II

(Acte fără caracter legislativ)

DECIZII

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2021/1772 AL COMISIEI

din 28 iunie 2021

în temeiul Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția adecvată a datelor cu caracter personal de către Regatul Unit al Marii Britanii și Irlandei de Nord

[notificată cu numărul C(2021) 4800]

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) ([1]), în special articolul 45 alineatul (3),

întrucât:

1. INTRODUCERE

(1) Regulamentul (UE) 2016/679 stabilește normele pentru transferul de date cu caracter personal de la operatori sau persoane împuternicite de către operatori din Uniunea Europeană către țări terțe și organizații internaționale, în măsura în care astfel de transferuri intră în domeniul său de aplicare. Normele privind transferurile internaționale de date sunt prevăzute în capitolul V din regulamentul menționat, mai precis la articolele 44-50. Deși fluxul de date cu caracter personal către și dinspre țări situate în afara Uniunii Europene este esențial pentru dezvoltarea cooperării internaționale și a comerțului transfrontalier, nivelul de protecție conferit datelor cu caracter personal din Uniunea Europeană nu trebuie să fie subminat de transferurile către țări terțe ([2]).

(2) În temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679, Comisia poate decide, prin intermediul unui act de punere în aplicare, că o țară terță, un teritoriu sau unul ori mai multe sectoare specificate dintr-o țară terță sau o organizație internațională asigură un nivel de protecție adecvat. În astfel de condiții, transferurile de date cu caracter personal către o țară terță pot avea loc fără a fi necesar să se obțină autorizări suplimentare, astfel cum se prevede la articolul 45 alineatul (1) și în considerentul 103 din regulamentul menționat.

(3) În conformitate cu articolul 45 alineatul (2) din Regulamentul (UE) 2016/679, adoptarea unei decizii privind caracterul adecvat al nivelului de protecție trebuie să se bazeze pe o analiză cuprinzătoare a ordinii juridice a țării terțe, în ceea ce privește atât normele aplicabile importatorilor de date, cât și limitările și garanțiile referitoare la accesul autorităților publice la datele cu caracter personal. În evaluare, Comisia trebuie să stabilească dacă țara terță în cauză garantează un nivel de protecție „echivalent în esență” cu cel garantat în cadrul Uniunii Europene [considerentul 104 din Regulamentul (UE) 2016/679]. Standardul în raport cu care este evaluată „echivalența substanțială” este cel stabilit de legislația Uniunii Europene, în special de Regulamentul (UE) 2016/679, precum și de jurisprudența Curții de Justiție a Uniunii Europene ([3]). Criteriile de referință privind caracterul adecvat al nivelului de protecție ale Comitetului european pentru protecția datelor (CEPD) sunt, de asemenea, importante în această privință ([4]).

([1]) JO L 119, 4.5.2016, p. 1.
([2]) A se vedea considerentul 101 din Regulamentul (UE) 2016/679.
([3]) A se vedea, cel mai recent, cauza C-311/18, *Facebook Ireland și Schrems („Schrems II”)* ECLI:EU:C:2020:559.
([4]) Comitetul european pentru protecția datelor, *Criterii de referință privind caracterul adecvat al nivelului de protecție*, WP 254 rev. 01., disponibile la următoarea adresă: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

(4) Conform clarificărilor aduse de Curtea de Justiție a Uniunii Europene, aceasta nu necesită găsirea unui nivel identic de protecție ([5]). În special, mijloacele la care țara terță în cauză recurge pentru protecția datelor cu caracter personal pot fi diferite de cele utilizate în cadrul Uniunii Europene, cu condiția ca acestea să se dovedească, în practică, eficace pentru asigurarea unui nivel adecvat de protecție ([6]). Prin urmare, standardul caracterului adecvat nu necesită o reproducere punct cu punct a normelor Uniunii. Mai curând, testul constă în a stabili dacă, prin esența drepturilor în materie de protecție a datelor și punerea în aplicare efectivă, supravegherea și exercitarea acestora, sistemul străin în cauză, în ansamblul său, oferă nivelul de protecție necesar ([7]).

(5) Comisia a analizat cu atenție legislația și practica din Regatul Unit al Marii Britanii și Irlandei de Nord. Pe baza constatărilor prezentate în considerentele 8-270, Comisia concluzionează că Regatul Unit asigură un nivel adecvat de protecție pentru datele cu caracter personal care intră în domeniul de aplicare al Regulamentului (UE) 2016/679, transferate din Uniunea Europeană către Regatul Unit.

