷⁾. La «common law» si è sviluppata mediante precedenti stabiliti attraverso decisioni degli organi giurisdizionali ed è rilevante nel contesto dei poteri a disposizione della polizia che derivano da tale fonte di diritto il loro dovere principale di proteggere il pubblico accertando e prevenendo i reati ⁽⁴⁸⁾. Per esercitare tale dovere, la polizia dispone

⁽⁴⁵⁾ Note esplicative sulla legge del 2018 sulla protezione dei dati, punto 181, disponibili al seguente indirizzo: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

⁽⁴⁶⁾ La *National Crime Agency* deriva ad esempio i propri poteri dalla *Crime and Courts Act 2013* (legge del 2013 sui reati e sugli organi giurisdizionali), disponibile al seguente indirizzo: <https://www.legislation.gov.uk/ukpga/2013/22/contents>. Analogamente, i poteri della *Food Standards Agency* sono previsti dalla *Food Standards Act 1999* (legge del 1999 sulle norme in materia di alimenti), disponibile al seguente indirizzo: <https://www.legislation.gov.uk/ukpga/1999/28/contents>. Ulteriori esempi comprendono la *Prosecution of Offenders Act 1985* (legge del 1985 sulle azioni giudiziarie contro gli autori di reati) che ha istituito il *Crown Prosecution Service* (cfr. <https://www.legislation.gov.uk/ukpga/1985/23/contents>); la *Commissioners for Revenue and Customs Act 2005* (legge del 2005 che sui commissari per le entrate e le dogane) che ha istituito l'*Her Majesty's Revenue and Customs* (cfr. <https://www.legislation.gov.uk/ukpga/2005/11/contents>); la *Criminal Procedure (Scotland) Act 1995* (legge del 1995 sulla procedura penale — Scozia), che ha istituito la *Scottish Criminal Cases Review Commission* (cfr. <https://www.legislation.gov.uk/ukpga/1995/46/contents>); la *Justice (Northern Ireland) Act 2002* (legge del 2002 sulla giustizia — Irlanda del Nord), che ha istituito l'Ufficio del pubblico ministero in Irlanda del Nord (cfr. <https://www.legislation.gov.uk/ukpga/2002/26/contents>), mentre il *Serious Fraud Office* è stato istituito dalla *Criminal Justice Act 1987* (legge del 1987 sulla giustizia penale) che ne stabilisce anche i poteri (cfr. <https://www.legislation.gov.uk/ukpga/1987/38/contents>).

⁽⁴⁷⁾ Ad esempio secondo le informazioni fornite dalle autorità del Regno Unito, all'interno del *Crown Office and Procurator Fiscal Service* (Ufficio del pubblico ministero scozzese), competente per le azioni giudiziarie in Scozia, il *Lord Advocate* (Avvocato di Sua Maestà), che è a capo del sistema dei pubblici ministeri in Scozia, deriva i propri poteri per indagare in merito a decessi e per perseguire reati dalla «common law», mentre alcune delle sue funzioni sono stabilite dalla legge ordinaria. Inoltre la Corona e, per estensione, varie amministrazioni e vari dipartimenti e ministri, derivano anch'essi i loro poteri da una combinazione di legislazione, «common law» e prerogative reali (in quest'ultimo caso si tratta di poteri sanciti dalla «common law» conferiti alla Corona, ma esercitati dai ministri).

⁽⁴⁸⁾ Regno Unito, *Explanatory Framework for Adequacy Discussion, section F: Law enforcement*, pag. 8 (cfr. nota 9).

in ogni caso di poteri conferiti sia dalla «common law» che dalle leggi ⁽⁴⁹⁾. Laddove la polizia disponga di un potere basato sulla legge ordinaria, tale potere prevale su qualsiasi potere derivante dalla «common law» ⁽⁵⁰⁾.

- (31) Gli organi giurisdizionali hanno riconosciuto che la portata dei poteri e degli obblighi di un operatore di polizia sanciti dalla «common law» include «tutte le misure che gli sembrano necessarie per mantenere la pace, prevenire i reati e proteggere i beni da azioni lesive criminali» ⁽⁵¹⁾. I poteri derivanti dalla «common law» non sono poteri illimitati; sono soggetti a una serie di limitazioni, stabilite fra l'altro dagli organi giurisdizionali ⁽⁵²⁾ e dalla legislazione, in particolare dalla legge del 1998 sui diritti umani e dalla *Equality Act 2010* ⁽⁵³⁾ (legge del 2010 sulla parità). Per le autorità competenti che trattano dati in virtù della parte 3 della legge del 2018 sulla protezione dei dati, ciò implica l'obbligo di esercitare i poteri derivanti dalla «common law» in maniera coerente con le disposizioni della legge del 2018 sulla protezione dei dati ⁽⁵⁴⁾. La decisione di svolgere qualsiasi tipo di trattamento di dati deve inoltre tenere conto dei requisiti stabiliti negli orientamenti applicabili, come il codice di pratica MoPI e gli orientamenti specifici di uno dei paesi del Regno Unito ⁽⁵⁵⁾. Alcuni documenti di orientamento sono emessi dal governo e da servizi di polizia operativa con l'obiettivo di garantire che gli operatori di polizia esercitino le loro competenze di trattamento entro i limiti stabiliti dalla «common law» o dalla legge ordinaria pertinente ⁽⁵⁶⁾.
- (32) Le prerogative reali rappresentano un'altra componente della «legge» e fanno riferimento a determinati poteri conferiti alla Corona ed esercitabili dal potere esecutivo che non si basano sulla legge ordinaria, bensì derivano dalla sovranità del monarca ⁽⁵⁷⁾. Sono rarissimi gli esempi di poteri di questo tipo pertinenti nel contesto delle attività di contrasto. Tra essi figurano, ad esempio, il quadro di mutua assistenza giudiziaria che consente la condivisione di dati da parte di un segretario di Stato con paesi terzi per finalità di contrasto; il potere di condividere i dati in questo

⁽⁴⁹⁾ Gli atti legislativi principali che definiscono il regime in merito ai principali poteri di polizia (arresto, perquisizione, autorizzazione al perdurare della detenzione, acquisizione di impronte digitali, assunzione di campioni intimi, intercettazione su mandato, accesso ai dati relativi alle comunicazioni) sono: i) per Inghilterra e Galles, la legge del 1984 sulle prove nelle attività di polizia e di azione penale (PACE), disponibile all'indirizzo <https://www.legislation.gov.uk/ukpga/1984/60/contents>, come modificata dalla *Protection of Freedoms Act 2012* (PoFA) (legge del 2012 sulla protezione delle libertà), disponibile all'indirizzo <https://www.legislation.gov.uk/ukpga/2012/9/contents> e la *Investigatory Powers Act 2016* (IPA, legge del 2016 sui poteri di indagine), disponibile all'indirizzo <https://www.legislation.gov.uk/ukpga/2016/25/contents>; ii) per la Scozia, la *Criminal Justice (Scotland) Act 2016* (legge del 2016 sulla giustizia penale - Scozia), disponibile all'indirizzo <https://www.legislation.gov.uk/asp/2016/1/contents>, e la *Criminal Procedure (Scotland) Act 1995* (legge del 1995 sulla procedura penale - Scozia), disponibile all'indirizzo <https://www.legislation.gov.uk/ukpga/1995/46/contents>; iii) per l'Irlanda del Nord, la *Police and Criminal Evidence (Northern Ireland) Order 1989* (ordinanza del 1989 sulle prove nelle attività di polizia e di azione penale - Irlanda del Nord), disponibile all'indirizzo <https://www.legislation.gov.uk/nisi/1989/1341/contents>.

⁽⁵⁰⁾ Le autorità del Regno Unito hanno spiegato che la supremazia della legge ordinaria è una lunga tradizione nel Regno Unito, che risale fino alla sentenza *Entick v Carrington* [1765] EWHC KB 98, nella quale è stato riconosciuto che vi erano dei limiti all'esercizio dei poteri da parte del potere esecutivo; tale sentenza ha infatti stabilito il principio secondo il quale i poteri sanciti dalla «common law» e i poteri derivanti da prerogative del monarca e del governo sono subordinati alla legge del paese.

⁽⁵¹⁾ Cfr. causa *Rice v Connolly* [1966] 2 QB 414.

⁽⁵²⁾ Cfr. causa *R(Catt) v Association of Chief Police Officers* [2015] AC 1065, nella quale in relazione al potere della polizia di ottenere e conservare informazioni in merito a una persona fisica (che ha commesso un reato), il giudice Sumption ha ritenuto che secondo la «common law» la polizia abbia il potere di ottenere e conservare informazioni per finalità relative ad attività di polizia, ossia in generale per il mantenimento dell'ordine pubblico e la prevenzione e l'accertamento di reati. Tale potere non autorizza metodi intrusivi di ottenimento delle informazioni, quali l'accesso a una proprietà privata o atti (diversi da un arresto in conformità con i poteri sanciti dalla «common law») che costituirebbero un'aggressione. Il giudice ha ritenuto che, nel caso di specie, i poteri sanciti dalla «common law» fossero ampiamente sufficienti per autorizzare l'ottenimento e la conservazione della tipologia di informazioni pubbliche in questione su tali ricorsi.

⁽⁵³⁾ *Equality Act 2010*, disponibile al seguente indirizzo: <https://www.legislation.gov.uk/ukpga/2010/15/contents>.

⁽⁵⁴⁾ Per un esempio di una causa nella quale i poteri della polizia sanciti dalla «common law» sono valutati nel quadro della legge del 1998 sulla protezione dei dati, cfr. la decisione dell'Alta Corte nella causa *Bridges v the Chief Constable of South Wales Police* (cfr. nota 33). Cfr. anche le cause *Vidal-Hall v Google Inc* [2015] EWCA Civ 311 e *Richard v BBC* [2018] EWHC 1837 (Ch).

⁽⁵⁵⁾ Cfr. ad esempio gli orientamenti del servizio di polizia dell'Irlanda del Nord in merito all'istruzione di servizio sulla gestione di registrazioni, disponibili al seguente indirizzo: <https://www.psn.police.uk/globalassets/advice-information/our-publications/policies-and-service-procedures/records-management-080819.pdf>.

⁽⁵⁶⁾ La Camera dei Comuni ha pubblicato un documento informativo che espone i principali poteri attribuiti dalla «common law» e dalla legge ordinaria alle forze di polizia in Inghilterra e in Galles (cfr. <https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf>). Secondo tale documento, ad esempio, mentre i poteri di mantenimento della «pace della Corona» sono un potere derivato dalla «common law», l'uso della forza e i poteri di fermo e perquisizione sono sempre derivati dalla legge ordinaria. Inoltre il governo scozzese offre informazioni sul proprio sito web in merito ai poteri della polizia in materia di arresto, fermo e perquisizione (cfr. <https://www.gov.scot/policies/police/police-powers/>).

⁽⁵⁷⁾ Secondo le informazioni fornite dalle autorità del Regno Unito, i poteri di prerogativa esercitati dal governo comprendono ad esempio la realizzazione e la ratifica di trattati, le attività di diplomazia, e l'uso delle forze armate all'interno del Regno Unito per mantenere la pace a sostegno delle forze di polizia.

modo non è sempre stabilito dalla legge ordinaria ⁽⁵⁸⁾. Le prerogative reali sono vincolate dai principi della «common law» ⁽⁵⁹⁾ e sono subordinate alla legge ordinaria, e di conseguenza soggette alle limitazioni previste dalla legge del 1998 sui diritti umani e dalla legge del 2018 sulla protezione dei dati ⁽⁶⁰⁾.

- (33) Analogamente all'articolo 8 della direttiva (UE) 2016/680, il regime del Regno Unito impone alle autorità competenti, al fine di rispettare il principio di liceità, di assicurare che, quando il trattamento si basa su disposizioni legislative, sia anche «necessario» per svolgere il compito effettuato per finalità di contrasto. L'ICO fornisce orientamenti a questo proposito chiarendo che il trattamento deve costituire un modo mirato e proporzionato di conseguire la finalità. La base legittima non si applica se è possibile conseguire ragionevolmente la finalità impiegando altri mezzi meno intrusivi. Non è sufficiente sostenere che il trattamento è necessario perché si è deciso di svolgere le proprie attività in un determinato modo. Occorre appurare se il trattamento sia necessario per la finalità dichiarata ⁽⁶¹⁾.

2.4.1.2. Trattamento sulla base del «consenso» dell'interessato

- (34) Come menzionato al considerando 28, la sezione 35, paragrafo 2, della legge del 2018 sulla protezione dei dati prevede la possibilità di trattare dati personali sulla base del «consenso» della persona fisica.
- (35) Tuttavia il consenso non sembra essere una base giuridica pertinente per le operazioni di trattamento che rientrano nell'ambito di applicazione della presente decisione, le quali riguarderanno sempre dati trasferiti a norma della direttiva (UE) 2016/680 da un'autorità competente di uno Stato membro a un'autorità competente del Regno Unito. Di conseguenza, in genere esse non comporteranno il tipo di interazione diretta (raccolta) tra un'autorità pubblica e gli interessati che può essere basata sul consenso ai sensi della sezione 35, paragrafo 2, lettera a), della legge del 2018 sulla protezione dei dati.
- (36) Sebbene il ricorso al consenso non sia quindi considerato pertinente ai fini della valutazione condotta nel contesto della presente decisione, vale la pena sottolineare, per ragioni di completezza, che, in un contesto di contrasto, il trattamento non si fonda mai esclusivamente sul consenso, dato che l'autorità competente deve disporre sempre di un potere di base che le consente di trattare i dati ⁽⁶²⁾. Nello specifico, e analogamente a quanto autorizzato a norma della direttiva (UE) 2016/680 ⁽⁶³⁾, ciò significa che il consenso è una condizione aggiuntiva per consentire alcuni trattamenti limitati e specifici che non potrebbero essere svolti altrimenti, ad esempio la raccolta e il trattamento di un campione di DNA di una persona fisica che non è un indiziato: in tal caso il trattamento non può essere effettuato in assenza di consenso o in caso di revoca di tale consenso ⁽⁶⁴⁾.

⁽⁵⁸⁾ A tale riguardo, cfr. la valutazione del regime di trasferimento successivo del Regno Unito di cui ai considerando da 74 a 87.

⁽⁵⁹⁾ Cfr. causa *Bancoult v Secretary of State for Foreign and Commonwealth Affairs* [2008] UKHL 61 nel contesto della quale l'organo giurisdizionale ha ritenuto che anche il potere di emettere ordinanze in seno al consiglio fosse soggetto ai motivi ordinari di controllo giurisdizionale.

⁽⁶⁰⁾ Cfr. causa *Attorney-General v De Keyser's Royal Hotel Ltd* [1920] [1920] AC 508 nel contesto della quale l'organo giurisdizionale ha ritenuto che i poteri di prerogativa non possano essere esercitati quando sono sostituiti da poteri sanciti dalla legge ordinaria; causa *Laker Airways Ltd v Department of Trade* [1977] QB 643, nel contesto della quale l'organo giurisdizionale ha constatato che i poteri di prerogativa non possono essere esercitati per invalidare la legge ordinaria; causa *R v Secretary of State for the Home Department, ex p. Fire Brigades Union* [1995] UKHL 3 nel contesto della quale l'organo giurisdizionale ha ritenuto che i poteri di prerogativa non possano essere esercitati quando sono in conflitto con la legislazione emanata, anche quando quest'ultima non è ancora in vigore; causa *R (Miller) v Secretary of State for Exiting the European Union* [2017] UKSC 5 nel contesto della quale l'organo giurisdizionale ha confermato la capacità da parte del diritto ordinario di adeguare e abolire i poteri di prerogativa. Per una panoramica generale della relazione tra le prerogative reali e i poteri derivanti dalla legge ordinaria o dalla «common law», si rimanda al documento informativo della Camera dei Comuni disponibile al seguente indirizzo: <https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf>.

⁽⁶¹⁾ *Guide to Law Enforcement Processing*, «What is the first principle about?», disponibile al seguente indirizzo: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2>.

⁽⁶²⁾ Ciò si evince dalla formulazione della disposizione pertinente della legge del 2018 sulla protezione dei dati, secondo la quale il trattamento dei dati personali per una finalità di contrasto è lecito soltanto se e nella misura in cui «si basa sulla legge» e a) l'interessato ha prestato il proprio consenso al trattamento per tale finalità oppure b) il trattamento è necessario per l'esecuzione di un compito svolto per tale finalità da un'autorità competente».

⁽⁶³⁾ Cfr. considerando 35 e 37 della direttiva (UE) 2016/680.

⁽⁶⁴⁾ Le autorità del Regno Unito hanno addotto come caso esemplare in cui il consenso potrebbe costituire una base adeguata per il trattamento quello in cui la polizia ottiene un campione di DNA in relazione a una persona scomparsa da confrontare con un cadavere eventualmente trovato. In tali circostanze, sarebbe inappropriato per la polizia costringere l'interessato a fornire un campione; la polizia, piuttosto, chiederebbe il consenso dell'interessato, che dovrebbe essere concesso liberamente e potrebbe essere revocato in qualsiasi momento. In caso di revoca del consenso, i dati non potrebbero più essere trattati, fatto salvo il caso in cui si stabilisca una nuova base giuridica per continuare a trattare il campione (ad esempio se l'interessato è diventato un indiziato). Un ulteriore esempio riguarda il caso in cui le forze di polizia indagano in merito a un reato nel contesto del quale una vittima (potrebbe trattarsi di una vittima di rapina, di un reato sessuale, di violenza domestica, di parenti di una vittima di omicidio o altre vittime di un reato) potrebbe beneficiare del riferimento a un ente di sostegno alle vittime (un ente di beneficenza indipendente dedicato a fornire sostegno alle persone vittime di reati e di incidenti traumatici). In tali circostanze, la polizia condirebbe con l'ente di sostegno alle vittime informazioni personali quali il nome e i dati di contatto soltanto se dispone del consenso della vittima.

- (37) Nei casi che richiedono il consenso della persona fisica, tale consenso deve essere inequivocabile e comportare una chiara azione positiva ⁽⁶⁵⁾. Le forze di polizia sono tenute a disporre di un'informativa sulla protezione dei dati che comprenda tra l'altro le informazioni necessarie per il valido utilizzo del consenso. Inoltre alcune di esse pubblicano materiale aggiuntivo su come rispettano la legislazione in materia di protezione dei dati, nonché sulle modalità e sui casi in cui ricorrono al consenso come base giuridica ⁽⁶⁶⁾.