(6) Această concluzie nu se referă la datele cu caracter personal transferate în scopul controlului imigrației în Regatul Unit sau care intră în domeniul de aplicare al derogării de la anumite drepturi ale persoanelor vizate în scopul menținerii unui control eficace al imigrației („derogarea în materie de imigrație") în temeiul punctului 4 alineatul (1) din anexa 2 la Legea Regatului Unit privind protecția datelor. Validitatea și interpretarea derogării în materie de imigrație în temeiul legislației Regatului Unit nu sunt soluționate în urma unei hotărâri a Curții de Apel din Regatul Unit din 26 mai 2021. Deși recunoaște că, în principiu, drepturile persoanelor vizate pot fi restricționate în scopul controlului imigrației ca și „aspect important al interesului public", Curtea de Apel a constatat că derogarea în materie de imigrație este, în forma sa actuală, incompatibilă cu legislația Regatului Unit, deoarece măsura legislativă nu conține dispoziții specifice care să stabilească garanțiile enumerate la articolul 23 alineatul (2) din Regulamentul general al Regatului Unit privind protecția datelor (RGPD al Regatului Unit) ([8]). În aceste condiții, transferurile de date cu caracter personal din Uniune către Regatul Unit cărora li se poate aplica derogarea în materie de imigrație ar trebui excluse din domeniul de aplicare al prezentei decizii ([9]). Odată ce este remediată incompatibilitatea cu legislația Regatului Unit, derogarea în materie de imigrație ar trebui reevaluată, precum și necesitatea de a menține limitarea domeniului de aplicare al prezentei decizii.

(7) Prezenta decizie nu ar trebui să aducă atingere aplicării directe a Regulamentului (UE) 2016/679 în cazul organizațiilor stabilite în Regatul Unit în cazul în care sunt îndeplinite condițiile privind domeniul de aplicare teritorial al regulamentului respectiv, astfel cum se prevede la articolul 3.

2. NORMELE APLICABILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

2.1. Cadrul constituțional

(8) Regatul Unit este o democrație parlamentară care are un suveran constituțional în calitate de șef de stat. Acesta are un parlament suveran, care exercită o autoritate supremă asupra tuturor celorlalte instituții guvernamentale, un executiv ai cărui membri provin din parlament și care este responsabil în fața acestuia, precum și un sistem judiciar independent. Executivul își bazează autoritatea pe capacitatea sa de a atrage încrederea Camerei Comunelor alese și răspunde în fața ambelor camere ale Parlamentului, care sunt responsabile de controlul Guvernului și de dezbaterea și adoptarea legilor.

([5]) Cauza C-362/14, *Schrems* („*Schrems I*"), ECLI:EU:C:2015:650, punctul 73.

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

([7]) A se vedea Comunicarea Comisiei către Parlamentul European și Consiliu, „Schimbul de date cu caracter personal și protecția acestora într-o lume globalizată", COM(2017) 7 din 10 ianuarie 2017, secțiunea 3.1, p. 6-7, disponibilă la următoarea adresă: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52017DC0007&from=EN

([8]) Court of Appeal (Civil Division), *Open Rights Group v Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport*, [2021] EWCA Civ 800, punctele 53-56. Curtea de Apel a anulat hotărârea Înaltei Curți de Justiție care evaluase anterior derogarea în lumina Regulamentului (UE) 2016/679 (în special, a articolul 23 din acesta) și a Cartei drepturilor fundamentale a Uniunii Europene și a constatat că derogarea este legală [Open Rights Group & Anor, R (on the application Of)/Secretary of State for the Home Department & Anor [2019] EWHC 2562].

([9]) Sub rezerva îndeplinirii condițiilor aplicabile, transferurile în scopul controlului imigrației în Regatul Unit pot fi efectuate pe baza mecanismelor de transfer prevăzute la articolele 46-49 din Regulamentul (UE) 2016/679.

(9) Parlamentul Regatului Unit a delegat Parlamentului scoțian, Parlamentului Țării Galilor (Senedd Cymru) și Adunării Irlandei de Nord responsabilitatea pentru legiferarea chestiunilor interne din Scoția, Țara Galilor și Irlanda de Nord pe care Parlamentul Regatului Unit nu și le-a rezervat. În timp ce protecția datelor reprezintă o chestiune rezervată, și anume aceeași legislație se aplică în întreaga țară, alte domenii de politică relevante pentru prezenta decizie sunt descentralizate. De exemplu, sistemele de justiție penală, inclusiv poliția, din Scoția și Irlanda de Nord sunt transferate Parlamentului scoțian și, respectiv, Adunării Irlandei de Nord. Regatul Unit nu are o constituție codificată în sensul unui document constitutiv cu vechime. Principiile constituționale au apărut de-a lungul timpului, provenind în special din jurisprudență și din convenție. Valoarea constituțională a anumitor statute, cum ar fi Magna Carta, Declarația drepturilor din 1689 (*Bill of Rights 1689*) și Legea privind drepturile omului din 1998 (*Human Rights Act 1998*), a fost recunoscută de instanțe. Drepturile fundamentale ale persoanelor au fost dezvoltate, ca parte a constituției, prin intermediul common law, al acestor statute și al tratatelor internaționale, în special al Convenției europene a drepturilor omului, pe care Regatul Unit a ratificat-o în 1951. În 1987, Regatul Unit a ratificat, de asemenea, Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108) ([10]).

(10) Legea privind drepturile omului din 1998 încorporează în legislația Regatului Unit drepturile cuprinse în Convenția europeană a drepturilor omului. Legea privind drepturile omului acordă oricărei persoane drepturile și libertățile fundamentale prevăzute la articolele 2-12 și articolul 14 din Convenția europeană a drepturilor omului, la articolele 1, 2 și 3 din Protocolul nr. 1 și la articolul 1 din Protocolul nr. 13, coroborate cu articolele 16, 17 și 18 din convenția menționată. Aceasta include dreptul la respectarea vieții private și de familie (și dreptul la protecția datelor ca parte a acestui drept) și dreptul la un proces echitabil ([11]). În special, în temeiul articolului 8 din convenția menționată, nu este admis amestecul unei autorități publice în exercitarea dreptului la viață privată decât în măsura în care acest amestec este prevăzut de lege, dacă constituie o măsură care, într-o societate democratică, este necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protecția sănătății sau a moralei, ori protecția drepturilor și libertăților altora.

(11) În conformitate cu Legea privind drepturile omului din 1998, orice acțiune a autorităților publice trebuie să fie compatibilă cu un drept conferit prin convenție ([12]). În plus, legislația primară și cea secundară trebuie interpretate și puse în aplicare într-un mod compatibil cu drepturile conferite prin convenție ([13]).

2.2. **Cadrul de protecție a datelor din Regatul Unit**

(12) Regatul Unit s-a retras din Uniunea Europeană la 31 ianuarie 2020. Pe baza Acordului privind retragerea Regatului Unit al Marii Britanii și Irlandei de Nord din Uniunea Europeană și din Comunitatea Europeană a Energiei Atomice ([14]), dreptul Uniunii a continuat să se aplice pe teritoriul Regatului Unit pe parcursul perioadei de tranziție până la 31 decembrie 2020. Înainte de retragere și pe parcursul perioadei de tranziție, cadrul legislativ privind protecția datelor cu caracter personal în Regatul Unit consta în legislația relevantă a UE [în special Regulamentul (UE) 2016/679 și Directiva (UE) 2016/680 a Parlamentului European și a Consiliului ([15])] și în legislația națională, în special Legea privind protecția datelor din 2018 (DPA din 2018) ([16]) care prevedea norme de drept intern, în cazul în care erau permise de Regulamentul (UE) 2016/679, care specificau și restricționau aplicarea normelor din Regulamentul (UE) 2016/679, și transpunea Directiva (UE) 2016/680.

([10]) Principiile Convenției 108 au fost transpuse inițial în legislația Regatului Unit prin Legea privind protecția datelor (DPA – *Data Protection Act*) din 1984, care a fost înlocuită de DPA din 1998 și apoi, la rândul său, de DPA din 2018 (coroborat cu RGPD al Regatului Unit). Regatul Unit a semnat, de asemenea, în 2018, Protocolul de modificare a Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (cunoscută sub denumirea de Convenția 108+) și lucrează în prezent la ratificarea convenției.

([11]) Articolele 6 și 8 din CEDO (a se vedea, de asemenea, anexa 1 la Legea privind drepturile omului din 1998).

([12]) Secțiunea 6 din Legea privind drepturile omului din 1998.

([13]) Secțiunea 3 din Legea privind drepturile omului din 1998.

([14]) Acord privind retragerea Regatului Unit al Marii Britanii și Irlandei de Nord din Uniunea Europeană și din Comunitatea Europeană a Energiei Atomice 2019/C 384 I/01, XT/21054/2019/INIT (JO C 384I, 12.11.2019, p. 1), disponibil la următoarea adresă: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=RO

([15]) Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119 4.5.2016, p. 89), disponibilă la următoarea adresă: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L0680&from=RO

([16]) Legea privind protecția datelor din 2018, disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

(13) Pentru a pregăti retragerea din Uniunea Europeană, Guvernul Regatului Unit a adoptat European Union (Withdrawal) Act 2018 [Legea din 2018 privind Uniunea Europeană (retragere)] ([17]), care încorporează legislația direct aplicabilă a Uniunii în legislația Regatului Unit ([18]). Acest așa-numit „drept menținut al Uniunii" include Regulamentul (UE) 2016/679 în întregime (inclusiv considerentele acestuia) ([19]). Conform actului respectiv, dreptul menținut nemodificat al Uniunii trebuie să fie interpretat de instanțele din Regatul Unit în conformitate cu jurisprudența relevantă a Curții de Justiție a Uniunii Europene și cu principiile generale ale dreptului Uniunii, întrucât acestea produc efecte imediat înainte de încheierea perioadei de tranziție (denumite „jurisprudența menținută a Uniunii" și, respectiv, „principiile generale menținute ale dreptului Uniunii") ([20]).

(14) În temeiul Legii din 2018 privind Uniunea Europeană (retragere), miniștrii Regatului Unit au competența de a introduce legislație secundară, prin intermediul instrumentelor statutare, pentru a aduce modificările necesare dreptului menținut al Uniunii Europene ca urmare a retragerii Regatului Unit din Uniunea Europeană. Această competență a fost exercitată prin adoptarea *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019* [Regulamentele din 2019 privind protecția datelor, a vieții private și comunicațiile electronice (modificări etc.) (ieșirea din UE)] (Regulamentele DPPEC) ([21]). Regulamentele DPPEC modifică Regulamentul (UE) 2016/679 astfel cum a fost introdus în legislația Regatului Unit prin Legea din 2018 privind Uniunea Europeană (retragere), prin DPA din 2018 și prin alte acte legislative privind protecția datelor pentru a se potrivi în contextul național ([22]).