2.4.1.3. Trattamento di dati sensibili

- (38) Garanzie specifiche dovrebbero essere applicate al trattamento di «categorie particolari» di dati. A tale riguardo, analogamente a quanto previsto dall'articolo 10 della direttiva (UE) 2016/680, la parte 3 della legge del 2018 sulla protezione dei dati offre garanzie più rigorose per il cosiddetto «trattamento di dati sensibili» ⁽⁶⁷⁾.
- (39) Conformemente alla sezione 35, paragrafo 3, della legge del 1998 sulla protezione dei dati, i dati sensibili possono essere trattati dalle autorità competenti per finalità di contrasto soltanto in due casi: 1) l'interessato ha prestato il consenso al trattamento per la finalità di contrasto e, nel momento in cui viene effettuato il trattamento, il titolare del trattamento dispone di un documento adeguato di informativa in merito ⁽⁶⁸⁾; oppure 2) il trattamento è strettamente necessario per la finalità di contrasto, il trattamento soddisfa almeno una delle condizioni di cui all'allegato 8 della legge del 2018 sulla protezione dei dati e al momento dello svolgimento del trattamento il titolare del trattamento dispone di un documento adeguato di informativa in merito ⁽⁶⁹⁾.
- (40) Per quanto concerne il primo caso e come spiegato al considerando 38, il ricorso al consenso non è considerato rilevante nel tipo di situazione di trasferimento oggetto della presente decisione ⁽⁷⁰⁾.
- (41) Quando il trattamento di dati sensibili non si basa sul consenso, può essere effettuato ricorrendo a una delle condizioni di cui all'allegato 8 della legge del 2018 sulla protezione dei dati. Tali condizioni si riferiscono a quanto segue: trattamento necessario per finalità previste dalla legge ordinaria; amministrazione della giustizia; tutela degli interessi vitali dell'interessato o di un'altra persona fisica; tutela di minori o di persone fisiche a rischio; diritti fatti valere in sede giudiziaria; atti giudiziari; prevenzione di frodi; archiviazione; casi nei quali i dati personali sono manifestamente resi pubblici dall'interessato. Fatta eccezione per il caso in cui i dati siano manifestamente resi pubblici, tutte le condizioni di cui all'allegato 8 sono soggette a una verifica dell'«effettiva necessità». Come chiarito

⁽⁶⁵⁾ Non vi è alcuna definizione distinta di «consenso» ai fini del trattamento dei dati personali nella parte 3 della legge del 2018 sulla protezione dei dati. L'ICO ha fornito orientamenti sul concetto di «consenso» ai sensi della parte 3 della legge del 2018 sulla protezione dei dati, in cui si chiarisce che tale termine ha il medesimo significato e dovrebbe essere allineato con la definizione fornita dal GDPR, in particolare «il consenso deve manifestare l'intenzione libera, specifica e informata nonché una scelta autentica ad acconsentire al trattamento dei dati personali» (*Guide to Law Enforcement Processing*, «What is the first principle about?» — cfr. nota 64 — e *Guide to Data Protection on consent*, disponibile al seguente indirizzo: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>).

⁽⁶⁶⁾ Cfr. ad esempio le informazioni fornite sulla pagina web della polizia del Lincolnshire (<https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/>) o sulla pagina web della polizia del West Yorkshire (https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

⁽⁶⁷⁾ Sezione 35, paragrafo 8, della legge del 2018 sulla protezione dei dati.

⁽⁶⁸⁾ Sezione 35, paragrafo 4, della legge del 2018 sulla protezione dei dati.

⁽⁶⁹⁾ Sezione 35, paragrafo 5, della legge del 2018 sulla protezione dei dati.

⁽⁷⁰⁾ Per ragioni di completezza vale la pena sottolineare che, se il trattamento si basa sul consenso, quest'ultimo deve essere manifestato liberamente, essere specifico e informato e deve manifestare una scelta specifica ad acconsentire al trattamento dei dati. Durante il trattamento sulla base del consenso dell'interessato, il titolare del trattamento è altresì tenuto a disporre di un «documento adeguato di informativa». La sezione 42 della legge del 2018 sulla protezione dei dati definisce i requisiti che tale documento deve soddisfare. Tale disposizione chiarisce che il documento deve quanto meno spiegare le procedure attuate dal titolare del trattamento per assicurare il rispetto dei principi di protezione dei dati nonché le politiche di tale titolare del trattamento in materia di conservazione e cancellazione dei dati personali. Conformemente alla sezione 42 della legge del 2018 sulla protezione dei dati, ciò significa che il titolare del trattamento deve produrre un documento che: a) spieghi le procedure attuate dal titolare del trattamento per assicurare il rispetto dei principi di protezione dei dati; e b) spieghi le politiche del titolare del trattamento per quanto concerne la conservazione e la cancellazione dei dati personali trattati basandosi sul consenso dell'interessato o fornendo un'indicazione del termine probabile di conservazione di tali dati personali. In particolare il documento di informativa richiede che il titolare del trattamento, nel rispettare il proprio dovere di registrazione delle attività di trattamento, includa sempre gli elementi di cui ai punti a) e b). L'ICO ha pubblicato un documento modello (*Guide to Law Enforcement Processing*, «Conditions for sensitive processing», disponibile al seguente indirizzo: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing/>) e può intraprendere un'azione di contrasto nel caso in cui i titolari del trattamento non rispettino tali requisiti. Il documento adeguato di informativa viene altresì esaminato dagli organi giurisdizionali nelle loro valutazioni in merito a potenziali violazioni della legge del 2018 sulla protezione dei dati. Ad esempio nella recente causa di *R (Bridges) v Chief Constable of South Wales Police*, l'organo giurisdizionale ha esaminato il documento adeguato di informativa del titolare del trattamento e ha riscontrato che era appropriato, ma avrebbe tratto beneficio dall'aggiunta di ulteriori dettagli. Di conseguenza la polizia del Galles meridionale ha rivisto il documento adeguato di informativa e l'ha aggiornato in linea con la nuova guida ICO (cfr. nota 33). Inoltre, ai sensi della sezione 42, paragrafo 3, della legge del 2018 sulla protezione dei dati, il documento adeguato di informativa dovrebbe essere sottoposto a un esame periodico da parte del titolare del trattamento. Infine, come garanzia supplementare, ai sensi della sezione 42, paragrafo 4, della legge del 2018 sulla protezione dei dati, il titolare del trattamento è tenuto a mantenere un registro consolidato dei trattamenti, che prevede elementi aggiuntivi rispetto all'obbligo generale in capo al titolare del trattamento di tenere registri dei trattamenti di cui alla sezione 61 della legge del 2018 sulla protezione dei dati.

dall'ICO, in questo contesto il concetto di «effettiva necessità» significa che il trattamento deve riguardare un'urgente esigenza sociale che non può essere ragionevolmente soddisfatta ricorrendo a mezzi meno intrusivi ⁽⁷¹⁾. Alcune condizioni sono inoltre soggette a limitazioni aggiuntive. Ad esempio, per invocare la condizione delle «finalità statutarie» e la condizione di «tutela» (allegato 8, paragrafi 1 e 4) occorre che sia effettuata un'ulteriore verifica dell'interesse pubblico sostanziale. Inoltre, per quanto riguarda le condizioni relative alla tutela di minori (allegato 8, paragrafo 4) l'interessato deve avere altresì un'età specifica ed essere considerato a rischio. Inoltre il titolare del trattamento può applicare la condizione prevista al paragrafo 4 dell'allegato 8 soltanto in circostanze specifiche ⁽⁷²⁾. Analogamente vi sono limitazioni per le condizioni «atti giudiziari» e «prevenzione di frodi» (allegato 8, rispettivamente paragrafo 7 e 8), entrambe applicabili soltanto a specifici titolari del trattamento: alla condizione relativa agli atti giudiziari può ricorrere soltanto un organo giurisdizionale o un'altra autorità giudiziaria, mentre a quella relativa alla prevenzione di frodi possono ricorrere soltanto i titolari del trattamento che sono organizzazioni antifrode.

- (42) Quando infine il trattamento si basa su una delle condizioni elencate nell'allegato 8 e di cui alla sezione 42 della legge del 2018 sulla protezione dei dati, deve esistere un «documento adeguato di informativa», che spieghi le procedure attuate dal titolare del trattamento per assicurare il rispetto dei principi di protezione dei dati nonché le politiche del titolare del trattamento in materia di conservazione e cancellazione dei dati personali, e si applica l'obbligo di tenere un registro consolidato.

2.4.2. Limitazione delle finalità

- (43) I dati personali dovrebbero essere trattati per una finalità specifica e, di conseguenza, dovrebbero essere utilizzati soltanto nella misura in cui l'uso non sia incompatibile con la finalità del trattamento. Tale principio di protezione dei dati è garantito dalla sezione 36 della legge del 2018 sulla protezione dei dati. Analogamente all'articolo 4, paragrafo 1, lettera b), della direttiva (UE) 2016/680, tale disposizione impone che: a) la finalità di contrasto per la quale si raccolgono i dati in qualsiasi occasione sia determinata, esplicita e legittima; e b) i dati personali così raccolti non vengano trattati in modo incompatibile con la finalità per cui sono stati raccolti.
- (44) Quando le autorità competenti trattano i dati per una finalità di contrasto, ciò può comprendere l'archiviazione, la ricerca scientifica o storica o finalità statistiche ⁽⁷³⁾. In tali casi, la legge del 2018 sulla protezione dei dati chiarisce anche che l'archiviazione (o il trattamento per finalità di ricerca scientifica o storica e per finalità statistiche) non è consentita se viene effettuata in relazione a decisioni prese nei confronti di un determinato interessato o se ciò può arrecargli un danno o un disagio sostanziale ⁽⁷⁴⁾.

2.4.3. Esattezza e minimizzazione dei dati

- (45) I dati devono essere esatti e, se necessario, devono essere aggiornati. Devono inoltre essere adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali sono trattati. Le sezioni 37 e 38 della legge del 2018 sulla protezione dei dati sanciscono tali principi in modo analogo all'articolo 4, paragrafo 1, lettere c), d) ed e), della direttiva (UE) 2016/680. Occorre adottare tutte le misure ragionevoli per assicurare che i dati personali inesatti ⁽⁷⁵⁾ siano cancellati o rettificati

⁽⁷¹⁾ *Guide to Law Enforcement Processing*, «Conditions for sensitive processing» (cfr. nota 70).

⁽⁷²⁾ Il trattamento viene effettuato senza il consenso dell'interessato quando: a) l'interessato non può esprimere il consenso al trattamento; b) non ci si può ragionevolmente attendere che il titolare del trattamento ottenga il consenso dell'interessato al trattamento; c) il trattamento deve essere effettuato senza il consenso dell'interessato perché l'ottenimento di tale consenso pregiudicherebbe la fornitura della protezione di cui al punto 1, lettera a).

⁽⁷³⁾ Cfr. sezione 41, paragrafo 1, della legge del 2018 sulla protezione dei dati.

⁽⁷⁴⁾ Cfr. sezione 41, paragrafo 2, della legge del 2018 sulla protezione dei dati.

⁽⁷⁵⁾ La sezione 205 della legge del 2018 sulla protezione dei dati definisce l'aggettivo «inesatti» riferito ai dati personali come «errati o fuorvianti». Le autorità del Regno Unito hanno spiegato che i dati relativi ad indagini penali sono spesso incompleti, ma indipendentemente da ciò possono essere esatti.

senza indugio ⁽⁷⁶⁾, tenendo conto della finalità di contrasto per la quale sono trattati ⁽⁷⁷⁾, così come per garantire che i dati personali non esatti, incompleti o non più aggiornati non vengano trasmessi né resi disponibili per alcuna finalità di contrasto ⁽⁷⁸⁾.

- (46) Analogamente all'articolo 7 della direttiva (UE) 2016/680, il regime di protezione dei dati del Regno Unito specifica che i dati personali basati su fatti devono, per quanto possibile, essere distinti da quelli basati su valutazioni personali ⁽⁷⁹⁾. Laddove pertinente e per quanto possibile, occorre operare una chiara distinzione tra i dati personali relativi a diverse categorie di interessati, quali indiziati, persone condannate per un reato, vittime di reato e testimoni ⁽⁸⁰⁾.

2.4.4. Limitazione della conservazione

- (47) Ai sensi dell'articolo 5 della direttiva (UE) 2016/680, in linea di principio i dati non devono essere conservati più a lungo di quanto necessario a conseguire le finalità per cui sono trattati. Conformemente alla sezione 39 della legge del 2018 sulla protezione dei dati e analogamente all'articolo 5 di detta direttiva, è vietato conservare dati personali trattati per una finalità di contrasto per un periodo superiore a quello necessario in relazione alla finalità per la quale vengono trattati. Il regime giuridico del Regno Unito impone di fissare termini adeguati per l'esame periodico della necessità di continuare a conservare i dati personali per una qualsiasi finalità di contrasto. Ulteriori norme relative alle pratiche concernenti la conservazione dei dati personali e i termini applicabili sono stati stabiliti nella normativa pertinente e negli orientamenti che disciplinano i poteri e il funzionamento delle forze di polizia. Ad esempio in Inghilterra e nel Galles il codice di pratica MoPI del *College of Policing*, unitamente agli orientamenti APP sulla gestione delle informazioni di polizia, forniscono un quadro destinato ad assicurare un processo coerente di conservazione, riesame e cancellazione, basato sui rischi, per la gestione delle informazioni operative relative alle attività di polizia ⁽⁸¹⁾. Tale quadro stabilisce criteri chiari per l'intero servizio in merito alle modalità di creazione, condivisione, utilizzo e gestione delle informazioni nell'ambito della polizia e tra le singole forze di polizia e altre agenzie ⁽⁸²⁾. La polizia è tenuta a rispettare il codice di pratica e il rispetto di tale obbligo viene verificato da *Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services* ⁽⁸³⁾.
- (48) Il servizio di polizia dell'Irlanda del Nord (PSNI, *Police Service of Northern Ireland*) non è tenuto per legge a seguire il codice di pratica MoPI. Tuttavia, il quadro per la gestione delle informazioni relative alle attività di polizia adottato nel 2011 è integrato da un manuale del PSNI ⁽⁸⁴⁾, che stabilisce politiche e procedure concernenti le modalità di applicazione del codice di pratica MoPI in Irlanda del Nord.

⁽⁷⁶⁾ Sezione 38, paragrafo 1, lettera b), della legge del 2018 sulla protezione dei dati.

⁽⁷⁷⁾ Secondo l'*Explanatory Framework for Adequacy Discussion* del Regno Unito, ciò assicura il riconoscimento tanto dei diritti degli interessati quanto delle esigenze operative delle autorità di contrasto. Il punto di cui sopra è stato preso attentamente in considerazione durante le fasi di redazione della *Data Protection Bill* (legge sulla protezione dei dati), in quanto possono esservi ragioni operative specifiche e limitate che giustificano l'impossibilità di rettificare i dati. Con molta probabilità ciò si verifica se i dati personali inesatti in questione devono essere preservati nella loro forma originale per fini probatori (cfr. Regno Unito, *Explanatory Framework for Adequacy Discussions*, section F: *Law Enforcement*, pag. 21; cfr. nota 9).

⁽⁷⁸⁾ Sezione 38, paragrafo 4, della legge del 2018 sulla protezione dei dati. Inoltre, ai sensi della sezione 38, paragrafo 5, della legge del 2018 sulla protezione dei dati, prima di trasmettere o mettere a disposizione i dati personali occorre verificarne la qualità; in tutte le trasmissioni di dati personali occorre includere le informazioni necessarie che consentano al destinatario di valutare il grado di esattezza, completezza e affidabilità dei dati e il loro grado di aggiornamento; e qualora dopo la trasmissione dei dati personali emerga che i dati erano errati o che la trasmissione è stata illecita, tale circostanza deve essere notificata al destinatario senza indugio.

⁽⁷⁹⁾ Sezione 38, paragrafo 2, della legge del 2018 sulla protezione dei dati.

⁽⁸⁰⁾ Sezione 38, paragrafo 3, della legge del 2018 sulla protezione dei dati.

⁽⁸¹⁾ Tale quadro assicura coerenza nell'applicazione della conservazione dei dati personali acquisiti. L'esame periodico dipende dai reati, che sono suddivisi in 4 gruppi: 1) determinate questioni di protezione della collettività; 2) altri reati sessuali violenti e gravi; 3) tutti gli altri reati; 4) reati vari. Maggiori dettagli sono riportati negli orientamenti APP sulla gestione delle informazioni di polizia (cfr. nota 26).

⁽⁸²⁾ Secondo le informazioni fornite dalle autorità del Regno Unito, altre organizzazioni sono libere di seguire i principi del codice di pratica MoPI, qualora lo desiderino; ad esempio, *Her Majesty's Revenue and Customs* e *National Crime Agency* adottano volontariamente molti dei principi previsti dal codice di pratica MoPI al fine di assicurare la coerenza nelle attività di contrasto. In generale la maggior parte delle organizzazioni fornisce al proprio personale politiche ed orientamenti specifici destinati a tutto il personale in merito alle modalità di gestione dei dati personali nel contesto del loro ruolo, adattati all'organizzazione specifica. Di norma in tale contesto rientra anche una formazione obbligatoria.

⁽⁸³⁾ Il codice di pratica MoPI è stato formulato sulla base dei poteri previsti dalla legge del 1996 sulla polizia che consente al *College of Policing* di adottare codici di pratica relativi al funzionamento efficace delle attività di polizia. Qualsiasi codice di pratica adottato ai sensi di tale legge deve ottenere l'approvazione da parte del segretario di Stato ed è oggetto di consultazione con la *National Crime Agency* prima di essere presentato al parlamento. La sezione 39 A, paragrafo 7, della legge del 1996 sulla polizia impone alle forze di polizia di tenere in debito conto i codici emessi ai sensi di tale legge.

⁽⁸⁴⁾ PSNI, *MoPI Handbook*, capitoli da 1 a 6.

- (49) In Scozia le forze di polizia fanno riferimento alla procedura operativa standard (POS) per la conservazione di registrazioni ⁽⁸⁵⁾ che sostiene la politica per la gestione delle registrazioni ⁽⁸⁶⁾ del servizio di polizia. Tale procedura operativa standard stabilisce norme specifiche per la conservazione dei registri gestiti dalla polizia scozzese.
- (50) Oltre al requisito generale di esaminare i registri che si applica in tutto il Regno Unito, ulteriori dettagli sono forniti nel contesto di norme a livello locale. Ad esempio, per quanto concerne Inghilterra e Galles, la legge sulle prove nelle attività di polizia e di azione penale, come modificata dalla legge del 2012 sulla protezione delle libertà, prevede la conservazione delle impronte digitali e dei profili DNA nonché un regime specifico per le persone fisiche non condannate ⁽⁸⁷⁾. La legge del 2012 sulla protezione delle libertà ha altresì creato la posizione del *Biometrics Commissioner* ⁽⁸⁸⁾ (commissario per la conservazione e l'uso di materiale biometrico). Le norme specifiche sulle immagini di custodia sono riportate nel riesame del 2017 sulle immagini di custodia ⁽⁸⁹⁾. Per quanto riguarda la Scozia, la legge del 1995 sulla procedura penale (Scozia) fissa le norme per l'ottenimento e la conservazione di impronte digitali e campioni biologici ⁽⁹⁰⁾. Come nel caso di Inghilterra e Galles, la legislazione regola la conservazione di dati biometrici in casi diversi ⁽⁹¹⁾.