(15) În consecință, cadrul juridic privind protecția datelor cu caracter personal în Regatul Unit după încheierea perioadei de tranziție constă în:

— RGPD al Regatului Unit, astfel cum a fost încorporat în legislația Regatului Unit în temeiul Legii din 2018 privind Uniunea Europeană (retragere) și modificat prin Regulamentele DPPEC ([23]); și

— DPA din 2018 ([24]), astfel cum a fost modificată prin Regulamentele DPPEC.

(16) Întrucât RGPD al Regatului Unit este întemeiat pe legislația UE, normele privind protecția datelor din Regatul Unit reflectă îndeaproape, în numeroase aspecte, normele corespunzătoare aplicabile în cadrul Uniunii Europene.

(17) Pe lângă competențele conferite secretarului de stat prin Legea din 2018 privind Uniunea Europeană (retragere), mai multe dispoziții ale DPA din 2018 conferă secretarului de stat competența de a adopta legislație secundară pentru a modifica anumite dispoziții ale legii sau pentru a prevedea norme suplimentare și adiționale ([25]). Până în prezent, secretarul de stat și-a exercitat competența în temeiul secțiunii 137 din DPA din 2018 doar pentru a adopta Data

([17]) European Union (Withdrawal) Act 2018 [Legea din 2018 privind Uniunea Europeană (retragere)], disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2018/16/contents

([18]) Potrivit intenției și efectului Legii din 2018 privind Uniunea Europeană (retragere), întreaga legislație directă a Uniunii care a fost încorporată în dreptul Regatului Unit la încheierea perioadei de tranziție este încorporată în legislația Regatului Unit, deoarece produce efecte în dreptul Uniunii imediat înainte de încheierea perioadei de tranziție. A se vedea secțiunea 3 din Legea din 2018 privind Uniunea Europeană (retragere).

([19]) Notele explicative la Legea din 2018 privind Uniunea Europeană (retragere) precizează următoarele: „În cazul în care legislația este convertită în temeiul prezentei secțiuni, textul legislației în sine este cel care va face parte din legislația internă. Acesta va include textul integral al oricărui instrument al UE (inclusiv considerentele sale)". [Notele explicative la Legea din 2018 privind Uniunea Europeană (retragere), alineatul (83), disponibile la următoarea adresă: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf]. Potrivit informațiilor furnizate de autoritățile Regatului Unit, întrucât considerentele nu au statutul de norme juridice obligatorii, nu a fost necesar ca acestea să fie modificate în același mod în care articolele din Regulamentul (UE) 2016/679 au fost modificate prin regulamentele DPPEC.

([20]) Secțiunea 6 din Legea din 2018 privind Uniunea Europeană (retragere).

([21]) *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019* [Regulamentele din 2019 privind protecția datelor, a vieții private și comunicațiile electronice (modificări etc.) (ieșirea din UE)], disponibile la următoarea adresă: https://www.legislation.gov.uk/uksi/2019/419/contents/made, astfel cum au fost modificate prin Regulamentele DPPEC din 2020, disponibile la următoarea adresă: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

([22]) Aceste modificări ale RGPD al Regatului Unit și ale DPA din 2018 sunt, în cea mai mare parte, de natură tehnică, cum ar fi eliminarea trimiterilor la „statele membre" sau adaptarea terminologiei, de exemplu înlocuirea trimiterilor la Regulamentul (UE) 2016/679 cu trimiteri la RGPD al Regatului Unit. În unele cazuri, au fost necesare modificări pentru a reflecta contextul pur național al prevederilor, de exemplu referitor la „cine" adoptă „regulamente privind caracterul adecvat al nivelului de protecție" în sensul cadrului legislativ al Regatului Unit privind protecția datelor (a se vedea secțiunea 17A din DPA din 2018), și anume secretarul de stat în locul Comisiei Europene.

([23]) Regulamentul general privind protecția datelor, *Keeling Schedule* (Anexa Keeling), disponibilă la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf

([24]) Legea privind protecția datelor din 2018, Anexa Keeling, disponibilă la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf

([25]) Astfel de competențe sunt incluse, de exemplu, în secțiunea 16 (competența de a adopta, în situații specifice, strict delimitate, derogări suplimentare de la dispozițiile specifice ale RGPD al Regatului Unit), în secțiunea 17A (competența de a adopta regulamente privind caracterul adecvat al nivelului de protecție), în secțiunile 212 și 213 (competențele de a iniția acte legislative și de a adopta dispoziții tranzitorii) și în secțiunea 211 (competența de a aduce modificări minore și derivate) din DPA din 2018.

Protection (Charges and Information) (Amendment) Regulations 2019 [Regulamentele din 2019 privind protecția datelor (taxe și informații) (modificare)], care stabilesc circumstanțele în care operatorii de date sunt obligați să plătească o taxă anuală autorității independente pentru protecția datelor din Regatul Unit, *Information Commissioner* (comisarul pentru informații).