2.4.5. Sicurezza dei dati

- (51) I dati personali devono 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 le autorità pubbliche devono adottare misure tecniche od organizzative per proteggere i dati personali da possibili minacce. Tali misure devono essere valutate tenendo conto dello stato attuale delle conoscenze e dei costi connessi.
- (52) Questi principi si riflettono nella sezione 40 della legge del 2018 sulla protezione dei dati che prevede, analogamente all'articolo 4, paragrafo 1, lettera f), della direttiva (UE) 2016/680, che i dati personali trattati per qualsiasi finalità di contrasto siano trattati in maniera tale da garantirne un'adeguata sicurezza, utilizzando misure tecniche od organizzative adeguate. Ciò comprende la protezione dei dati da trattamenti non autorizzati o illeciti nonché da

⁽⁸⁵⁾ *Record Retention - Standard Operating Procedure (SOP)*, disponibile al seguente indirizzo: <https://www.scotland.police.uk/spa-media/nhoby5i/record-retention-sop.pdf>.

⁽⁸⁶⁾ Per maggiori dettagli sulla gestione delle registrazioni, cfr. informazioni relative al *National Records of Scotland*, disponibili al seguente indirizzo: <https://www.nrscotland.gov.uk/record-keeping/records-management>.

⁽⁸⁷⁾ I periodi di conservazione variano a seconda che una persona fisica sia stata condannata o meno (sezioni da 63I a 63KI della legge del 1984 sulle prove). Ad esempio nel caso di un adulto condannato per un reato registrabile, le sue impronte digitali e il suo profilo del DNA possono essere conservati a tempo indeterminato (sezione 63I, paragrafo 2, della legge del 1984 sulle prove), mentre la conservazione è limitata nel tempo se la persona condannata ha meno di 18 anni, se il reato è un reato registrabile come «minore» e se la persona è incensurata (sezione 63K della legge del 1984 sulle prove). La conservazione nel caso di una persona arrestata o accusata ma non condannata è limitata nel tempo a tre anni (sezione 63F della legge del 1984 sulle prove). Una proroga di tale periodo di conservazione deve essere approvata dall'autorità giudiziaria (sezione 63F, paragrafo 7, della legge del 1984 sulle prove). Nel caso di persone arrestate o accusate ma non condannate per un reato minore, non è possibile conservare le prove (sezioni 63D e 63H della legge del 1984 sulle prove).

⁽⁸⁸⁾ La sezione 20 della legge del 2012 sulla protezione delle libertà crea la posizione del *Biometrics Commissioner*. Tra le altre funzioni, il *Biometrics Commissioner* decide se la polizia può o meno conservare registrazioni dei profili DNA e impronte digitali ottenute da persone fisiche arrestate ma non accusate di un reato qualificato (sezione 63G della legge del 1984 sulle prove nelle attività di polizia e di azione penale). Spetta inoltre al *Biometrics Commissioner* la competenza generale per sottoporre ad esame la conservazione e l'utilizzo di DNA e impronte digitali, così come la loro conservazione per motivi di sicurezza nazionale (sezione 20, paragrafo 2, della legge del 2012 sulla protezione delle libertà). Il *Biometrics Commissioner* è nominato secondo il *Governance Code for Public Appointments* (codice sulla governance delle nomine pubbliche, disponibile al seguente indirizzo: [Governance Code for Public Appointments - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/publications/governance-code-for-public-appointments)) e nel suo mandato è dichiarato specificamente che può essere rimosso dalle sue funzioni solo dal *Home Secretary* (segretario di Stato per gli Affari interni) in una serie strettamente definita di circostanze, tra cui l'inadempienza agli obblighi professionali per un periodo di tre mesi, la condanna per un reato o il mancato adempimento del mandato.

⁽⁸⁹⁾ *Review of the use and retention of custody images*, disponibile al seguente indirizzo: <https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention>.

⁽⁹⁰⁾ Sezione 18 e seguenti della legge del 1995 sulla procedura penale — Scozia.

⁽⁹¹⁾ I periodi di conservazione variano in base al fatto che la persona sia stata condannata o meno (sezione 18, paragrafo 3, della legge del 1995 sulla procedura penale — Scozia) o che sia o meno minorenni. In quest'ultimo caso, il periodo di conservazione è di tre anni dalla condanna nell'udienza di minori (sezione 18E, paragrafo 8, della legge del 1995 sulla procedura penale — Scozia). I dati delle persone arrestate ma non condannate non possono essere conservati (sezione 18, paragrafo 3, della legge del 1995 sulla procedura penale — Scozia) fatta eccezione per casi specifici e a seconda della gravità del reato (sezione 18 A della legge del 1995 sulla procedura penale — Scozia). La *Scottish Biometrics Commissioner Act 2020* (legge del 2020 sul commissario per la biometrica della Scozia) (cfr. <https://www.legislation.gov.uk/asp/2020/8/contents>) istituisce la posizione del *Biometrics Commissioner* della Scozia, incaricato di redigere e rivedere i codici di pratica (approvati dal parlamento scozzese) riguardanti l'acquisizione, la conservazione, l'uso e la distruzione di dati biometrici per finalità di giustizia penale e di polizia (sezione 7 della legge del 2020 sul commissario per la biometrica della Scozia).

perdita, distruzione o danno accidentali ⁽⁹²⁾. La sezione 66 della legge del 2018 sulla protezione dei dati specifica inoltre che ciascun titolare del trattamento e ciascun responsabile del trattamento deve attuare misure tecniche e organizzative adeguate per assicurare un livello di sicurezza adeguato ai rischi derivanti dal trattamento di dati personali. Secondo le note esplicative, il titolare del trattamento deve valutare i rischi e attuare misure di sicurezza adeguate basate su tale valutazione, ad esempio la cifratura o livelli specifici di nulla osta di sicurezza per il personale che tratta i dati ⁽⁹³⁾. La valutazione deve tenere conto, ad esempio, della natura dei dati trattati e di qualsiasi altro fattore o circostanza pertinente che potrebbe incidere sulla sicurezza del trattamento.

- (53) Il regime che disciplina il rispetto dei principi di sicurezza dei dati è molto simile a quello stabilito dagli articoli da 29 a 31 della direttiva (UE) 2016/680. In particolare, nel caso di una violazione dei dati personali in relazione a dati personali per i quali il titolare del trattamento è responsabile, ai sensi della sezione 67, paragrafo 1, della legge del 2018 sulla protezione dei dati, detto titolare deve notificare tale violazione dei dati personali all'ICO senza ingiustificato ritardo, e laddove fattibile, entro 72 ore dal momento in cui è venuto a conoscenza della violazione ⁽⁹⁴⁾. L'obbligo di notifica non si applica quando è improbabile che la violazione dei dati personali possa comportare un rischio per i diritti e le libertà di persone fisiche ⁽⁹⁵⁾. Il titolare del trattamento deve documentare i fatti relativi a qualsiasi violazione dei dati personali, le sue conseguenze e i provvedimenti adottati per porvi rimedio in maniera tale da consentire all'ICO di verificare il rispetto della legge sulla protezione dei dati ⁽⁹⁶⁾. Se un responsabile del trattamento viene a conoscenza di una violazione della sicurezza, deve notificare tale circostanza al titolare del trattamento senza ingiustificato ritardo ⁽⁹⁷⁾.
- (54) Conformemente alla sezione 68, paragrafo 1, della legge del 2018 sulla protezione dei dati, se è probabile che una violazione dei dati personali costituisca un rischio elevato per i diritti e le libertà di persone fisiche, il titolare del trattamento deve informare l'interessato della violazione senza ingiustificato ritardo ⁽⁹⁸⁾. Tale notifica deve comprendere le stesse informazioni della notifica all'ICO di cui al considerando 53. Tale obbligo non si applica se il titolare del trattamento ha attuato misure di protezione tecniche ed organizzative adeguate che sono state applicate ai dati personali interessati dalla violazione. Non si applica inoltre se il titolare del trattamento ha adottato misure successive grazie alle quali non è più probabile che il rischio elevato per i diritti e le libertà degli interessati si realizzi. Infine il titolare del trattamento non è tenuto a informare l'interessato qualora la notifica comporti uno sforzo sproporzionato ⁽⁹⁹⁾. In tal caso le informazioni devono essere rese disponibili all'interessato in un altro modo altrettanto efficace, ad esempio per mezzo di una comunicazione pubblica ⁽¹⁰⁰⁾. Se il titolare del trattamento non ha informato l'interessato in merito alla violazione, l'ICO, che ha ricevuto la notifica ai sensi della sezione 67 della legge sulla protezione dei dati, dopo aver considerato la probabilità che la violazione comporti un rischio elevato, può richiedere al titolare del trattamento di notificare la violazione all'interessato ⁽¹⁰¹⁾.

⁽⁹²⁾ Conformemente alle note esplicative sulla legge del 2018 sulla protezione dei dati (cfr. nota 45), in particolare, il titolare del trattamento deve: progettare e organizzare le proprie misure di sicurezza in maniera da adattare alla natura dei dati personali conservati e al danno che può derivare da una violazione della sicurezza; definire con chiarezza le persone responsabili all'interno della propria organizzazione per garantire la sicurezza delle informazioni; assicurarsi di disporre della giusta sicurezza fisica e tecnica, sostenuta da politiche e procedure solide e da personale affidabile e ben addestrato; essere pronto a reagire a qualsiasi violazione della sicurezza in modo rapido ed efficace.

⁽⁹³⁾ Punto 221 delle note esplicative sulla legge del 2018 sulla protezione dei dati (cfr. nota 45).

⁽⁹⁴⁾ La sezione 67, paragrafo 4, della legge del 2018 sulla protezione dei dati prevede che la notifica comprenda una descrizione della natura della violazione dei dati personali (comprese, ove possibile, le categorie e il numero approssimativo di interessati coinvolti nonché le categorie e il numero approssimativo di registrazioni dei dati personali coinvolti), il nome e le coordinate di un punto di contatto, una descrizione delle probabili conseguenze della violazione dei dati personali così come una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per rimediare alla violazione dei dati personali (comprese, ove appropriato, misure per attenuarne i possibili effetti negativi).

⁽⁹⁵⁾ Sezione 67, paragrafo 2, della legge del 2018 sulla protezione dei dati.

⁽⁹⁶⁾ Sezione 67, paragrafo 6, della legge del 2018 sulla protezione dei dati.

⁽⁹⁷⁾ Sezione 67, paragrafo 9, della legge del 2018 sulla protezione dei dati.

⁽⁹⁸⁾ Ai sensi della sezione 68, paragrafo 7, della legge del 2018 sulla protezione dei dati il titolare del trattamento può limitare, interamente o parzialmente, la fornitura di informazioni agli interessati nella misura in cui è fittantoché, tenendo conto dei diritti fondamentali e degli interessi legittimi dell'interessato, tale limitazione costituisce una misura necessaria e proporzionata per: a) non ostacolare indagini, inchieste o procedimenti ufficiali o giudiziari; b) non compromettere la prevenzione, l'accertamento, l'indagine e il perseguimento di reati o l'esecuzione di sanzioni penali; c) proteggere la sicurezza pubblica; d) proteggere la sicurezza nazionale; e) proteggere i diritti e le libertà altrui.

⁽⁹⁹⁾ Sezione 68, paragrafo 3, della legge del 2018 sulla protezione dei dati.

⁽¹⁰⁰⁾ Sezione 68, paragrafo 5, della legge del 2018 sulla protezione dei dati.

⁽¹⁰¹⁾ Sezione 68, paragrafo 6, della legge del 2018 sulla protezione dei dati, con la limitazione di cui alla sezione 68, paragrafo 8, della medesima legge.

2.4.6. Trasparenza

- (55) Gli interessati devono essere informati dei principali aspetti del trattamento dei dati personali che li riguardano. Questo principio di protezione dei dati si riflette nella sezione 44 della legge del 2018 sulla protezione dei dati che, analogamente all'articolo 13 della direttiva (UE) 2016/680, prevede che il titolare del trattamento abbia un dovere generale di mettere a disposizione degli interessati informazioni sul trattamento dei loro dati personali (mettendo tali informazioni a disposizione del pubblico in generale o in qualsiasi altro modo) ⁽¹⁰²⁾. Tra le informazioni necessarie che devono essere messe a disposizione figurano: a) l'identità e i dati di contatto del titolare del trattamento; b) ove applicabile, i dati di contatto del responsabile della protezione dei dati; c) le finalità per le quali il titolare del trattamento tratta i dati personali; d) il fatto che gli interessati hanno il diritto di richiedere al titolare del trattamento l'accesso ai loro dati personali, la rettifica e la cancellazione degli stessi, oppure la limitazione del loro trattamento; e) l'esistenza del diritto di proporre reclamo all'ICO e i dati di contatto di quest'ultimo ⁽¹⁰³⁾.
- (56) In casi specifici, al fine di consentire l'esercizio dei diritti di un interessato in virtù della legge del 2018 sulla protezione dei dati (ad esempio quando i dati personali trattati sono stati raccolti all'insaputa dell'interessato), il titolare del trattamento deve fornire inoltre informazioni in merito ai seguenti aspetti: a) la base giuridica per il trattamento; b) il periodo di conservazione dei dati personali oppure, se non è possibile fornire questa informazione, i criteri utilizzati per determinare tale periodo; c) se del caso, le categorie di destinatari dei dati personali (anche in paesi terzi o in seno a organizzazioni internazionali); d) ulteriori informazioni necessarie per consentire l'esercizio dei diritti dell'interessato in virtù della parte 3 della legge del 2018 sulla protezione dei dati ⁽¹⁰⁴⁾.

2.4.7. Diritti delle persone fisiche

- (57) Gli interessati devono disporre di diversi diritti azionabili. Il capo 3 della parte 3 della legge del 2018 sulla protezione dei dati riconosce alle persone fisiche diritti di accesso, rettifica, cancellazione e limitazione ⁽¹⁰⁵⁾ paragonabili a quelli previsti al capo 3 della direttiva (UE) 2016/680.
- (58) Il diritto di accesso è sancito dalla sezione 45 della legge del 2018 sulla protezione dei dati. Innanzitutto una persona fisica ha il diritto di ottenere una conferma dal titolare del trattamento in merito al fatto che i suoi dati personali siano o meno oggetto di trattamento ⁽¹⁰⁶⁾. In secondo luogo, laddove i dati personali siano oggetto di trattamento, l'interessato ha il diritto di accedere ai dati e ricevere le seguenti informazioni in merito al trattamento: a) le finalità e la base giuridica del trattamento; b) le categorie di dati interessate; c) il destinatario a cui i dati sono stati divulgati; d) il periodo per il quale saranno conservati i dati personali; e) l'esistenza del diritto dell'interessato alla rettifica e alla cancellazione dei dati personali; f) il diritto di proporre reclamo; g) qualsiasi informazione sull'origine dei dati personali interessati ⁽¹⁰⁷⁾.
- (59) Ai sensi della sezione 46 della legge del 2018 sulla protezione dei dati, l'interessato ha il diritto di richiedere al titolare del trattamento di rettificare dati personali inesatti che lo riguardano. Il titolare del trattamento deve rettificare (o, laddove i dati siano inesatti perché incompleti, completare) i dati senza ingiustificato ritardo. Se i dati personali devono essere conservati a fini probatori, il titolare del trattamento deve, anziché rettificare i dati personali, limitarne il trattamento ⁽¹⁰⁸⁾.

⁽¹⁰²⁾ Il documento *Guide to Law Enforcement Processing* fornisce il seguente esempio: sul vostro sito web avete un'informativa sulla protezione dei dati generica che contiene le informazioni di base sull'organizzazione, la finalità per la quale trattate i dati personali, i diritti degli interessati e il loro diritto a proporre reclamo all'ICO. Avete ricevuto informazioni di intelligence secondo le quali una persona era presente nel momento in cui è stato commesso un reato. In occasione del primo colloquio con tale persona, dovete fornire informazioni generali, nonché le ulteriori informazioni di sostegno, per consentirle l'esercizio dei suoi diritti. Potete limitare le informazioni sul trattamento lecito che state fornendo soltanto se divulgarle inciderebbe negativamente sull'indagine che state svolgendo (*Guide to Law Enforcement Processing*, «What information should we supply to an individual?», disponibile al seguente indirizzo: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3>).

⁽¹⁰³⁾ Nel documento *Guide to Law Enforcement Processing* si afferma che le informazioni fornite in merito al trattamento dei dati personali devono essere concise, intelligibili e facilmente accessibili; scritte in un linguaggio chiaro e semplice, adattato alle esigenze di persone vulnerabili, quali i minori; e fornite gratuitamente (*Guide to Law Enforcement Processing*, «How should we provide this information?», disponibile al seguente indirizzo: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1>).

⁽¹⁰⁴⁾ Sezione 44, paragrafo 2, della legge del 2018 sulla protezione dei dati.

⁽¹⁰⁵⁾ Per un'analisi dettagliata dei diritti degli interessati, cfr.: *Guide to Law Enforcement Processing on individual rights*, disponibile al seguente indirizzo: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/>.

⁽¹⁰⁶⁾ Sezione 45, paragrafo 1, della legge del 2018 sulla protezione dei dati.

⁽¹⁰⁷⁾ Sezione 45, paragrafo 2, della legge del 2018 sulla protezione dei dati.

⁽¹⁰⁸⁾ Sezione 46, paragrafo 4, della legge del 2018 sulla protezione dei dati.