(18) În cele din urmă, orientări suplimentare privind legislația Regatului Unit în materie de protecție a datelor sunt furnizate în codurile de bune practici și în alte orientări adoptate de comisarul pentru informații. Deși nu au caracter juridic obligatoriu din punct de vedere formal, aceste orientări au o pondere interpretativă și demonstrează modul în care se aplică legislația privind protecția datelor și în care aceasta este pusă în practică de către comisar. În special, secțiunile 121-125 din DPA din 2018 impun comisarului să elaboreze coduri de bune practici privind schimbul de date, marketingul direct, proiectarea adecvată vârstei, protecția datelor și jurnalismul.

(19) Prin urmare, în structura și componentele sale principale, cadrul juridic al Regatului Unit care se aplică datelor transferate în temeiul prezentei decizii este foarte similar cu cel aplicabil în Uniunea Europeană. Aceasta include faptul că acest cadru nu se bazează numai pe obligațiile prevăzute în dreptul intern, care au fost conturate de dreptul Uniunii, ci și pe obligațiile consacrate în dreptul internațional public, în special prin aderarea Regatului Unit la CEDO și la Convenția 108, precum și prin recunoașterea de către acesta a competenței Curții Europene a Drepturilor Omului. Aceste obligații care decurg din instrumentele internaționale obligatorii din punct de vedere juridic, în special în ceea ce privește protecția datelor cu caracter personal, reprezintă, prin urmare, un element deosebit de important al cadrului juridic evaluat în prezenta decizie.

2.3. **Domeniul de aplicare material și teritorial**

(20) La fel ca în cazul Regulamentului (UE) 2016/679, RGPD al Regatului Unit se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, sau altor tipuri de prelucrare, în cazul în care datele cu caracter personal fac parte dintr-un sistem de evidență a datelor ([26]). Definițiile termenilor „date cu caracter personal", „persoană vizată" și „prelucrarea datelor cu caracter personal" din RGPD al Regatului Unit sunt identice cu cele prevăzute în Regulamentul (UE) 2016/679 ([27]). În plus, RGPD al Regatului Unit se aplică prelucrării nestructurate manuale a datelor cu caracter personal ([28]) deținute de anumite autorități publice din Regatul Unit ([29]), deși secțiunile 24 și 25 din DPA din 2018 nu aplică principiile și drepturile prevăzute în RGPD al Regatului Unit care nu sunt relevante pentru aceste date cu caracter personal. În mod similar cu dispozițiile Regulamentului (UE) 2016/679, RGPD al Regatului Unit nu se aplică prelucrării datelor cu caracter personal efectuate de către o persoană fizică în cursul unei activități exclusiv personale sau domestice ([30]).

(21) RGPD al Regatului Unit își extinde domeniul de aplicare și la prelucrarea în cursul unei activități care, imediat înainte de încheierea perioadei de tranziție, nu intra în domeniul de aplicare al dreptului Uniunii Europene (de exemplu, securitatea națională) ([31]) sau se încadra în domeniul de aplicare al titlului 5 capitolul 2 din Tratatul privind Uniunea Europeană (activități din domeniul politicii externe și de securitate comună) ([32]). La fel ca în sistemul Uniunii Europene, RGPD al Regatului Unit nu se aplică prelucrării datelor cu caracter personal de către o autoritate competentă în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării

([26]) Articolul 2 alineatele (1) și (5) din RGPD al Regatului Unit.

([27]) Articolul 4 alineatele (1) și (2) din RGPD al Regatului Unit.

([28]) Prelucrarea nestructurată manuală a datelor cu caracter personal este definită la articolul 2 alineatul (5) litera (b) ca fiind prelucrarea datelor cu caracter personal care nu este prelucrarea automată sau structurată a datelor cu caracter personal.

([29]) Articolul 2 alineatul (1A) din RGPD al Regatului Unit prevede că regulamentul se aplică, de asemenea, prelucrării nestructurate manuale a datelor cu caracter personal deținute de o autoritate publică FOI. Trimiterea la autorități publice FOI înseamnă orice autorități publice, astfel cum sunt definite în *Freedom of Information Act 2000* (Legea din 2000 privind liberul acces la informațiile de interes public) sau orice autorități publice scoțiene, astfel cum sunt definite în *Freedom of Information (Scotland) Act 2002* [Legea din 2002 privind liberul acces la informațiile de interes public (Scoția)] (asp 13). Secțiunea 21 punctul 5 din DPA din 2018.

([30]) Articolul 2 alineatul (2) litera (a) din RGPD al Regatului Unit.