- (60) La sezione 47 della legge del 2018 sulla protezione dei dati riconosce alle persone fisiche il diritto alla cancellazione e alla limitazione del trattamento. Il titolare del trattamento deve ⁽¹⁰⁹⁾ cancellare i dati personali senza ingiustificato ritardo quando il trattamento dei dati personali violerebbe uno dei principi di protezione dei dati, le basi giuridiche per il trattamento o le garanzie relative all'archiviazione e al trattamento di dati sensibili. Il titolare del trattamento deve altresì cancellare i dati qualora sia soggetto a un obbligo giuridico che glielo impone. Se i dati personali devono essere conservati a fini probatori, il titolare del trattamento deve limitarne il trattamento (anziché cancellarli) ⁽¹¹⁰⁾. Il titolare del trattamento deve limitare il trattamento dei dati personali se un soggetto ne contesta l'esattezza, ma non è possibile accertare se sono esatti o meno ⁽¹¹¹⁾.
- (61) Se l'interessato richiede la rettifica o la cancellazione di dati personali o la limitazione del loro trattamento, il titolare del trattamento deve informare l'interessato per iscritto se la richiesta è stata accolta e, qualora sia stata rifiutata, informarlo dei motivi del rifiuto e dei mezzi di ricorso disponibili (diritto dell'interessato di presentare una richiesta all'ICO affinché indaghi per stabilire se la limitazione è stata applicata lecitamente, diritto di proporre reclamo presso l'ICO e diritto di presentare un'istanza per ottenere un'ordinanza da un organo giurisdizionale che intimi il rispetto della normativa) ⁽¹¹²⁾.
- (62) Laddove il titolare del trattamento rettifichi dati personali ricevuti da un'altra autorità competente, deve notificarlo a quest'ultima ⁽¹¹³⁾. Qualora rettifichi, cancelli o limiti il trattamento di dati personali che ha divulgato, il titolare del trattamento deve informare i destinatari, i quali a loro volta devono analogamente rettificare, cancellare o limitare il trattamento dei dati personali (nella misura in cui ne siano responsabili) ⁽¹¹⁴⁾.
- (63) L'interessato ha inoltre il diritto di essere informato senza ingiustificato ritardo dal titolare del trattamento in merito a una violazione dei dati personali quando ciò potrebbe comportare un rischio elevato per i diritti e le libertà di persone fisiche ⁽¹¹⁵⁾.
- (64) In relazione a tutti questi diritti dell'interessato e analogamente a quanto previsto dall'articolo 12 della direttiva (UE) 2016/680, il titolare del trattamento è tenuto ad assicurare che qualsiasi informazione sia fornita all'interessato in forma concisa, intelligibile e facilmente accessibile ⁽¹¹⁶⁾; inoltre, ove possibile, tali informazioni dovrebbero essere fornite nella stessa forma della richiesta ⁽¹¹⁷⁾. Il titolare del trattamento deve soddisfare una richiesta dell'interessato senza ritardi ingiustificati e in ogni caso, in linea di principio, entro un mese dalla richiesta ⁽¹¹⁸⁾. Laddove il titolare del trattamento nutra dubbi ragionevoli in merito all'identità della persona fisica, può richiedere informazioni supplementari e ritardare la gestione della richiesta fino a quando non ne abbia accertato l'identità. Il titolare del trattamento può richiedere il pagamento di diritti ragionevoli o rifiutarsi di dare seguito alla richiesta quando la ritiene manifestamente infondata ⁽¹¹⁹⁾. L'ICO ha fornito orientamenti in merito ai casi nei quali una richiesta è considerata manifestamente infondata o eccessiva e nei quali è possibile richiedere un pagamento ⁽¹²⁰⁾.
- (65) Inoltre, ai sensi della sezione 53, paragrafo 4, della legge del 2018 sulla protezione dei dati, il segretario di Stato può specificare, mediante regolamenti, l'ammontare massimo dei diritti.

⁽¹⁰⁹⁾ L'interessato può chiedere al titolare del trattamento di cancellare i dati personali o di limitarne il trattamento (ma gli obblighi del titolare del trattamento di cancellare i dati o di limitarne il trattamento si applicano indipendentemente dal fatto che tale richiesta venga fatta o meno).

⁽¹¹⁰⁾ Sezione 46, paragrafo 4, e sezione 47, paragrafo 2, della legge del 2018 sulla protezione dei dati.

⁽¹¹¹⁾ Sezione 47, paragrafo 3, della legge del 2018 sulla protezione dei dati.

⁽¹¹²⁾ Sezione 48, paragrafo 1, della legge del 2018 sulla protezione dei dati.

⁽¹¹³⁾ Sezione 48, paragrafo 7, della legge del 2018 sulla protezione dei dati.

⁽¹¹⁴⁾ Sezione 48, paragrafo 9, della legge del 2018 sulla protezione dei dati.

⁽¹¹⁵⁾ Sezione 68 della legge del 2018 sulla protezione dei dati.

⁽¹¹⁶⁾ Sezione 52, paragrafo 1, della legge del 2018 sulla protezione dei dati.

⁽¹¹⁷⁾ Sezione 52, paragrafo 3, della legge del 2018 sulla protezione dei dati.

⁽¹¹⁸⁾ La sezione 54 della legge del 2018 sulla protezione dei dati definisce il significato di «termine applicabile», che indica un mese o un periodo più lungo, che può essere specificato nei regolamenti, a decorrere dal momento rilevante (quando il titolare del trattamento riceve la richiesta in questione; quando il titolare del trattamento riceve l'eventuale informazione chiesta in relazione alla richiesta ai sensi della sezione 52, paragrafo 4, della legge sulla protezione dei dati; oppure quando vengono versati gli eventuali diritti addebitati in relazione alla richiesta ai sensi della sezione 53 della legge sulla protezione dei dati).

⁽¹¹⁹⁾ Sezione 53, paragrafo 1, della legge del 2018 sulla protezione dei dati.

⁽¹²⁰⁾ Conformemente agli orientamenti dell'ICO, un titolare del trattamento può decidere di addebitare diritti a un interessato qualora la sua richiesta sia manifestamente infondata o eccessiva, ma scelga comunque di rispondervi. I diritti devono essere ragionevoli e poter giustificare il costo. *Guide to Law Enforcement Processing «Manifestly unfounded and excessive requests»*, disponibile al seguente indirizzo: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/>

2.4.7.1. Limitazioni dei diritti dell'interessato e obblighi di trasparenza

- (66) Un'autorità competente può, in determinate circostanze, limitare determinati diritti dell'interessato: il diritto di accesso ⁽¹²¹⁾, di essere informato ⁽¹²²⁾, di venire a conoscenza di una violazione dei dati personali ⁽¹²³⁾ e di essere informato in merito al motivo del rifiuto di una richiesta di rettifica o cancellazione ⁽¹²⁴⁾. Analogamente al regime di cui al capo III della direttiva (UE) 2016/680, l'autorità competente può applicare una limitazione soltanto quando, considerati i diritti fondamentali e gli interessi legittimi dell'interessato, tale limitazione è necessaria e proporzionata per: a) non ostacolare indagini, inchieste o procedimenti ufficiali o giudiziari; b) non compromettere la prevenzione, l'accertamento, l'indagine e il perseguimento di reati o l'esecuzione di sanzioni penali; c) proteggere la sicurezza pubblica; d) proteggere la sicurezza nazionale; e) proteggere i diritti e le libertà altrui.
- (67) L'ICO ha fornito orientamenti sull'applicazione di tali limitazioni. Conformemente a tali orientamenti, i titolari del trattamento devono effettuare un'analisi caso per caso per trovare un equilibrio tra i diritti della persona fisica e i danni che causerebbe una divulgazione. In particolare essi devono giustificare qualsiasi limitazione in quanto misura necessaria e proporzionata e possono applicare limitazioni soltanto nei confronti di ciò che rischia di compromettere le finalità di cui sopra ⁽¹²⁵⁾.
- (68) Le autorità competenti hanno pubblicato altri documenti di orientamento che forniscono informazioni dettagliate su tutti gli aspetti della legislazione in materia di protezione dei dati, compresa l'applicazione delle limitazioni dei diritti degli interessati ⁽¹²⁶⁾. Ad esempio, in relazione alla sezione 45, paragrafo 4, il *Data Protection Manual* del *National Police Chief's Counsel* afferma: «è importante osservare che le limitazioni possono essere applicate soltanto nella misura necessaria e possono essere applicate soltanto purché sia necessario. Di conseguenza non è consentito applicare in maniera indiscriminata la limitazione a tutti i dati personali di un richiedente o applicarla in modo permanente. In merito a quest'ultimo punto, spesso accade che dati personali raccolti all'insaputa dell'interessato che è un indiziato nel contesto di un'indagine debbano inizialmente essere protetti dalla divulgazione a tale persona per evitare di compromettere l'indagine mentre è in corso; tuttavia in un secondo momento la divulgazione non causerebbe danni se i dati personali fossero divulgati alla persona in questione durante il suo interrogatorio. Le forze di polizia devono adottare processi che garantiscano che l'applicazione di tali limitazioni avvenga soltanto nella misura necessaria e soltanto per la durata necessaria» ⁽¹²⁷⁾. Tali orientamenti forniscono altresì esempi di casi nei quali è probabile il ricorso a ciascuna di tali limitazioni ⁽¹²⁸⁾.
- (69) Inoltre, in relazione alla possibilità di limitare uno dei diritti di cui sopra per proteggere la «sicurezza nazionale», un titolare del trattamento può richiedere un certificato firmato da un ministro o dal procuratore generale (o dall'avvocato generale per la Scozia) che certifichi che la limitazione di tali diritti è una misura necessaria e proporzionata per la protezione della sicurezza nazionale ⁽¹²⁹⁾. Il governo del Regno Unito ha pubblicato orientamenti sui certificati di sicurezza nazionale ai sensi della legge del 2018 sulla protezione dei dati, in cui si sottolinea che qualsiasi limitazione dei diritti degli interessati a favore della protezione della sicurezza nazionale deve essere proporzionata e necessaria ⁽¹³⁰⁾ (per ulteriori dettagli sui certificati di sicurezza nazionale si vedano i considerando da 131 a 134).

⁽¹²¹⁾ Sezione 45, paragrafo 4, della legge del 2018 sulla protezione dei dati.

⁽¹²²⁾ Sezione 44, paragrafo 4, della legge del 2018 sulla protezione dei dati.

⁽¹²³⁾ Sezione 68, paragrafo 7, della legge del 2018 sulla protezione dei dati.

⁽¹²⁴⁾ Sezione 48, paragrafo 3, della legge del 2018 sulla protezione dei dati.

⁽¹²⁵⁾ Cfr. ad esempio *Guide to Law Enforcement Processing* sul diritto di accesso, disponibile al seguente indirizzo: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8>.

⁽¹²⁶⁾ Cfr. ad esempio il manuale *Data Protection Manual for Police Data Protection Professional* pubblicato dal *National Police Chief Counsel* (cfr. nota 27) o gli orientamenti forniti dal *Serious Fraud Office*, disponibili al seguente indirizzo: <https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/>.

⁽¹²⁷⁾ *Data protection Manual* del *National Police Chief Counsel*, pag. 140 (nota 27).

⁽¹²⁸⁾ Secondo il *Data protection Manual* del *National Police Chief Counsel*, è probabile che evitare di ostacolare indagini, inchieste o procedimenti ufficiali o giudiziari sia pertinente per i dati personali trattati per indagini, procedimenti giudiziari in materia di famiglia, indagini disciplinari interne non penali ed inchieste quali un'inchiesta indipendente in merito ad abusi sessuali su minori; proteggere i diritti e le libertà di altri è invece pertinente per i dati personali che sarebbero riferiti anche ad altre persone fisiche oltre che al richiedente (*Data protection Manual* del *National Police Chief Counsel*, pagina 140, cfr. nota 27).

⁽¹²⁹⁾ Sezione 79 della legge del 2018 sulla protezione dei dati.

⁽¹³⁰⁾ *Orientamenti governativi del Regno Unito sui certificati di sicurezza nazionale*, disponibili 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.

- (70) Inoltre, laddove sia limitato un diritto di un interessato, l'autorità competente deve informarlo, senza ingiustificato ritardo, del fatto che i suoi diritti sono stati limitati, dei motivi di tale limitazione e dei mezzi di ricorso disponibili, fatto salvo il caso in cui fornire tali informazioni comprometta il motivo per il quale la limitazione è stata applicata ⁽¹³¹⁾. Come ulteriore garanzia contro l'uso improprio delle limitazioni, il titolare del trattamento deve registrare i motivi per cui limita le informazioni e rendere la registrazione disponibile all'ICO, laddove richiesto ⁽¹³²⁾.
- (71) Se il titolare del trattamento si rifiuta di fornire ulteriori informazioni sulla trasparenza oppure nega l'accesso o rifiuta una richiesta di rettifica, cancellazione o limitazione del trattamento, la persona fisica può richiedere all'ICO di indagare per stabilire se il titolare del trattamento ha applicato la limitazione in maniera lecita ⁽¹³³⁾. L'interessato può inoltre promuovere un reclamo presso l'ICO o adire un organo giurisdizionale affinché quest'ultimo ordini al titolare del trattamento di soddisfare la richiesta ⁽¹³⁴⁾.

2.4.7.2. Processo decisionale automatizzato

- (72) Le sezioni 49 e 50 della legge del 2018 sulla protezione dei dati trattano rispettivamente i diritti relativi al processo decisionale automatizzato e alle garanzie da applicare ⁽¹³⁵⁾. Analogamente a quanto previsto dall'articolo 11 della direttiva (UE) 2016/680, il titolare del trattamento può prendere una decisione determinante basata esclusivamente sul trattamento automatizzato di dati personali soltanto se ciò è necessario o autorizzato dalla legge ⁽¹³⁶⁾. Una decisione è determinante se produce effetti giuridici negativi nei confronti dell'interessato o incide significativamente sulla sua persona ⁽¹³⁷⁾.
- (73) Laddove il titolare del trattamento sia tenuto o autorizzato dalla legge a prendere una decisione significativa, la sezione 50 della legge del 2018 sulla protezione dei dati stabilisce le garanzie che si applicano a tale decisione (definita come «decisione significativa qualificativa»). Non appena ragionevolmente praticabile, il titolare del trattamento deve notificare all'interessato che è stata adottata tale decisione. L'interessato dispone quindi di un mese di tempo per richiedere al titolare del trattamento di riconsiderare la decisione o di adottare una nuova decisione non basata esclusivamente sul trattamento automatizzato. Il titolare del trattamento deve prendere in considerazione la richiesta e informare l'interessato in merito agli esiti di tale valutazione. La legge del 2018 sulla protezione dei dati riconosce al segretario di Stato il potere di adottare regolamenti che prevedano garanzie supplementari ⁽¹³⁸⁾. Non sono ancora stati adottati regolamenti di tale sorta.

2.4.8. Trasferimenti successivi

- (74) Il livello di protezione dei dati personali trasferiti da un'autorità di contrasto di uno Stato membro verso un'autorità di contrasto del 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 dell'autorità di contrasto 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.

⁽¹³¹⁾ Sezione 44, paragrafi 5 e 6; sezione 45, paragrafi 5 e 6; sezione 48, paragrafo 4, della legge del 2018 sulla protezione dei dati.

⁽¹³²⁾ Sezione 44, paragrafo 7; sezione 45, paragrafo 7; sezione 48, paragrafo 6, della legge del 2018 sulla protezione dei dati.

⁽¹³³⁾ Sezione 51 della legge del 2018 sulla protezione dei dati.

⁽¹³⁴⁾ Sezione 167 della legge del 2018 sulla protezione dei dati.

⁽¹³⁵⁾ Per quanto concerne l'ambito di applicazione del trattamento automatizzato, nelle note esplicative sulla legge del 2018 sulla protezione dei dati si afferma che tali disposizioni fanno riferimento a un processo decisionale completamente automatizzato e non a un trattamento automatizzato. Si parla di trattamento automatizzato (compresa la profilazione) quando viene eseguita un'operazione su dati senza che sia necessario l'intervento umano. Nelle attività di contrasto si ricorre regolarmente a tale trattamento per filtrare serie di dati di grandi dimensioni per portarle a dimensioni gestibili da parte di un operatore umano che può quindi utilizzarle. Il processo decisionale automatizzato è una forma di trattamento automatizzato e richiede che la decisione finale sia presa senza interferenza umana (Note esplicative sulla legge sulla protezione dei dati, punto 204, cfr. nota 45).

⁽¹³⁶⁾ Oltre alle protezioni previste dalla legge sulla protezione dei dati, il quadro giuridico del Regno Unito prevede altre limitazioni che si applicano alle autorità di contrasto e che impedirebbero il trattamento automatizzato (compresa la profilazione) da cui deriverebbe una discriminazione illecita. La legge del 1998 sui diritti umani integra nel diritto del Regno Unito i diritti sanciti dalla CEDU, compreso il divieto di discriminazione sancito dall'articolo 14 della convenzione. Analogamente, la legge del 2010 sulla parità vieta la discriminazione nei confronti di persone con caratteristiche protette (tra cui sesso, razza, disabilità ecc.).

⁽¹³⁷⁾ Sezione 49, paragrafo 2, della legge del 2018 sulla protezione dei dati.

⁽¹³⁸⁾ Sezione 50, paragrafo 4, della legge del 2018 sulla protezione dei dati.

- (75) Il regime del Regno Unito in materia di trasferimenti internazionali è disciplinato dalla parte 3, capo 5, della legge del 2018 sulla protezione dei dati ⁽¹³⁹⁾ e riflette l'approccio adottato nel capo V della direttiva (UE) 2016/680. In particolare, al fine di trasferire dati personali verso un paese terzo, un'autorità competente deve soddisfare tre condizioni: a) il trasferimento deve essere necessario per una finalità di contrasto; b) il trasferimento i) deve essere basato su un regolamento di adeguatezza in relazione a tale paese terzo; ii) qualora non sia basato su un regolamento di adeguatezza, si deve basare sull'esistenza di garanzie adeguate; iii) qualora non sia basato su un regolamento di adeguatezza né su garanzie adeguate, si deve basare su circostanze speciali; c) il destinatario del trasferimento deve essere: i) un'autorità competente (ossia l'equivalente di un'autorità competente) nel paese terzo; ii) una «organizzazione internazionale pertinente», ad esempio un organismo internazionale che svolge funzioni corrispondenti a una delle finalità di contrasto; o iii) una persona diversa da un'autorità competente, ma soltanto se il trasferimento è strettamente necessario per lo svolgimento di una delle finalità di contrasto; non vi sono diritti e libertà fondamentali dell'interessato che prevalgano sull'interesse pubblico che rende necessario il trasferimento; un trasferimento dei dati personali a un'autorità competente nel paese terzo sarebbe inefficace o inadeguato; e il destinatario è informato delle finalità per le quali i dati possono essere trattati ⁽¹⁴⁰⁾.
- (76) I regolamenti di adeguatezza relativi a un paese terzo, un territorio o un settore all'interno di un paese terzo, un'organizzazione internazionale o una descrizione ⁽¹⁴¹⁾ di tale paese, territorio, settore od organizzazione sono adottati dal segretario di Stato. Per quanto concerne il livello di protezione da soddisfare, il segretario di Stato deve valutare se tale territorio/settore/organizzazione garantisce un livello adeguato di protezione dei dati personali. La sezione 74 A, paragrafo 4, della legge del 2018 sulla protezione dei dati specifica che, a tal fine, il segretario di Stato deve considerare una serie di aspetti che riflettono quelli elencati all'articolo 36 della direttiva (UE) 2016/680 ⁽¹⁴²⁾. A tale riguardo, dalla fine del periodo di transizione la parte 3 della legge del 2018 sulla protezione dei dati costituisce «legislazione interna derivata da quella dell'Unione» che, come spiegato, sarà interpretata dagli organi giurisdizionali del Regno Unito in conformità con la giurisprudenza pertinente della Corte di giustizia antecedente al recesso del Regno Unito dall'Unione e con i principi generali del diritto dell'Unione, così come efficaci immediatamente prima della fine del periodo di transizione. Rientra in tale contesto la nozione di «equivalenza sostanziale» che si applicherà quindi alle valutazioni di adeguatezza effettuate dalle autorità del Regno Unito.
- (77) Per quanto riguarda la procedura, i regolamenti 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

⁽¹³⁹⁾ Tale nuovo quadro è entrato in vigore alla fine del periodo di transizione, compreso il potere spettante al segretario di Stato per effettuare regolamenti di adeguatezza. Tuttavia i regolamenti DPPEC (in particolare, i punti da 10 a 12 dell'allegato 21, che tali regolamenti inseriscono nella legge del 2018 sulla protezione dei dati) prevedono che determinati trasferimenti di dati personali alla fine del periodo di transizione e successivamente siano trattati come se fossero basati su regolamenti di adeguatezza. Tali trasferimenti includono quelli verso paesi terzi che sono oggetto di una decisione di adeguatezza dell'UE alla fine del periodo di transizione nonché verso Stati membri dell'UE, verso Stati EFTA e verso il territorio di Gibilterra, in virtù della loro applicazione della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (gli Stati EFTA applicano la direttiva (UE) 2016/680 in conseguenza dei loro obblighi a norma dell'*acquis* di Schengen). Ciò significa che alla fine del periodo di transizione i trasferimenti verso tali paesi possono continuare come prima dell'uscita dell'UE. Dopo la fine del periodo di transizione, il segretario dello Stato deve condurre un riesame degli accertamenti di adeguatezza entro 4 anni.

⁽¹⁴⁰⁾ Sezioni 73 e 77 della legge del 2018 sulla protezione dei dati.

⁽¹⁴¹⁾ 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 un regolamento di adeguatezza in relazione soltanto a un certo tipo di trasferimenti di dati).

⁽¹⁴²⁾ A norma della sezione 74 A, paragrafo 4, della legge del 2018 sulla protezione dei dati, nel valutare l'adeguatezza del livello di protezione il segretario di Stato deve tenere conto, in particolare: a) dello Stato di diritto, del rispetto dei diritti umani e delle libertà fondamentali, della legislazione pertinente, tanto generale quanto settoriale, anche in materia di sicurezza pubblica, difesa, sicurezza nazionale e diritto penale, nonché dell'accesso da parte di autorità pubbliche ai dati personali, nonché dell'attuazione di tale legislazione, delle norme sulla protezione dei dati, delle norme professionali e delle misure di sicurezza, comprese le norme per il trasferimento successivo di dati personali verso un altro paese terzo o un'organizzazione internazionale, che sono rispettate in tale paese od organizzazione internazionale, della giurisprudenza così come dei diritti effettivi e azionabili degli interessati e dei mezzi di ricorso effettivi in sede amministrativa e giudiziale per gli interessati i cui dati personali vengono trasferiti; b) dell'esistenza e del funzionamento effettivo di una o più autorità di controllo indipendenti nel paese terzo o a cui un'organizzazione internazionale sia soggetta, aventi la competenza per assicurare e imporre il rispetto delle norme in materia di protezione dei dati, compresi adeguati poteri esecutivi, per fornire assistenza e consulenza agli interessati nell'esercizio dei loro diritti nonché per cooperare con il commissario; e c) degli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione oppure di altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti, nonché dalla partecipazione del paese terzo o dell'organizzazione in questione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali.

adeguatezza del Regno Unito il segretario di Stato deve consultare l'ICO ⁽¹⁴³⁾. 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 esaminarli e hanno la facoltà di presentare una mozione di annullamento entro un termine di 40 giorni ⁽¹⁴⁴⁾.

- (78) Ai sensi della sezione 74B, paragrafo 1, della legge del 2018 sulla protezione dei dati, i regolamenti di adeguatezza devono essere riesaminati a intervalli di tempo non superiori a quattro anni e il segretario di Stato deve monitorare continuamente 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.
- (79) Analogamente a quanto previsto dall'articolo 37 della direttiva (UE) 2016/680, in assenza di un regolamento di adeguatezza, un trasferimento di dati personali nel settore delle attività di contrasto è possibile qualora siano in atto garanzie adeguate. Tali garanzie sono fornite mediante: a) uno strumento giuridicamente vincolante contenente garanzie adeguate per la protezione dei dati personali; o b) una valutazione effettuata dal titolare del trattamento che, avendo esaminato tutte le circostanze relative al trasferimento, conclude che esistono garanzie adeguate per proteggere i dati ⁽¹⁴⁵⁾. Inoltre, quando i trasferimenti si basano su garanzie adeguate, la legge del 2018 sulla protezione dei dati prevede che, oltre al normale ruolo di vigilanza dell'ICO, le autorità competenti forniscano a quest'ultimo informazioni specifiche sui trasferimenti ⁽¹⁴⁶⁾.
- (80) Se non si basa su una decisione di adeguatezza né su garanzie adeguate, il trasferimento può avvenire soltanto in determinate circostanze specifiche, indicate come «circostanze speciali» ⁽¹⁴⁷⁾. 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 legale (ad esempio in relazione a procedimenti giudiziari o per ottenere consulenza legale) ⁽¹⁴⁸⁾. 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 ⁽¹⁴⁹⁾. 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.
- (81) In tali circostanze occorre documentare e trasmettere all'ICO, su richiesta, la data, l'ora e la giustificazione del trasferimento, il nome del destinatario e qualsiasi altra informazione pertinente in merito a quest'ultimo, così come una descrizione dei dati personali trasferiti ⁽¹⁵⁰⁾.
- (82) La sezione 78 della legge del 2018 sulla protezione dei dati disciplina lo scenario dei «trasferimenti successivi», ossia i casi in cui dati personali che sono stati trasferiti dal Regno Unito a un paese terzo vengono successivamente trasferiti in un altro paese terzo o ad un'organizzazione internazionale. Conformemente alla sezione 78, paragrafo 1, il titolare del trattamento che trasferisce i dati dal Regno Unito deve imporre come condizione del trasferimento il fatto che i dati non siano ulteriormente trasferiti verso un paese terzo senza l'autorizzazione del titolare del trattamento che effettua il trasferimento. Inoltre, conformemente alla sezione 78, paragrafo 3, e analogamente a quanto previsto all'articolo 35, paragrafo 1, lettera e), della direttiva (UE) 2016/680, qualora sia richiesta

⁽¹⁴³⁾ Si veda il protocollo d'intesa tra il segretario di Stato per il dipartimento per il Digitale, la cultura, i media e lo sport (*Department for Digital, Culture, MEDIA and Sport*) e l'ICO sul ruolo dell'ICO in relazione alla nuova valutazione di 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>.

⁽¹⁴⁴⁾ Durante tale termine di 40 giorni, entrambe le camere del parlamento hanno l'opportunità, qualora lo desiderino, di votare contro i regolamenti; laddove tale votazione abbia esito positivo, i regolamenti cesseranno in definitiva di avere ulteriore effetto giuridico.

⁽¹⁴⁵⁾ Sezione 75 della legge del 2018 sulla protezione dei dati.

⁽¹⁴⁶⁾ Conformemente alla sezione 75, paragrafo 3, della legge del 2018 sulla protezione dei dati, nei casi in cui un trasferimento di dati avvenga facendo affidamento su garanzie adeguate: a) il trasferimento deve essere documentato; b) la documentazione deve essere fornita all'ICO su richiesta; c) la documentazione deve comprendere, in particolare: i) la data e l'ora del trasferimento; ii) il nome del destinatario e qualsiasi altra informazione pertinente in merito allo stesso; iii) la giustificazione per il trasferimento; e iv) una descrizione dei dati personali trasferiti.

⁽¹⁴⁷⁾ *Guide to Law Enforcement Processing*, «Are there any special circumstances?», disponibile al seguente indirizzo: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3>.

⁽¹⁴⁸⁾ Sezione 76 della legge del 2018 sulla protezione dei dati.

⁽¹⁴⁹⁾ Sezione 76 della legge del 2018 sulla protezione dei dati.

⁽¹⁵⁰⁾ Sezione 76, paragrafo 3, della legge del 2018 sulla protezione dei dati.

un'autorizzazione di questo tipo si applica una serie di prescrizioni sostanziali. Nello specifico, nel decidere se autorizzare o meno il trasferimento, un'autorità competente deve assicurarsi che l'ulteriore trasferimento sia necessario per una finalità di contrasto e considerare, tra gli altri fattori: a) la gravità delle circostanze che hanno portato alla richiesta di autorizzazione; b) la finalità per la quale i dati personali sono stati originariamente trasferiti; e c) le norme per la protezione dei dati personali che si applicano nel paese terzo o all'organizzazione internazionale verso cui i dati personali verrebbero trasferiti.

- (83) Inoltre, qualora i dati oggetto di ulteriore trasferimento dal Regno Unito siano stati originariamente trasferiti dall'Unione europea, si applicano garanzie supplementari.
- (84) In primo luogo, la sezione 73, paragrafo 1, lettera b), della legge del 2018 sulla protezione dei dati - analogamente all'articolo 35, paragrafo 1, lettera c), della direttiva (UE) 2016/680 - prevede che, qualora i dati personali siano stati originariamente trasmessi o altrimenti messi a disposizione del titolare del trattamento o di un'altra autorità competente da uno Stato membro, quest'ultimo o qualsiasi persona stabilita in tale Stato membro che è un'autorità competente ai fini della direttiva (UE) 2016/680 debba aver autorizzato il trasferimento in conformità con la normativa di tale Stato membro.
- (85) Tuttavia, analogamente all'articolo 35, paragrafo 2, della direttiva (UE) 2016/680, tale autorizzazione non è richiesta quando: a) il trasferimento è necessario per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un paese terzo o agli interessi vitali di uno Stato membro; e b) tale autorizzazione non può essere ottenuta tempestivamente. In tal caso l'autorità nello Stato membro che sarebbe stata responsabile della decisione in merito all'autorizzazione del trasferimento deve essere informata senza indugio ⁽¹⁵¹⁾.
- (86) In secondo luogo, lo stesso si applica per i dati originariamente trasferiti dall'Unione europea al Regno Unito e in seguito ulteriormente trasferiti dal Regno Unito a un paese terzo, che a sua volta li trasferisca ulteriormente a un altro paese terzo. In tal caso, conformemente alla sezione 78, paragrafo 4, l'autorità competente del Regno Unito non può autorizzare quest'ultimo trasferimento, a norma della sezione 78, paragrafo 1, a meno che lo Stato membro che ha originariamente trasferito i dati in questione, o qualsiasi persona basata in tale Stato membro che sia un'autorità competente ai fini della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, non abbia autorizzato il trasferimento in conformità della legge dello Stato membro stesso. Tali misure di salvaguardia sono importanti in quanto permettono alle autorità degli Stati membri di garantire la continuità della protezione, nel rispetto della legge dell'UE sulla protezione dei dati, lungo tutta la «catena di trasferimento».
- (87) Questo nuovo quadro per i trasferimenti internazionali è diventato applicabile alla fine del periodo di transizione ⁽¹⁵²⁾. Tuttavia i punti da 10 a 12 dell'allegato 21 (introdotto dai regolamenti DPPC) prevedono 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 membro, uno Stato EFTA, un paese terzo che è oggetto di una decisione di adeguatezza dell'UE alla fine del periodo di transizione e il territorio di Gibilterra. Di conseguenza i trasferimenti verso tali paesi possono continuare come prima del recesso del Regno Unito dall'Unione. Dopo la fine del periodo di transizione, il segretario di Stato deve condurre un riesame di tali accertamenti di adeguatezza entro un termine di quattro anni, ossia entro la fine di 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 norma relativa alla scadenza e le disposizioni transitorie pertinenti non cesseranno automaticamente di avere effetto se il riesame non viene completato entro la fine di dicembre del 2024.

2.4.9. Responsabilizzazione

- (88) Secondo il principio di responsabilizzazione, le autorità pubbliche che trattano dati sono tenute 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.
- (89) Tale principio si riflette nella sezione 56 della legge del 2018 sulla protezione dei dati, che introduce un obbligo generale di responsabilizzazione per il titolare del trattamento, ossia l'obbligo di attuare misure tecniche e organizzative adeguate per assicurare, e poter dimostrare, che il trattamento dei dati personali è conforme ai requisiti di cui alla parte 3 della legge del 2018 sulla protezione dei dati. Le misure attuate devono essere riviste e aggiornate se necessario e, se proporzionato in relazione al trattamento, comprendere politiche adeguate di protezione dei dati.

⁽¹⁵¹⁾ Sezione 73, paragrafo 5, della legge del 2018 sulla protezione dei dati.

⁽¹⁵²⁾ L'applicabilità di questo nuovo quadro deve essere letta alla luce dell'articolo 728 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) («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](https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:22020A1231(01)&from=IT).

- (90) In linea con il capo IV della direttiva (UE) 2016/680, gli articoli da 55 a 71 della legge del 2018 sulla protezione dei dati prevedono diversi meccanismi per garantire la responsabilizzazione e consentire ai titolari del trattamento e ai responsabili del trattamento di dimostrare la conformità. In particolare i titolari del trattamento sono tenuti ad attuare misure di protezione dei dati fin dalla progettazione e per impostazione predefinita, ossia a garantire che i principi di protezione dei dati siano attuati in modo efficace, e sono tenuti a mantenere registri di tutte le categorie di trattamenti per i quali il titolare del trattamento è responsabile (comprese le informazioni sull'identità del titolare del trattamento, i dati di contatto del responsabile della protezione dei dati, le finalità del trattamento, le categorie di destinatari delle comunicazioni e una descrizione delle categorie di interessati e dei dati personali) e a mantenere tali registri a disposizione dell'ICO su richiesta. Il titolare del trattamento e il responsabile del trattamento devono altresì tenere registri per determinate operazioni di trattamento e metterli a disposizione dell'ICO ⁽¹⁵³⁾. I titolari del trattamento sono altresì specificamente tenuti a cooperare con l'ICO nell'esecuzione dei compiti spettanti a quest'ultimo.
- (91) La legge del 2018 sulla protezione dei dati stabilisce requisiti supplementari per un trattamento che determini probabilmente un rischio elevato per i diritti e le libertà delle persone fisiche, tra cui l'obbligo di effettuare valutazioni d'impatto sulla protezione dei dati e di consultare l'ICO prima del trattamento qualora una di tali valutazioni indichi che il trattamento comporta un rischio elevato per i diritti e le libertà delle persone fisiche (in assenza di misure per attenuare il rischio).
- (92) Il titolare del trattamento deve inoltre nominare un responsabile della protezione dei dati, fatto salvo il caso in cui tale titolare sia un organo giurisdizionale o un'altra autorità giudiziaria che agisce nell'adempimento delle sue funzioni giurisdizionali ⁽¹⁵⁴⁾. Il titolare del trattamento deve garantire che il responsabile della protezione dei dati sia coinvolto in tutte le questioni relative alla protezione dei dati personali, disponga delle risorse necessarie nonché dell'accesso ai dati personali e alle operazioni di trattamento, e possa svolgere i propri compiti in maniera indipendente. I compiti del responsabile della protezione dei dati sono stabiliti nella sezione 71 della legge del 2018 sulla protezione dei dati e comprendono la fornitura di informazioni e consulenza, il controllo del rispetto delle norme e la cooperazione con l'ICO, in relazione al quale egli funge da punto di contatto. Nello svolgimento dei suoi compiti, il responsabile della protezione dei dati deve prendere in considerazione i rischi associati alle operazioni di trattamento, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

2.5. Vigilanza e applicazione

2.5.1. Vigilanza indipendente

- (93) Al fine di garantire un livello adeguato di protezione dei dati anche nella pratica, deve 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 deve agire in piena indipendenza e imparzialità nell'esercizio delle proprie funzioni e dei propri poteri.
- (94) 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 (ICO)* ⁽¹⁵⁵⁾, il quale vigila anche sul trattamento dei dati personali da parte delle autorità competenti che rientra nell'ambito di applicazione della parte 3 della legge del 2018 sulla protezione dei dati ⁽¹⁵⁶⁾. L'ICO è una «*corporation sole*», ossia un'entità giuridica distinta costituita da un socio unico. Nelle sue attività l'ICO è sostenuto da un ufficio, il cui personale al 31 marzo 2020 era composto di 768 membri permanenti ⁽¹⁵⁷⁾. Il dipartimento di riferimento dell'ICO è il dipartimento per il Digitale, la cultura, i media e lo sport ⁽¹⁵⁸⁾.

⁽¹⁵³⁾ Sezione 62 della legge del 2018 sulla protezione dei dati.

⁽¹⁵⁴⁾ Sezione 69 della legge del 2018 sulla protezione dei dati.

⁽¹⁵⁵⁾ Articolo 36, paragrafo 2, lettera b), della direttiva (UE) 2016/680.

⁽¹⁵⁶⁾ Sezione 116 della legge del 2018 sulla protezione dei dati.

⁽¹⁵⁷⁾ *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>.

⁽¹⁵⁸⁾ Un accordo di gestione disciplina la relazione tra le due entità. In particolare, tra le principali responsabilità del Dipartimento per il Digitale, la cultura, i media e lo sport in qualità di dipartimento promotore figurano: garantire che l'ICO disponga di finanziamenti e risorse adeguati; rappresentare gli interessi dell'ICO 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>).