([31]) Activitățile de securitate națională intră în domeniul de aplicare al RGPD al Regatului Unit numai în măsura în care nu sunt efectuate de o autoritate competentă în scopuri de asigurare a respectării legii, caz în care se aplică partea 3 din DPA din 2018, sau de către sau în numele unui serviciu de informații ale cărui activități sunt excluse din domeniul de aplicare al RGPD al Regatului Unit și fac obiectul părții 4 din DPA din 2018 în temeiul articolului 2 alineatul (2) litera (c) din RGPD al Regatului Unit. De exemplu, o forță de poliție poate efectua controale de securitate ale unui angajat pentru a se asigura că acesta prezintă încredere în ceea ce privește accesarea materialelor de securitate națională. În pofida faptului că poliția este o autoritate competentă în scopuri de asigurare a respectării legii, prelucrarea în cauză nu are un scop de asigurare a respectării legii și s-ar aplica RGPD al Regatului Unit. A se vedea *UK Explanatory Framework for Adequacy Discussions* (Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat), secțiunea H: *National Security Data Protection and Investigatory Powers Framework* (Cadrul privind protecția datelor în materie de securitate națională și competențele de investigare), pagina 8, disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf

([32]) Articolul 2 alineatul (1) literele (a) și (b) din RGPD al Regatului Unit.

sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora (așa-numitele „scopuri de asigurare a respectării legii") – această prelucrare este reglementată, în schimb, de partea 3 din DPA din 2018, așa cum este cazul Directivei (UE) 2016/680 în temeiul dreptului Uniunii Europene – sau prelucrarea datelor cu caracter personal de către serviciile de informații [*Security Service* (Serviciul de Securitate), *Secret Intelligence Service* (Serviciul Secret de Informații) și *Government Communications Headquarters* (Cartierul General pentru Comunicații)], care este reglementată de partea 4 din DPA din 2018 ([33]).

(22) Domeniul de aplicare teritorial al RGPD al Regatului Unit este descris la articolul 3 din RGPD al Regatului Unit ([34]) și include prelucrarea datelor cu caracter personal (indiferent de locul în care se desfășoară) în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Regatului Unit, precum și prelucrarea datelor cu caracter personal ale unor persoane vizate care se află în Regatul Unit, în cazul în care activitățile de prelucrare sunt legate de oferirea de bunuri sau servicii unor astfel de persoane vizate sau de monitorizarea comportamentului acestora ([35]). Aceasta reflectă abordarea adoptată la articolul 3 din Regulamentul (UE) 2016/679.

2.4. **Definițiile datelor cu caracter personal și conceptele de operator și persoană împuternicită de operator**

(23) Definițiile următorilor termeni: date cu caracter personal, prelucrare, operator, persoană împuternicită de operator și pseudonimizare, prevăzute în Regulamentul (UE) 2016/679, au fost menținute fără modificări substanțiale în RGPD al Regatului Unit ([36]). În plus, categoriile speciale de date sunt definite la articolul 9 alineatul (1) din RGPD al Regatului Unit în același mod ca în Regulamentul (UE) 2016/679 („originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, afilierea sindicală, prelucrarea datelor genetice, prelucrarea datelor biometrice pentru identificarea unică a unei persoane fizice sau prelucrarea datelor privind sănătatea sau a datelor privind viața sexuală și orientarea sexuală a unei persoane fizice"). Secțiunea 205 din DPA din 2018 prevede definiția „datelor biometrice" ([37]), a „datelor privind sănătatea" ([38]) și a „datelor genetice" ([39]).

2.5. **Garanții, drepturi și obligații**

2.5.1. *Legalitatea și corectitudinea prelucrării*

(24) Datele cu caracter personal ar trebui prelucrate în mod legal și echitabil.

(25) Principiile legalității, echității și transparenței, precum și motivele prelucrării legale sunt garantate în legislația Regatului Unit prin articolul 5 alineatul (1) litera (a) și prin articolul 6 alineatul (1) din RGPD al Regatului Unit, care sunt identice cu dispozițiile corespunzătoare din Regulamentul (UE) 2016/679 ([40]). Secțiunea 8 din DPA din 2018 completează articolul 6 alineatul (1) litera (e) prin stipularea faptului că prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (e) din RGPD al Regatului Unit (necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul) include

([33]) Articolul 2 alineatul (2) literele (b) și (c) din RGPD al Regatului Unit.

([34]) Același domeniu de aplicare teritorial se aplică prelucrării datelor cu caracter personal în temeiul părții 2 din DPA din 2018 care completează RGPD al Regatului Unit (secțiunea 207 punctul 1A).

([35]) Aceasta înseamnă în special că DPA din 2018 și, prin urmare, prezenta decizie nu se aplică teritoriilor dependente ale Coroanei Britanice (Jersey, Guernsey și Insula Man) și teritoriilor de peste mări ale Regatului Unit, cum ar fi, de exemplu, Insulele Falkland și teritoriul Gibraltarului.

([36]) Articolul 4 alineatele (1), (2), (5), (7) și (8) din RGPD al Regatului Unit.

([37]) „Date biometrice" înseamnă date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice.

([38]) „Date privind sănătatea" înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv acordarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia.

([39]) „Date genetice" înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea respectivei persoane fizice, astfel cum rezultă în special în urma unei analize a unei probe biologice prelevate de la acea persoană fizică.

([40]) În temeiul articolului 6 alineatul (1) din RGPD al Regatului Unit, prelucrarea este legală numai dacă și în măsura în care: (a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice; (b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract; (c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului; (d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice; (e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul; sau (f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

prelucrarea datelor cu caracter personal care este necesară pentru administrarea justiției, exercitarea unei funcții a oricăreia dintre camerele Parlamentului, exercitarea unei funcții conferite unei persoane de o lege sau o normă juridică, exercitarea unei funcții a Coroanei, a unui ministru al Coroanei sau a unui departament guvernamental sau a unei activități care sprijină sau promovează angajamentul democratic.