- (95) L'indipendenza dell'ICO è sancita esplicitamente dall'articolo 52 del GDPR del Regno Unito, che riflette i requisiti previsti all'articolo 52, paragrafi da 1 a 3, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ⁽¹⁵⁹⁾. L'ICO 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 sollecitare né accettare istruzioni da alcuno. Deve inoltre 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.
- (96) Le condizioni per la nomina e la revoca dell'incarico dell'ICO sono stabilite nell'allegato 12 della legge del 2018 sulla protezione dei dati. L'ICO 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* ⁽¹⁶⁰⁾ (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 ⁽¹⁶¹⁾.
- (97) L'ICO resta in carica per un mandato massimo di sette anni. Il suo incarico può essere revocato dalla Regina a seguito di una raccomandazione formulata da entrambe le camere del parlamento ⁽¹⁶²⁾. Non può essere presentata alcuna richiesta di rimozione dall'incarico dell'ICO ad alcuna delle camere del parlamento fintantoché un ministro non abbia presentato a tale camera una relazione nella quale si dichiara convinto che l'ICO si sia reso colpevole di una colpa grave e/o non soddisfi più le condizioni richieste per lo svolgimento delle sue funzioni ⁽¹⁶³⁾.
- (98) I finanziamenti dell'ICO provengono da tre fonti: i) i contributi spese in materia di protezione dei dati versati dai titolari del trattamento, che sono fissati da regolamenti di un segretario di Stato ⁽¹⁶⁴⁾ e ammontano all'85 %-90 % del bilancio annuale dell'ICO ⁽¹⁶⁵⁾; ii) una sovvenzione che può essere corrisposta dal governo all'ICO ed è principalmente utilizzata per finanziare i costi operativi dell'ICO in relazione a compiti concernenti attività non correlate alla protezione di dati ⁽¹⁶⁶⁾; iii) commissioni addebitate per servizi ⁽¹⁶⁷⁾. Attualmente, tali commissioni non vengono addebitate.
- (99) Le funzioni generali dell'ICO in relazione al trattamento dei dati personali a cui si applica la parte 3 della legge del 2018 sulla protezione dei dati sono stabilite nell'allegato 13 di quest'ultima legge. Tali funzioni comprendono il monitoraggio e l'applicazione delle norme di cui alla parte 3 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
-
- ⁽¹⁵⁹⁾ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).
- ⁽¹⁶⁰⁾ *Governance Code on Public Appointments*, disponibile al seguente indirizzo: <https://www.gov.uk/government/publications/governance-code-for-public-appointments>.
- ⁽¹⁶¹⁾ *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/cmcomeds/990/990.pdf>.
- ⁽¹⁶²⁾ Una raccomandazione («address») è una mozione presentata dinanzi al parlamento che intende comunicare al monarca il parere del parlamento in merito a una questione specifica.
- ⁽¹⁶³⁾ Allegato 12, punto 3, della legge del 2018 sulla protezione dei dati.
- ⁽¹⁶⁴⁾ Sezione 137 della legge del 2018 sulla protezione dei dati.
- ⁽¹⁶⁵⁾ Le sezioni 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, della legge del 2018 sulla protezione dei dati elenca le questioni che il segretario di Stato deve considerare quando emette regolamenti che specificano l'importo che le diverse organizzazioni devono versare. La sezione 138, paragrafo 1, e la sezione 182 della legge del 2018 sulla protezione dei dati contengono inoltre un requisito giuridico che impone al segretario di Stato di consultare l'ICO 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'ICO è tenuto a riesaminare 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, tranne nel caso in cui 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 adottati fino a quando non sono stati approvati mediante una risoluzione di ciascuna camera del parlamento.
- ⁽¹⁶⁶⁾ 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 punto 9 dell'allegato 12 della legge del 2018 sulla protezione dei dati. In seguito a consultazione con l'ICO, il dipartimento per il Digitale, la cultura, i media e lo sport corrisponderà all'ICO somme adeguate (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 158).
- ⁽¹⁶⁷⁾ Sezione 134 della legge del 2018 sulla protezione dei dati.

trattamento e dei responsabili del trattamento in merito ai loro obblighi, la comunicazione di informazioni a un interessato in merito all'esercizio dei diritti di quest'ultimo, e lo svolgimento di indagini. Ai fini del mantenimento dell'indipendenza del potere giudiziario, l'ICO 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, illustrati in appresso.

2.5.1.1 Applicazione (sanzioni comprese)

(100) L'ICO ha poteri generali di indagine, correttivi, autorizzativi e consultivi in relazione al trattamento di dati personali cui si applica la parte 3 della legge del 2018 sulla protezione dei dati. L'ICO dispone dei poteri per notificare al titolare del trattamento o al responsabile del trattamento una presunta violazione della parte 3, di rivolgere avvertimenti al titolare del trattamento o al responsabile sul fatto che i trattamenti previsti violano verosimilmente le disposizioni della parte 3, e di rivolgere ammonimenti al titolare del trattamento o al responsabile del trattamento laddove i trattamenti abbiano violato le disposizioni della parte 3. Inoltre, su iniziativa propria o su richiesta, l'ICO può emettere pareri rivolti al parlamento del Regno Unito, al governo o ad altre istituzioni e ad altri organismi, nonché al pubblico, in merito a qualsiasi questione relativa alla protezione dei dati personali ⁽¹⁶⁸⁾.

(101) L'ICO dispone anche dei poteri per:

- 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» (*information notice*) ⁽¹⁶⁹⁾;
- effettuare indagini e verifiche trasmettendo un «avviso di valutazione» (*assessment notice*), che può imporre al titolare del trattamento o al responsabile del trattamento di consentire all'ICO di accedere a locali specificati, ispezionare o esaminare documenti o apparecchiature, e interrogare persone che trattano dati personali per conto del titolare del trattamento ⁽¹⁷⁰⁾;
- ottenere altrimenti l'accesso a documenti di titolari del trattamento e responsabili del trattamento così come l'accesso ai loro locali in conformità con la sezione 154 della legge del 2018 sulla protezione dei dati («poteri di accesso e ispezione»);
- esercitare poteri correttivi, anche mediante avvertimenti e ammonimenti, oppure emettere ordini per mezzo di un «avviso di esecuzione» (*enforcement notice*), che impone ai titolari del trattamento/responsabili del trattamento di adottare o di astenersi dall'adottare misure specificate ⁽¹⁷¹⁾; e
- comminare sanzioni amministrative pecuniarie sotto forma di un «avviso di irrogazione di sanzioni» (*penalty notice*) ⁽¹⁷²⁾.

(102) Il documento *Regulatory Action Policy* dell'ICO stabilisce le circostanze nelle quali quest'ultimo emetterà rispettivamente un avviso di informazione, valutazione, esecuzione e irrogazione di sanzioni ⁽¹⁷³⁾. Un avviso di esecuzione può imporre i requisiti che l'ICO ritiene opportuni al fine di porre rimedio a un inadempimento. Un avviso di irrogazione di sanzioni impone a una persona di corrispondere all'ICO un importo specificato nell'avviso stesso; può essere notificato in caso di mancato rispetto di talune disposizioni della legge del 2018 sulla protezione dei dati ⁽¹⁷⁴⁾ oppure può essere notificato a un titolare del trattamento o a un responsabile del trattamento che non ha rispettato un avviso di informazione, un avviso di valutazione o un avviso di esecuzione.

(103) Più specificamente, nel decidere se notificare o meno un avviso di irrogazione di sanzioni a un titolare del trattamento o a un responsabile del trattamento e determinare l'ammontare della sanzione, l'ICO deve tenere conto delle questioni elencate alla sezione 155, paragrafo 3, della legge del 2018 sulla protezione dei dati, tra cui la natura e la gravità della violazione, il carattere doloso o colposo della violazione, le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati, il grado di

⁽¹⁶⁸⁾ Allegato 13, paragrafo 2, della legge del 2018 sulla protezione dei dati.

⁽¹⁶⁹⁾ Sezione 142 della legge del 2018 sulla protezione dei dati (con le limitazioni di cui alla sezione 143 della medesima legge).

⁽¹⁷⁰⁾ Sezione 146 della legge del 2018 sulla protezione dei dati (con le limitazioni di cui alla sezione 147 della medesima legge).

⁽¹⁷¹⁾ Sezioni da 149 a 151 della legge del 2018 sulla protezione dei dati (con le limitazioni di cui alla sezione 152 della medesima legge).

⁽¹⁷²⁾ Sezione 155 della legge del 2018 sulla protezione dei dati (con le limitazioni di cui alla sezione 156 della medesima legge).

⁽¹⁷³⁾ *Regulatory Action Policy*, disponibile al seguente indirizzo: <https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf>.

⁽¹⁷⁴⁾ In particolare l'ICO può emettere un avviso di irrogazione di sanzioni per il mancato rispetto di disposizioni di cui alla sezione 149, paragrafo 2, 3, 4 o 5, della legge del 2018 sulla protezione dei dati.

responsabilità del titolare del trattamento o del responsabile del trattamento (tenendo conto delle misure tecniche e organizzative da essi messe in atto) nonché eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento, le categorie di dati personali interessate dalla violazione e la possibilità o meno che la sanzione sia effettiva, proporzionata e dissuasiva.

- (104) L'ammontare massimo della sanzione che può essere comminata mediante un avviso di irrogazione di sanzioni è a) 17 500 000 GBP in relazione al mancato rispetto di principi di protezione dei dati (sezioni 35, 36, 37, sezione 38, paragrafo 1, sezione 39, paragrafo 1, e sezione 40 della legge del 2018 sulla protezione dei dati), di obblighi di trasparenza e di diritti individuali (sezioni 44, 45, 46, 47, 48, 49, 52 e 53 della legge del 2018 sulla protezione dei dati) nonché dei principi per i trasferimenti internazionali di dati personali (sezioni 73, 75, 76, 77 o 78 della legge del 2018 sulla protezione dei dati); b) 8 700 000 GBP negli altri casi ⁽¹⁷⁵⁾. In relazione al mancato rispetto di un avviso di informazione, di un avviso di valutazione o di un avviso di esecuzione, l'importo massimo della sanzione che può essere comminata mediante un avviso di irrogazione di sanzioni è pari a 17 500 000 GBP.
- (105) Secondo le sue ultime relazioni annuali [2018-2019 ⁽¹⁷⁶⁾, 2019-2020 ⁽¹⁷⁷⁾], l'ICO ha condotto una serie di indagini in relazione al trattamento di dati personali da parte delle autorità di contrasto in ambito penale. Ad esempio, 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. Inoltre l'ICO ha indagato in merito alla banca dati «Gangs Matrix» ⁽¹⁷⁸⁾ 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 nell'utilizzo dei dati.
- (106) Nel novembre del 2018 l'ICO ha emesso un avviso di esecuzione e il servizio di polizia 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.
- (107) Un ulteriore esempio di una recente azione esecutiva è la sanzione pecuniaria di 325 000 GBP comminata dall'ICO nel maggio del 2018 nei confronti del *Crown Prosecution Service*, per aver perso DVD non crittografati contenenti registrazioni di interrogatori di polizia. Inoltre l'ICO ha condotto 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 dei dati delle vittime da parte della polizia.
- (108) Oltre ai suddetti poteri di esecuzione dell'ICO, 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 o della comunicazione 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 ⁽¹⁷⁹⁾; della reidentificazione di informazioni a partire da dati personali anonimizzati senza il consenso del titolare del trattamento responsabile dell'anonimizzazione dei dati personali ⁽¹⁸⁰⁾; dell'ostruzione intenzionale dell'esercizio dei poteri dell'ICO in relazione all'ispezione di dati personali conformemente agli obblighi internazionali ⁽¹⁸¹⁾; del rilascio di dichiarazioni false in risposta a un avviso di informazione o della distruzione di informazioni relative ad avvisi di informazione e di valutazione ⁽¹⁸²⁾.
- (109) L'ICO è altresì tenuto, ai sensi della sezione 139 della legge del 2018 sulla protezione dei dati, a presentare a ciascuna camera del parlamento una relazione generale sull'esercizio delle proprie funzioni ai sensi di tale legge ⁽¹⁸³⁾.

⁽¹⁷⁵⁾ Sezione 157 della legge del 2018 sulla protezione dei dati.

⁽¹⁷⁶⁾ *Information Commissioner's Annual Report and Financial Statements 2018-2019*, disponibile al seguente indirizzo: <https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf>.

⁽¹⁷⁷⁾ *Information Commissioner, Annual Report 2019-2020* (nota 157).

⁽¹⁷⁸⁾ Una banca dati che registrava intelligence in merito a presunti membri di bande criminali e vittime di reati correlati alle bande.

⁽¹⁷⁹⁾ Sezione 170 della legge del 2018 sulla protezione dei dati.

⁽¹⁸⁰⁾ Sezione 171 della legge del 2018 sulla protezione dei dati.

⁽¹⁸¹⁾ Sezione 119 della legge del 2018 sulla protezione dei dati.

⁽¹⁸²⁾ Sezioni 144 e 148 della legge del 2018 sulla protezione dei dati.

⁽¹⁸³⁾ Come indicato nel *Management Agreement*, la relazione annuale deve: i) trattare qualsiasi attività istituzionale, sussidiaria o joint venture soggetta al controllo dell'ICO; ii) rispettare il manuale sulla rendicontazione finanziaria (FRM) del Tesoro; iii) contenere una dichiarazione di governance, che stabilisca le modalità con cui il contabile ha gestito e controllato le risorse utilizzate nell'organizzazione nel corso dell'anno, dimostrando il modo in cui l'organizzazione sta gestendo i rischi per il conseguimento dei suoi scopi e dei suoi obiettivi; e iv) delineare le attività principali e le prestazioni durante l'esercizio finanziario e stabilire in forma sintetica piani di avanzamento (*Management Agreement 2018-2021*, punto 3.26, cfr. nota 158).

2.5.2. Vigilanza sul potere giudiziario

- (110) 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 ⁽¹⁸⁴⁾ e detta vigilanza è esercitata da organismi speciali. Ciò riflette l'approccio dell'articolo 32 della direttiva (UE) 2016/680.
- (111) 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* ⁽¹⁸⁵⁾ (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 ⁽¹⁸⁶⁾ che stabilisce le modalità con cui gli organi giurisdizionali di Inghilterra e Galles trattano i dati personali per espletare una funzione giudiziaria. Un'informativa analoga è stata emessa dalla magistratura dell'Irlanda del Nord ⁽¹⁸⁷⁾ e della Scozia ⁽¹⁸⁸⁾.
- (112) In Irlanda del Nord, il Lord Giudice capo ha nominato un giudice dell'Alta Corte *Data Supervisory Judge* ⁽¹⁸⁹⁾ (DSJ, Giudice incaricato del controllo sui dati), e ha redatto orientamenti per la magistratura dell'Irlanda del Nord 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 ⁽¹⁹⁰⁾.
- (113) 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 stabilito dalle norme sui reclami in materia giudiziaria, che rispecchiano quelle adottate per l'Inghilterra e il Galles ⁽¹⁹¹⁾.
- (114) Infine, nell'ambito della Corte suprema uno dei giudici è incaricato di vigilare in merito alla protezione dei dati.

⁽¹⁸⁴⁾ Sezione 117 della legge del 2018 sulla protezione dei dati.

⁽¹⁸⁵⁾ Tale comitato è competente per l'erogazione di orientamenti e la formazione alla magistratura. Si occupa inoltre dei 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, e fornisce 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, esso può riconsiderare la propria decisione. Sebbene il comitato in sé non commini sanzioni pecuniarie, laddove 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 debba essere intrapresa nei confronti del funzionario in questione. Tali azioni potrebbero essere, 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 al 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.

⁽¹⁸⁶⁾ 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>.

⁽¹⁸⁷⁾ 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>.

⁽¹⁸⁸⁾ 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>

⁽¹⁸⁹⁾ 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.

⁽¹⁹⁰⁾ 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, consiglio, formazione o tutoraggio, avvertimento informale, avvertimento formale, avvertimento finale, limitazione dell'esercizio della professione o rinvio a un organo giurisdizionale. Il codice di pratica sui reclami emessi dal Lord Giudice capo dell'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.._.pdf.

⁽¹⁹¹⁾ 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 lo ritenga necessario (norme equivalenti esistono per i membri degli organi giurisdizionali e sono disponibili al seguente indirizzo: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3. Mezzi di ricorso

- (115) 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.
- (116) Innanzitutto l'interessato ha il diritto di proporre reclamo presso l'ICO 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 ⁽¹⁹²⁾. Come descritto nei considerando 100 e 109, l'ICO ha la competenza di valutare il rispetto della legge del 2018 sulla protezione dei dati da parte del titolare del trattamento e del responsabile del trattamento, di chiedere loro di adottare o di astenersi dall'adottare misure in caso di non conformità nonché di irrogare sanzioni pecuniarie.
- (117) In secondo luogo, la legge del 2018 sulla protezione dei dati riconosce il diritto di ricorso nei confronti dell'ICO. Se l'ICO non fa «progredire» ⁽¹⁹³⁾ un reclamo promosso dall'interessato, il reclamante ha accesso a un ricorso giurisdizionale e può adire un *First-tier Tribunal* ⁽¹⁹⁴⁾ (tribunale di primo grado) chiedendogli di ordinare all'ICO di adottare misure adeguate per dare seguito al reclamo oppure di informare il reclamante dei progressi compiuti in relazione al reclamo ⁽¹⁹⁵⁾. Inoltre chiunque riceva uno degli avvisi di cui sopra (di informazione, di valutazione, di esecuzione o di irrogazione di sanzioni) dall'ICO può impugnarlo adendo un *First-tier Tribunal*. Laddove quest'ultimo ritenga che la decisione dell'ICO non sia conforme alla legge o che l'ICO 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'ICO avrebbe potuto emettere o rendere ⁽¹⁹⁶⁾.
- (118) 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 virtù della sezione 167 della legge del 2018 sulla protezione dei dati. Se, su domanda di un interessato, un organo giurisdizionale dichiara che è 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 o di astenersi dall'adottare le misure specificate nell'ordinanza. Inoltre, a norma della sezione 169 della legge del 2018 sulla protezione dei dati, chiunque 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 nel caso in cui né il titolare del trattamento né il responsabile del trattamento siano in alcun modo responsabili dell'evento che ha cagionato i danni in questione. Sono compresi sia i danni che comportano una perdita finanziaria sia quelli che non la comportano, ad esempio una sofferenza.
- (119) In quarto luogo, 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. I titolari del trattamento di cui alla parte 3 della legge del 2018 sulla protezione dei dati, ossia le autorità competenti, sono sempre autorità pubbliche ai sensi della legge del 1998 sui diritti umani. 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 all'organo giurisdizionale adeguato oppure fare affidamento sui diritti in questione nel contesto di qualsiasi procedimento legale, quando tale persona è (o diventa) vittima dell'atto illecito ⁽¹⁹⁷⁾.

⁽¹⁹²⁾ Sezione 165 della legge del 2018 sulla protezione dei dati.

⁽¹⁹³⁾ La sezione 166 della legge del 2018 sulla protezione dei dati fa riferimento specificamente alle seguenti situazioni: a) l'ICO non adotta misure adeguate per rispondere al reclamo; b) l'ICO 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 tre mesi a decorrere dal momento della ricezione del reclamo da parte dello stesso; oppure c) laddove l'esame del reclamo da parte dell'ICO non venga concluso entro tale termine, quest'ultimo non fornisce al reclamante tali informazioni nel successivo periodo di tre mesi.

⁽¹⁹⁴⁾ 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. In caso di decisione dell'ICO, la camera competente è la *General Regulatory Chamber* avente competenza giurisdizionale su tutto il Regno Unito.

⁽¹⁹⁵⁾ Sezione 166 della legge del 2018 sulla protezione dei dati.

⁽¹⁹⁶⁾ Sezioni 161 e 162 della legge del 2018 sulla protezione dei dati.

⁽¹⁹⁷⁾ Cfr. causa *A. Brown v Commissioner of Police* del 2016 nel contesto della quale l'organo giurisdizionale ha riconosciuto un risarcimento a favore dell'attrice in relazione alla protezione dei dati nell'ambito di un'azione promossa contro il servizio di polizia metropolitana. L'organo giurisdizionale si è pronunciato a favore dell'attrice, accogliendo le sue asserzioni di violazione degli obblighi di cui alla legge del 1998 sulla protezione dei dati, di violazione della legge del 1998 sui diritti umani (e del relativo diritto di cui all'articolo 8 della CEDU) nonché di illecito per uso improprio di informazioni private (il convenuto ha infine ammesso di aver violato la legge sulla protezione dei dati e la CEDU, di conseguenza la sentenza si è concentrata sul definire quale rimedio fosse adeguato). A seguito di tali violazioni, l'organo giurisdizionale ha riconosciuto un risarcimento monetario dei danni a favore dell'attrice.

- (120) 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 ⁽¹⁹⁸⁾. L'organo giurisdizionale può altresì dichiarare che una disposizione del diritto primario è incompatibile con un diritto garantito dalla CEDU.
- (121) 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 CEDU.

2.6. Condivisione successiva

- (122) Il diritto del Regno Unito autorizza la condivisione di dati da parte di un'autorità di contrasto con altre autorità del Regno Unito per finalità diverse da quelle per le quali sono stati inizialmente raccolti (la cosiddetta «condivisione successiva») nel rispetto di determinate condizioni.
- (123) Analogamente a quanto previsto dall'articolo 4, paragrafo 2, della direttiva (UE) 2016/680, la sezione 36, paragrafo 3, della legge del 2018 sulla protezione dei dati prevede che i dati personali raccolti da un'autorità competente per una finalità di contrasto possano 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 per legge a trattare i dati per un'altra finalità e il trattamento sia necessario e proporzionato ⁽¹⁹⁹⁾. In tal caso tutte le garanzie fornite dalla parte 3 della legge del 2018 sulla protezione dei dati e analizzate sopra si applicano al trattamento effettuato dall'autorità ricevente.
- (124) 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 un'autorità pubblica ⁽²⁰⁰⁾ o in caso di un debito nei confronti di un'autorità pubblica o della Corona ⁽²⁰¹⁾; 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* ⁽²⁰²⁾ (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) consente alle autorità pubbliche di divulgare informazioni alle organizzazioni antifrode ai fini della prevenzione delle frodi ⁽²⁰³⁾.
- (125) Tali leggi prevedono esplicitamente che la condivisione di informazioni debba rispettare le norme stabilite nella legge del 2018 sulla protezione dei dati. Inoltre il *College of Policing* ha emesso una pratica professionale autorizzata sulla condivisione di informazioni ⁽²⁰⁴⁾ per aiutare le forze di polizia a rispettare i loro 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 può, naturalmente, essere soggetta a controllo giurisdizionale ⁽²⁰⁵⁾.
- (126) 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 ⁽²⁰⁶⁾. 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 (ad esempio un'autorità finanziaria o fiscale, un'autorità per la concorrenza, un ufficio per l'assistenza ai giovani); 2) quello in cui un'autorità di contrasto penale condivide dati con un'agenzia di intelligence. Nel primo scenario, il trattamento dei dati personali

⁽¹⁹⁸⁾ Sezione 8, paragrafo 1, della legge del 1998 sui diritti umani.

⁽¹⁹⁹⁾ Sezione 36, paragrafo 3, della legge del 2018 sulla protezione dei dati.

⁽²⁰⁰⁾ Sezione 56 della legge del 2017 sull'economia digitale, disponibile al seguente indirizzo: <https://www.legislation.gov.uk/ukpga/2017/30/contents>.

⁽²⁰¹⁾ Sezione 48 della legge del 2017 sull'economia digitale.

⁽²⁰²⁾ Sezione 7 della legge del 2013 sui reati e sugli organi giurisdizionali, disponibile al seguente indirizzo: <https://www.legislation.gov.uk/ukpga/2013/22/contents>.

⁽²⁰³⁾ Sezione 68 della legge del 2007 sui reati gravi, disponibile al seguente indirizzo: <https://www.legislation.gov.uk/ukpga/2007/27/contents>.

⁽²⁰⁴⁾ La pratica professionale autorizzata sulla condivisione delle informazioni è disponibile al seguente indirizzo: <https://www.app.college.police.uk/app-content/information-management/sharing-police-information>.

⁽²⁰⁵⁾ Cfr. ad esempio causa *M 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 un sistema 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.

⁽²⁰⁶⁾ Sezione 36, paragrafo 4, della legge del 2018 sulla protezione dei dati.

rientrerà nell'ambito di applicazione del GDPR del Regno Unito nonché in quello della parte 2 della legge del 2018 sulla protezione dei dati. Come specificato nella decisione adottata ai sensi del regolamento (UE) 2016/679, le garanzie previste dal GDPR del Regno Unito e dalla parte 2 della legge del 2018 sulla protezione dei dati forniscono un livello di protezione sostanzialmente equivalente a quello fornito all'interno dell'Unione ⁽²⁰⁷⁾.

- (127) 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 *Counter Terrorism Act 2008* ⁽²⁰⁸⁾ (legge antiterrorismo del 2008). Conformemente alla legge antiterrorismo del 2008, qualsiasi persona può fornire informazioni a un qualsiasi servizio di intelligence ai fini dell'adempimento di una qualsiasi delle funzioni di tale servizio, compresa la «sicurezza nazionale».
- (128) Per quanto concerne le condizioni in cui i dati possono essere condivisi per finalità di sicurezza nazionale, l'*Intelligence Services Act* (legge sui servizi di intelligence) e la *Security Service Act* (legge sui servizi di sicurezza) limitano la capacità dei servizi di intelligence di ottenere dati a quanto necessario per adempiere le loro funzioni statutarie. Le autorità competenti rientranti nell'ambito di applicazione della parte 3 della legge del 2018 sulla protezione dei dati 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 ⁽²⁰⁹⁾. 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 della legge del 2018 sulla protezione dei dati. Inoltre le autorità di contrasto e i servizi di intelligence sono autorità pubbliche ai fini della legge del 1998 sui diritti umani e devono quindi agire in conformità con i diritti sanciti dalla CEDU, compreso l'articolo 8. Tali requisiti assicurano che ogni 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.
- (129) Il trattamento da parte di servizi di intelligence di dati personali ricevuti od ottenuti da autorità di contrasto per finalità di sicurezza nazionale è soggetto a una serie di condizioni e garanzie ⁽²¹⁰⁾. 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
-
- ⁽²⁰⁷⁾ Decisione di esecuzione della Commissione a norma della direttiva (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito, C(2021)4800.
- ⁽²⁰⁸⁾ Sezione 19 della legge antiterrorismo del 2008, disponibile al seguente indirizzo: <https://www.legislation.gov.uk/ukpga/2008/28/section/19>.
- ⁽²⁰⁹⁾ La sezione 2, paragrafo 2, della legge del 1994 sui servizi di intelligence (cfr. <https://www.legislation.gov.uk/ukpga/1994/13/contents>) 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 sul servizio di sicurezza (cfr. <https://www.legislation.gov.uk/ukpga/1989/5/contents>) 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.
- ⁽²¹⁰⁾ Le garanzie e le limitazioni in relazione ai poteri dei servizi di intelligence sono disciplinate anche dalla legge del 2016 sui poteri di indagine la quale, unitamente alla *Regulation of Investigatory Powers Act 2000* (legge del 2000 sul regolamento sui poteri di indagine) per l'Inghilterra, Galles e Irlanda del Nord e alla *Regulation of Investigatory Powers (Scotland) Act 2000* (legge del 2000 sul regolamento sui poteri di indagine — Scozia) per la Scozia, fornisce la base giuridica per l'esercizio di tali poteri. Tuttavia tali poteri non sono pertinenti nel contesto della «ulteriore condivisione», dato che riguardano la raccolta diretta di dati personali da parte delle agenzie di intelligence. Per una valutazione dei poteri concessi alle agenzie di intelligence ai sensi della legge sui poteri di indagine, si veda la decisione di esecuzione della Commissione a norma della direttiva (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito, C(2021)4800.

particolare, stabilisce i principi fondamentali in materia di protezione dei dati [liceità, equità e trasparenza ⁽²¹¹⁾; limitazione della finalità ⁽²¹²⁾; minimizzazione dei dati ⁽²¹³⁾; esattezza ⁽²¹⁴⁾; limitazione ⁽²¹⁵⁾ e sicurezza ⁽²¹⁶⁾ della conservazione], impone le condizioni relative al trattamento di categorie particolari di dati ⁽²¹⁷⁾, fissa i diritti degli interessati ⁽²¹⁸⁾, impone la protezione dei dati fin dalla progettazione ⁽²¹⁹⁾ e disciplina i trasferimenti internazionali di dati personali ⁽²²⁰⁾.

- (130) Allo stesso tempo, la sezione 110 della legge del 2018 sulla protezione dei dati prevede un'esenzione da disposizioni specifiche previste nella parte 4 della legge del 2018 sulla protezione dei dati, quando tale esenzione è necessaria per salvaguardare la sicurezza nazionale. La sezione 110, paragrafo 2, della legge del 2018 sulla protezione dei dati elenca le disposizioni rispetto alle quali è consentita un'esenzione, tra cui i principi di protezione dei dati (fatta eccezione per il principio di liceità), i diritti degli interessati, l'obbligo di informare l'ICO in merito a una violazione dei dati, i poteri di ispezione dell'ICO in conformità con gli obblighi internazionali, alcuni dei poteri esecutivi dell'ICO, 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. Tale esenzione può essere invocata sulla base di un'analisi caso per caso ⁽²²¹⁾. Come spiegato dalle autorità del Regno Unito e confermato dalla giurisprudenza degli organi giurisdizionali del Regno Unito, «il titolare del trattamento deve considerare le conseguenze effettive per la sicurezza nazionale o la difesa che si verificherebbero qualora fosse tenuto a rispettare la disposizione specifica in materia di protezione dei dati, e valuta se può ragionevolmente rispettare la norma abituale senza ripercussioni per la sicurezza nazionale o la difesa» ⁽²²²⁾. Spetta all'ICO valutare se l'esenzione sia stata applicata adeguatamente o meno ⁽²²³⁾.

⁽²¹¹⁾ 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 di ottenimento dei dati. 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.

⁽²¹²⁾ 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, 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).

⁽²¹³⁾ I dati personali devono essere adeguati, pertinenti e non eccedenti (sezione 88 della legge del 2018 sulla protezione dei dati).

⁽²¹⁴⁾ I dati personali devono essere esatti ed aggiornati (sezione 89 della legge del 2018 sulla protezione dei dati).

⁽²¹⁵⁾ I dati personali devono essere conservati per un periodo di tempo non superiore a quanto necessario (sezione 90 della legge del 2018 sulla protezione dei dati).

⁽²¹⁶⁾ 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 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.

⁽²¹⁷⁾ Sezione 86, paragrafo 2, lettera b), e allegato 10 della legge del 2018 sulla protezione dei dati.

⁽²¹⁸⁾ 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.

⁽²¹⁹⁾ Sezione 103 della legge del 2018 sulla protezione dei dati.

⁽²²⁰⁾ Sezione 109 della legge del 2018 sulla protezione dei dati. I trasferimenti di dati personali a 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.

⁽²²¹⁾ Cfr. causa *Baker v Secretary of State for the Home Department* [2001] UKIT NSA2 («*Baker v Secretary of State*»).

⁽²²²⁾ Regno Unito, *Explanatory Framework for Adequacy Discussions*, section H: *National Security Data Protection and Investigatory Powers Framework*, pagg. 15 e 16, disponibile al seguente indirizzo: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Cfr. anche *Baker v Secretary of State* (cfr. nota 220), causa nella quale l'organo giurisdizionale ha annullato un certificato di sicurezza nazionale rilasciato dal 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.

⁽²²³⁾ 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 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>).

- (131) Inoltre, in relazione alla possibilità di limitare uno dei diritti di cui sopra per motivi di protezione della «sicurezza nazionale», la sezione 79 della legge del 2018 sulla protezione dei dati prevede la possibilità che un titolare del trattamento richieda un certificato firmato da un ministro o dal procuratore generale che attesti che la limitazione di tali diritti è, o era in qualsiasi momento, una misura necessaria e proporzionata per la protezione della sicurezza nazionale ⁽²²⁴⁾. Il governo del Regno Unito ha pubblicato orientamenti sui certificati 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 ⁽²²⁵⁾. Tutti i certificati di sicurezza nazionale devono essere pubblicati sul sito web dell'ICO ⁽²²⁶⁾.
- (132) Il certificato dovrebbe avere una durata fissa non superiore a cinque anni, in maniera da essere riesaminato regolarmente dal potere esecutivo ⁽²²⁷⁾. Il certificato deve individuare i dati personali o le categorie di dati personali soggetti a esenzione nonché le disposizioni della legge del 2018 sulla protezione dei dati a cui si applica l'esenzione ⁽²²⁸⁾.
- (133) 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 invocare l'esenzione prevista per motivi di sicurezza nazionale, che deve essere applicata caso per caso. Anche se alla questione in esame si applica un certificato di sicurezza nazionale, l'ICO può indagare per stabilire se il ricorso all'esenzione prevista per motivi di sicurezza nazionale sia stato giustificato in un caso specifico ⁽²²⁹⁾.
- (134) Qualsiasi persona direttamente interessata dal rilascio del certificato può presentare ricorso all'*Upper Tribunal* ⁽²³⁰⁾ (tribunale superiore) contro il certificato ⁽²³¹⁾ oppure, laddove il certificato individui i dati mediante una descrizione generale, impugnare l'applicazione del certificato a dati specifici ⁽²³²⁾.
- (135) Detto organo giurisdizionale riesamina la decisione di emettere un certificato e decide se vi erano motivi ragionevoli per il suo rilascio ⁽²³³⁾. 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 ⁽²³⁴⁾.

⁽²²⁴⁾ La legge del 2018 sulla protezione dei dati ha abolito la possibilità di rilasciare certificati a norma della sezione 28, paragrafo 2, della legge del 1998 sulla protezione dei dati. La possibilità di rilasciare «vecchi certificati» esiste ancora nella misura in cui vi è una contestazione storica in virtù 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. Al momento non esistono certificati di sicurezza nazionale rilasciati ai sensi della legge del 1998 sulla protezione dei dati.

⁽²²⁵⁾ Orientamenti del Regno Unito sui certificati di sicurezza nazionale ai sensi della legge del 2018 sulla protezione dei dati, disponibili 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.

⁽²²⁶⁾ 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.

⁽²²⁷⁾ Orientamenti governativi del Regno Unito sui certificati di sicurezza nazionale, punto 15, cfr. nota 225.

⁽²²⁸⁾ Orientamenti governativi del Regno Unito sui certificati di sicurezza nazionale, punto 5, cfr. nota 224.

⁽²²⁹⁾ 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 di aver considerato le circostanze specifiche del caso nell'invocare l'esenzione. 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/>.

⁽²³⁰⁾ 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.

⁽²³¹⁾ Sezione 111, paragrafo 3, della legge del 2018 sulla protezione dei dati.

⁽²³²⁾ Sezione 111, paragrafo 5, della legge del 2018 sulla protezione dei dati.

⁽²³³⁾ Nella causa *Baker v Secretary of State* (cfr. nota 221), 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 una deroga globale all'obbligo di rispondere a richieste di accesso e che consentire tale deroga in ogni circostanza senza un'analisi caso per caso andava oltre quanto necessario e proporzionato ai fini della protezione della sicurezza nazionale.

⁽²³⁴⁾ Orientamenti governativi del Regno Unito sui certificati di sicurezza nazionale, punto 25, cfr. nota 224.

- (136) 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⁽²³⁵⁾ 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. L'applicazione di tali disposizioni è esentata per determinate categorie di informazioni (esenzione «basata sulla classificazione») oppure esentata nella misura in cui potrebbe compromettere l'interesse tutelato (esenzione «basata sul pregiudizio») (236). Le esenzioni basate sul pregiudizio possono essere invocate soltanto nella misura in cui l'applicazione della disposizione di protezione dei dati elencati potrebbe pregiudicare lo specifico interesse in questione. Il ricorso a un'esenzione deve quindi essere sempre giustificato facendo riferimento al pregiudizio che potrebbe verificarsi nel singolo caso. L'esenzione basata sulla classificazione può essere invocata soltanto rispetto alla categoria di informazioni specifica, strettamente definita, per la quale è concessa. Si tratta di esenzioni analoghe, in termini di finalità ed effetto, a numerose delle eccezioni previste dal 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 GDPR dell'Unione europea.
- (137) Da quanto precede consegue che tali limitazioni e condizioni si attuano nel quadro di disposizioni giuridiche del Regno Unito applicabili, anche quali interpretate dagli organi giurisdizionali e dall'ICO, al fine di assicurare che tali esenzioni e limitazioni rimangano entro i limiti di quanto necessario e proporzionato per proteggere la sicurezza nazionale.
- (138) 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'ICO (237).
- (139) Le funzioni generali dell'ICO 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 monitoraggio e l'applicazione delle norme di cui alla parte 4 della legge del 2018 sulla protezione dei dati, la sensibilizzazione del pubblico, attività di consulenza a favore del parlamento, del governo e di altre istituzioni in merito a misure legislative e amministrative, la sensibilizzazione dei titolari del trattamento e dei responsabili del trattamento in merito ai loro obblighi, la trasmissione di informazioni a un interessato sull'esercizio dei suoi diritti, e lo svolgimento di indagini.
- (140) Per quanto concerne la parte 3 della legge del 2018 sulla protezione dei dati, l'ICO ha il potere di notificare ai titolari del trattamento una presunta violazione, emettere avvertimenti sulla probabilità che un trattamento violi le norme, e formulare ammonimenti quando la violazione è confermata. Può inoltre emettere avvisi di esecuzione e di irrogazione di sanzioni per violazioni di determinate disposizioni della legge (238). Tuttavia, contrariamente a quanto previsto per altre parti della legge del 2018 sulla protezione dei dati, l'ICO non può rivolgere un avviso di valutazione a un organismo di sicurezza nazionale (239).
- (141) Inoltre la sezione 110 della legge del 2018 sulla protezione dei dati prevede un'eccezione all'utilizzo di determinati poteri da parte dell'ICO quando ciò è necessario al fine di proteggere la sicurezza nazionale. Ciò riguarda tra l'altro il potere dell'ICO 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

(235) 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 stabilite negli allegati 9 e 10; ii) i diritti degli interessati; e iii) i doveri relativi alla segnalazione di violazioni all'ICO.