(26) În ceea ce privește consimțământul (unul dintre motivele prelucrării legale), RGPD al Regatului Unit menține, de asemenea, nemodificate condițiile prevăzute la articolul 7 din Regulamentul (UE) 2016/679, și anume operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul, o cerere scrisă privind consimțământul trebuie prezentată utilizând un limbaj clar și simplu, persoana vizată trebuie să aibă dreptul de a-și retrage în orice moment consimțământul, iar atunci când se evaluează dacă consimțământul este dat în mod liber, ar trebui să se țină seama de faptul că executarea unui contract este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract. În plus, în temeiul articolului 8 din RGPD al Regatului Unit, în contextul furnizării de servicii ale societății informaționale, consimțământul unui copil este legal numai atunci când copilul are o vârstă de cel puțin 13 ani. Aceasta se încadrează în categoria de vârstă stabilită la articolul 8 din Regulamentul (UE) 2016/679.

2.5.2. *Prelucrarea de categorii speciale de date cu caracter personal*

(27) Ar trebui să existe garanții specifice în cazul în care sunt prelucrate „categorii speciale” de date.

(28) RGPD al Regatului Unit și DPA din 2018 conțin norme specifice în ceea ce privește prelucrarea categoriilor speciale de date cu caracter personal, care sunt definite la articolul 9 alineatul (1) din RGPD al Regatului Unit în același mod ca în Regulamentul (UE) 2016/679 (a se vedea considerentul 23). În conformitate cu articolul 9 din RGPD al Regatului Unit, prelucrarea categoriilor speciale de date este, în principiu, interzisă, cu excepția cazului în care se aplică o excepție specifică.

(29) Aceste excepții [enumerate la articolul 9 alineatele (2) și (3) din RGPD al Regatului Unit] nu aduc nicio modificare de substanță celor de la articolul 9 alineatele (2) și (3) din Regulamentul (UE) 2016/679. Cu excepția cazului în care persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal, prelucrarea unor categorii speciale de date cu caracter personal este permisă numai în circumstanțe specifice și limitate. În majoritatea cazurilor, prelucrarea datelor sensibile trebuie să fie necesară pentru un scop specific definit în dispoziția relevantă [a se vedea articolul 9 alineatul (2) literele (b), (c), (f), (g), (h), (i) și (j)].

(30) În plus, în cazul în care o excepție în temeiul articolului 9 alineatul (2) din RGPD al Regatului Unit impune o autorizare prin lege sau se referă la interesul public, secțiunea 10 din DPA din 2018, împreună cu anexa 1 la DPA din 2018, precizează condițiile care trebuie îndeplinite pentru ca excepțiile să fie invocate. De exemplu, în cazul prelucrării datelor sensibile în scopul protejării „sănătății publice” [articolul 9 alineatul 2 litera (i) din RGPD al Regatului Unit], anexa 1 partea 1 punctul 3 litera (b) impune ca, pe lângă testul necesității, o astfel de prelucrare să fie efectuată „de către sau sub responsabilitatea unui cadru medical” sau „de către o altă persoană care are obligația de a păstra confidențialitatea în temeiul unei legi sau a unei norme juridice”, inclusiv în temeiul obligației bine stabilite de common law privind confidențialitatea.

(31) În cazul în care datele sensibile sunt prelucrate din motive de interes public major [articolul 9 alineatul (2) litera (g) din RGPD al Regatului Unit], partea 2 din anexa 1 la DPA din 2018 prevede o listă exhaustivă a scopurilor care pot fi considerate de interes public major și, pentru fiecare dintre aceste scopuri, stabilește condiții suplimentare specifice. De exemplu, promovarea diversității rasiale și etnice la nivelurile superioare ale organizațiilor este recunoscută ca fiind un interes public major. Prelucrarea datelor sensibile în acest scop specific face obiectul unor cerințe detaliate, inclusiv cerința ca prelucrarea să fie efectuată în cadrul unui proces de identificare a persoanelor potrivite pentru a deține funcții de conducere, să fie necesară pentru promovarea diversității rasiale și etnice și să nu fie susceptibilă de a cauza prejudicii sau suferințe clinice substanțiale persoanei vizate.

(32) Secțiunea 11 punctul 1 din DPA din 2018 stabilește condițiile pentru prelucrarea datelor cu caracter personal în circumstanțele descrise la articolul 9 alineatul (3) din RGPD al Regatului Unit în ceea ce privește obligația de păstrare a confidențialității. Aceasta include circumstanțele în care este efectuată de către sau sub responsabilitatea unui cadru medical sau a unui profesionist din domeniul asistenței sociale sau de către o altă persoană care, în circumstanțele respective, are obligația de păstrare a confidențialității în temeiul unei legi sau al unei norme juridice.

(33) În plus, multe dintre excepțiile enumerate la articolul 9 alineatul (2) din RGPD al Regatului Unit impun garanții adecvate și specifice pentru a fi utilizate. În funcție de natura prelucrării și de nivelul de risc pentru drepturile și libertățile persoanelor vizate, condițiile de prelucrare prevăzute în anexa 1 la DPA din 2018 stabilesc garanții diferite. Anexa 1 stabilește, pe rând, condițiile pentru fiecare situație de prelucrare.