(236) 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 222.

(237) Sezione 116 della legge del 2018 sulla protezione dei dati.

(238) Ai sensi dell'allegato 149, paragrafo 2, e della sezione 155 della legge del 2018 sulla protezione dei dati, lette in combinato disposto, 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'ICO 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 102 e 103).

(239) Ai sensi della sezione 147, paragrafo 6, della legge del 2018 sulla protezione dei dati, l'ICO 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 Headquarters*.

⁽²⁴⁹⁾ Le relazioni e le dichiarazioni della commissione sono disponibili online al seguente indirizzo: <http://isc.independent.gov.uk/committee-reports>. Nel 2015 l'ISC ha pubblicato una relazione dal titolo «Privacy and Security: A modern and transparent legal framework» (cfr.: https://b1cba9b3-a-5e6631fd-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.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-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf

operazioni in corso ⁽²⁴⁷⁾. Il protocollo d'intesa concordato tra il primo ministro e l'ISC ⁽²⁴⁸⁾ specifica in maniera dettagliata gli elementi da prendere in considerazione quando si valuta se un'attività non fa parte di alcuna operazione in corso ⁽²⁴⁹⁾. L'ISC può inoltre essere invitata a indagare in merito a operazioni in corso da parte del primo ministro e può esaminare le informazioni fornite volontariamente dalle agenzie.

- (145) In virtù dell'allegato 1 della legge del 2013 sulla giustizia e sulla sicurezza l'ISC può chiedere ai capi di uno 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 ⁽²⁵⁰⁾. Secondo le spiegazioni fornite dalle autorità del Regno Unito, nella pratica sono rarissime le informazioni che non vengono divulgate dall'ISC ⁽²⁵¹⁾.
- (146) Per quanto concerne i mezzi di ricorso, innanzitutto, ai sensi della sezione 165, paragrafo 2, della legge del 2018 sulla protezione dei dati, un interessato può proporre reclamo presso l'ICO qualora ritenga che, in relazione a dati personali che lo riguardano, sia stata commessa una violazione della parte 4 della legge del 2018 sulla protezione dei dati, compreso qualsiasi uso abusivo delle deroghe e delle limitazioni per motivi di sicurezza nazionale.
- (147) 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 ⁽²⁵²⁾, di opposizione al trattamento ⁽²⁵³⁾ e di rettifica o cancellazione.
- (148) 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 ⁽²⁵⁴⁾. Sono compresi sia i danni che comportano una perdita finanziaria sia quelli che non la comportano, ad esempio una sofferenza ⁽²⁵⁵⁾.
- (149) Infine, una persona può promuovere un reclamo all'*Investigatory Powers Tribunal* (IPT) per qualsiasi condotta da parte, o per conto, delle agenzie di intelligence del Regno Unito ⁽²⁵⁶⁾. L'IPT è istituito dalla *Regulation of Investigatory Powers Act 2000* (legge sul regolamento sui poteri di indagine) per Inghilterra, Galles e Irlanda del Nord, e dalla *Regulation of Investigatory Powers (Scotland) Act 2000* (legge sul regolamento sui poteri di indagine — Scozia) per la Scozia (RIPA 2000) ed è indipendente dal potere esecutivo ⁽²⁵⁷⁾. Conformemente alla sezione 65 della RIPA 2000, i membri dell'IPT sono nominati dalla Regina per un mandato di cinque anni.
- (150) Il loro incarico può essere revocato dalla Regina su raccomandazione ⁽²⁵⁸⁾ presentata da entrambe le camere del parlamento ⁽²⁵⁹⁾.
- (151) Al fine di promuovere un'azione dinanzi all'IPT («requisito sulla legittimazione»), a norma della sezione 65 della RIPA 2000, una persona fisica deve ritenere i) 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 ⁽²⁶⁰⁾, e ii) che la condotta abbia

⁽²⁴⁷⁾ Sezione 2 della legge del 2013 sulla giustizia e sulla sicurezza.

⁽²⁴⁸⁾ 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>

⁽²⁴⁹⁾ Protocollo d'intesa tra il primo ministro e l'ISC, punto 14, cfr. nota 248.

⁽²⁵⁰⁾ 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, punto 4, numero 2, della legge del 2013 sulla giustizia e sulla sicurezza).

⁽²⁵¹⁾ Regno Unito, Explanatory Framework, section H: National Security, pag. 43.

⁽²⁵²⁾ Sezione 94, paragrafo 11, della legge del 2018 sulla protezione dei dati.

⁽²⁵³⁾ Sezione 99, paragrafo 4, della legge del 2018 sulla protezione dei dati.

⁽²⁵⁴⁾ 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».

⁽²⁵⁵⁾ Sezione 169, paragrafo 5, della legge del 2018 sulla protezione dei dati.

⁽²⁵⁶⁾ Cfr. sezione 65, paragrafo 2, lettera b), della RIPA.

⁽²⁵⁷⁾ 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.

⁽²⁵⁸⁾ Sulla nozione di «Address», si veda la nota 183.

⁽²⁵⁹⁾ Allegato 3, paragrafo 1, punto 5, della RIPA 2000.

⁽²⁶⁰⁾ Sezione 65, paragrafo 4, della RIPA 2000.

avuto luogo in «circostanze impugnabili» ⁽²⁶¹⁾ o sia stata «adottata da o per conto dei servizi di intelligence» ⁽²⁶²⁾. Dato che tale livello di «convinzione» è stato interpretato in maniera alquanto ampia ⁽²⁶³⁾, promuovere un'azione dinanzi a detto organo giurisdizionale richiede il soddisfacimento di requisiti di legittimazione relativamente bassi.

- (152) Quando valuta un reclamo che gli è stato sottoposto, l'IPT 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 ⁽²⁶⁴⁾. Quando esamina un procedimento, l'IPT deve applicare i medesimi principi decisionali che verrebbero applicati da un organo giurisdizionale per un'istanza di controllo giurisdizionale ⁽²⁶⁵⁾.
- (153) L'IPT deve notificare al reclamante se è stata presa una decisione a suo favore o meno ⁽²⁶⁶⁾. Conformemente alla sezione 67, paragrafi 6 e 7, della RIPA 2000, l'IPT ha il potere di emettere provvedimenti provvisori e riconoscere risarcimenti o rendere qualsiasi altra ordinanza ritenuta opportuna ⁽²⁶⁷⁾. Conformemente alla sezione 67 A del RIPA 2000, una decisione dell'IPT può essere impugnata, a condizione che l'IPT o l'organo giurisdizionale di appello competente dia la propria autorizzazione.
- (154) In particolare le persone fisiche possono proporre reclamo, e ottenere un risarcimento, presso l'IPT nel caso in cui ritengano che un'autorità pubblica abbia agito (o proponga di agire) in maniera incompatibile con un diritto sancito dalla CEDU, compreso il diritto alla tutela della vita privata o alla protezione dei dati, e di conseguenza illecita ai sensi della sezione 6, paragrafo 1, della legge del 1998 sui diritti umani. All'IPT è stata concessa competenza giurisdizionale esclusiva per tutti i reclami in relazione alle agenzie di intelligence ai sensi della legge sui diritti umani. 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'IPT stesso può ormai formare oggetto di 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'IPT è in linea di principio assoggettabile a controllo giurisdizionale: cfr. *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219» ⁽²⁶⁸⁾. Laddove l'IPT 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 ⁽²⁶⁹⁾.

⁽²⁶¹⁾ Tali circostanze fanno riferimento alla condotta di autorità pubbliche che si svolge 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. Si ritiene che la condotta autorizzata da un commissario giudiziario abbia avuto luogo in circostanze impugnabili (sezione 65, paragrafo 7ZA, del RIPA 2000) mentre altre condotte che avvengono con il permesso di un funzionario dell'autorità giudiziaria non abbiano avuto luogo in circostanze impugnabili (sezione 65, paragrafi 7 e 8, della RIPA 2000).

⁽²⁶²⁾ 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'IPT specifica che nel 2016 detto organo 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'IPT, disponibile al seguente indirizzo: <https://www.ipt-uk.com/docs/IPT%20Statistical%20Report%202016.pdf>

⁽²⁶³⁾ Cfr. la causa *Human Rights Watch v Secretary of State* [2016] UKIPTrib15_165-CH. Nel contesto di tale causa l'IPT, facendo riferimento alla giurisprudenza della Corte europea dei diritti dell'uomo, ha ritenuto che la verifica adeguata 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 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).

⁽²⁶⁴⁾ Sezione 67, paragrafo 3, della RIPA 2000.

⁽²⁶⁵⁾ Sezione 67, paragrafo 2, della RIPA 2000.

⁽²⁶⁶⁾ Sezione 68, paragrafo 4, della RIPA 2000.

⁽²⁶⁷⁾ Può trattarsi di un'ordinanza che richieda la distruzione di qualunque registrazione di informazioni detenute da un'autorità pubblica in relazione a una persona.

⁽²⁶⁸⁾ *High Court of Justice, Liberty*, [2019] EWHC 2057 (Admin), punto 170.

⁽²⁶⁹⁾ Sezione 8, paragrafo 1, della legge del 1998 sui diritti umani.

- (155) 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 CEDU, compreso il diritto alla tutela della vita privata e alla protezione dei dati.
- (156) Ne consegue che la condivisione da parte delle autorità del Regno Unito preposte all'attività di contrasto di dati trasferiti a norma della presente decisione con altre autorità pubbliche, comprese le agenzie di intelligence, è inquadrata da limitazioni e condizioni che assicurano che tale condivisione successiva sia necessaria e proporzionata e soggetta a specifiche garanzie della protezione dei dati in virtù della legge del 2018 sulla protezione dei dati. Inoltre il trattamento di dati da parte delle autorità pubbliche in questione è oggetto di vigilanza da parte di organismi indipendenti e le persone interessate hanno accesso a ricorsi giurisdizionali efficaci.

3. CONCLUSIONI

- (157) La Commissione ritiene che la parte 3 della legge del 2018 sulla protezione dei dati assicuri un livello di protezione dei dati personali trasferiti per finalità di contrasto in materia penale dalle autorità competenti nell'Unione europea alle autorità competenti nel Regno Unito che è sostanzialmente equivalente a quello garantito dalla direttiva (UE) 2016/680.
- (158) 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.
- (159) 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, anche nel contesto della condivisione di dati personali tra le autorità di contrasto e altre autorità pubbliche come gli organismi 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.
- (160) Di conseguenza è opportuno decidere che il Regno Unito assicura un livello di protezione adeguato ai sensi dell'articolo 36, paragrafo 2, della direttiva (UE) 2016/680, interpretato alla luce della Carta dei diritti fondamentali dell'Unione europea.
- (161) 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.

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

- (162) 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.
- (163) Di conseguenza, una decisione di adeguatezza adottata dalla Commissione a norma dell'articolo 36, paragrafo 3, della direttiva (UE) 2016/680 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.
- (164) Allo stesso tempo è opportuno ricordare che, ai sensi dell'articolo 47, paragrafo 5, della direttiva (UE) 2016/680, e come spiegato dalla Corte di giustizia nella sentenza *Schrems*, 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 ⁽²⁷⁰⁾.

⁽²⁷⁰⁾ *Schrems*, punto 65.

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

- (165) Ai sensi dell'articolo 36, paragrafo 4, della direttiva (UE) 2016/680, la Commissione è tenuta a controllare 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, anche attraverso la conclusione di accordi internazionali, e all'impatto che ciò può avere sul livello di protezione offerto ai dati trasferiti a norma della presente decisione; così come all'effettività dell'esercizio dei diritti individuali nei settori contemplati dalla presente decisione. Assieme ad altri elementi, gli sviluppi giurisprudenziali e la vigilanza da parte dell'ICO e di altri organismi indipendenti contribuiranno al monitoraggio della Commissione.
- (166) Per agevolare tale monitoraggio, le autorità del Regno Unito dovrebbero informare tempestivamente e regolarmente 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, in particolare per quanto riguarda gli elementi di cui al considerando 165.
- (167) 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 autorità competenti nel Regno Unito. La Commissione dovrebbe inoltre essere informata di eventuali indicazioni del fatto che le azioni delle autorità pubbliche del Regno Unito competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, compresi gli organismi di vigilanza, non garantiscono il necessario livello di protezione.
- (168) 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.
- (169) 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 58, paragrafo 2, della direttiva (UE) 2016/680 al fine di sospendere o abrogare parzialmente o completamente la presente decisione.
- (170) 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.
- (171) In ragione di motivi imperativi d'urgenza debitamente giustificati, la Commissione farà ricorso alla possibilità di adottare, conformemente alla procedura di cui all'articolo 58, paragrafo 3, della direttiva (UE) 2016/680, atti di esecuzione immediatamente applicabili destinati a sospendere, abrogare o modificare la presente decisione.

6. DURATA E RINNOVO DELLA PRESENTE DECISIONE

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

- (174) 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 58, paragrafo 2, della direttiva (UE) 2016/680.

7. CONSIDERAZIONI FINALI

- (175) Il comitato europeo per la protezione dei dati ha pubblicato il proprio parere ⁽²⁷¹⁾, del quale si è tenuto conto nell'elaborazione della presente decisione.
- (176) Le misure di cui alla presente decisione sono conformi al parere del comitato istituito dall'articolo 58 della direttiva (UE) 2016/680.
- (177) A norma dell'articolo 6 bis del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al TUE e al TFUE, l'Irlanda non è vincolata dalle disposizioni previste dalla direttiva (UE) 2016/680, e di conseguenza dalla presente decisione di esecuzione, che riguardano il trattamento dei dati personali da parte degli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione della parte terza, titolo V, capi 4 o 5, TFUE laddove l'Irlanda non sia vincolata da norme che disciplinano forme di cooperazione giudiziaria in materia penale o di cooperazione di polizia nell'ambito delle quali devono essere rispettate le disposizioni stabilite in base all'articolo 16 TFUE. Inoltre, in virtù della decisione di esecuzione (UE) 2020/1745 del Consiglio ⁽²⁷²⁾, la direttiva (UE) 2016/680 è messa in applicazione e si applica in Irlanda in via provvisoria a decorrere dal 1° gennaio 2021. L'Irlanda è pertanto vincolata dalla presente decisione di esecuzione, alle stesse condizioni applicabili all'applicazione della direttiva (UE) 2016/680 in Irlanda come stabilito nella decisione di esecuzione (UE) 2020/1745, per quanto concerne l'*acquis* di Schengen al quale partecipa.
- (178) Conformemente agli articoli 2 e 2 bis del protocollo n. 22 sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, la Danimarca non è vincolata dalle disposizioni previste dalla direttiva (UE) 2016/680, e di conseguenza dalla presente decisione di esecuzione, né soggetta alla loro applicazione per quanto concerne il trattamento di dati personali da parte degli Stati membri durante lo svolgimento di attività che rientrano nell'ambito di applicazione della parte terza, titolo V, capo 4 o 5, TFUE. Tuttavia, dato che la direttiva (UE) 2016/680 si basa sull'*acquis* di Schengen, il 26 ottobre 2016 la Danimarca, conformemente all'articolo 4 di tale protocollo, ha notificato la propria decisione di attuare la direttiva (UE) 2016/680. La Danimarca è pertanto tenuta ad attuare la presente decisione di esecuzione in virtù del diritto internazionale.
- (179) Per quanto riguarda l'Islanda e la Norvegia, la presente decisione di esecuzione costituisce uno sviluppo delle disposizioni dell'*acquis* di Schengen ai sensi dell'accordo concluso dal Consiglio dell'Unione europea con la Repubblica d'Islanda e il Regno di Norvegia sulla loro associazione all'attuazione, all'applicazione e allo sviluppo dell'*acquis* di Schengen ⁽²⁷³⁾.
- (180) Per quanto riguarda la Svizzera, la presente decisione di esecuzione costituisce uno sviluppo delle disposizioni dell'*acquis* di Schengen ai sensi dell'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione di quest'ultima all'attuazione, all'applicazione e allo sviluppo dell'*acquis* di Schengen ⁽²⁷⁴⁾.
- (181) Per quanto riguarda il Liechtenstein, la presente decisione di esecuzione costituisce uno sviluppo delle disposizioni dell'*acquis* di Schengen, ai sensi del protocollo tra l'Unione europea, la Comunità europea, la Confederazione svizzera e il Principato del Liechtenstein sull'adesione del Principato del Liechtenstein all'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione della Confederazione svizzera all'attuazione, all'applicazione e allo sviluppo dell'*acquis* di Schengen ⁽²⁷⁵⁾,

⁽²⁷¹⁾ Parere 15/2021 relativo al progetto di decisione di esecuzione della Commissione europea a norma della direttiva (UE) 2016/680 sull'adeguata protezione dei dati personali nel Regno Unito, disponibile al seguente indirizzo: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

⁽²⁷²⁾ Decisione di esecuzione (UE) 2020/1745 del Consiglio, del 18 novembre 2020, relativa alla messa in applicazione delle disposizioni dell'*acquis* di Schengen in materia di protezione dei dati e all'applicazione provvisoria di talune disposizioni dell'*acquis* di Schengen in Irlanda (GU L 393 del 23.11.2020, pag. 3).

⁽²⁷³⁾ GU L 176 del 10.7.1999, pag. 36.

⁽²⁷⁴⁾ GU L 53 del 27.2.2008, pag. 52.

⁽²⁷⁵⁾ GU L 160 del 18.6.2011, pag. 21.

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Ai fini dell'articolo 36 della direttiva (UE) 2016/680, il Regno Unito assicura un livello di protezione adeguato dei dati personali trasferiti dall'Unione europea alle autorità pubbliche del Regno Unito competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali.

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 47 della direttiva (UE) 2016/680 in relazione a trasferimenti di dati ad autorità pubbliche del Regno Unito 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 e sono esercitati i diritti individuali, 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.
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 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 58, paragrafo 2, della direttiva (UE) 2016/680.

Articolo 5

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 28 giugno 2021

Per la Commissione
Didier REYNERS
Membro della Commissione