(34) În unele cazuri, DPA din 2018 reglementează și limitează tipul de date sensibile care pot fi prelucrate pentru ca un anumit temei juridic să fie respectat. De exemplu, punctul 8 din anexa 1 autorizează prelucrarea datelor sensibile în scopul promovării egalității de șanse sau de tratament. Această condiție de prelucrare poate fi utilizată numai dacă datele dezvăluie originea rasială sau etnică, convingerile religioase sau filozofice, orientarea sexuală sau dacă este vorba despre date privind sănătatea.

(35) În unele cazuri, DPA din 2018 limitează tipul de operator care poate utiliza condiția de prelucrare. De exemplu, punctul 23 din anexa 1 prevede prelucrarea datelor sensibile în ceea ce privește răspunsurile reprezentanților aleși către public. Această condiție de prelucrare poate fi utilizată numai în cazul în care operatorul este reprezentantul ales sau acționează sub autoritatea acestuia.

(36) În alte cazuri, DPA din 2018 stabilește limite privind categoriile de persoane vizate pentru condiția de prelucrare care urmează să fie utilizată. De exemplu, punctul 21 din anexa 1 reglementează prelucrarea datelor sensibile pentru sistemele de pensii ocupaționale. Această condiție poate fi utilizată numai în cazul în care persoanele vizate în cauză sunt frați/surori, părinți, bunici sau străbunici ai membrului afiliat.

(37) În plus, atunci când se bazează pe excepțiile prevăzute la articolul 9 alineatul (2) din RGPD al Regatului Unit, care sunt specificate mai detaliat în secțiunea 10 din DPA din 2018, împreună cu anexa 1 la DPA din 2018, operatorul trebuie să elaboreze, în majoritatea cazurilor, un „document de politică adecvat”. Acesta trebuie să prezinte procedurile operatorului de asigurare a conformității cu principiile prevăzute la articolul 5 din RGPD al Regatului Unit. Acesta trebuie, de asemenea, să stabilească politici de păstrare și ștergere, cu indicarea perioadei probabile de stocare. Operatorii trebuie să revizuiască și să actualizeze acest document, după caz. Operatorul trebuie să păstreze documentul de politică pentru o perioadă de șase luni de la finalizarea prelucrării și, la cerere, să îl pună la dispoziția comisarului pentru informații ([41]).

(38) În temeiul punctului 41 din anexa 1 la DPA din 2018, documentul de politică trebuie să fie întotdeauna însoțit de o înregistrare suplimentară a prelucrării. Această înregistrare trebuie să urmărească angajamentele incluse în documentul de politică, și anume dacă datele sunt șterse sau menținute în conformitate cu politicile. În cazul în care politicile nu au fost respectate, motivele trebuie să se înregistreze în registru. Înregistrarea trebuie să descrie, de asemenea, modul în care prelucrarea respectă articolul 6 din RGPD al Regatului Unit (legalitatea prelucrării) și condiția specifică din anexa 1 la DPA din 2018 invocată.

(39) În cele din urmă, la fel ca Regulamentul (UE) 2016/679, RGPD al Regatului Unit prevede, de asemenea, garanții generale pentru anumite operațiuni de prelucrare a unor categorii speciale de date. Articolul 35 din RGPD al Regatului Unit prevede efectuarea unei evaluări a impactului asupra protecției datelor în cazul în care categorii speciale de date sunt prelucrate pe scară largă. În temeiul articolului 37 din RGPD al Regatului Unit, un operator sau o persoană împuternicită de operator trebuie să desemneze un responsabil cu protecția datelor în cazul în care activitățile sale principale constau în prelucrarea pe scară largă a unor categorii speciale de date.

(40) În ceea ce privește datele cu caracter personal referitoare la condamnări penale și infracțiuni, articolul 10 din RGPD al Regatului Unit este identic cu articolul 10 din Regulamentul (UE) 2016/679. Acesta permite prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni numai sub controlul unei autorități de stat sau atunci când prelucrarea este autorizată de dreptul intern care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate.

(41) În cazul în care prelucrarea datelor referitoare la condamnări penale și infracțiuni nu se efectuează sub controlul unei autorități de stat, secțiunea 10 punctul 5 din DPA din 2018 prevede că o astfel de prelucrare poate avea loc numai în scopurile specifice/în situațiile specifice prevăzute în părțile 1, 2 și 3 din anexa 1 la DPA din 2018 și face obiectul cerințelor specifice care sunt stabilite pentru fiecare dintre aceste scopuri/situații. De exemplu, datele privind condamnările penale pot fi prelucrate de organisme fără scop lucrativ dacă prelucrarea este efectuată: (a) în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau un alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical; și (b) cu condiția ca: (i) prelucrarea să se refere numai la membrii sau la foștii membri ai organismului sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale; și (ii) ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate.

([41]) Punctele 38-40 din anexa 1 la DPA din 2018.

(42) În plus, partea 3 din anexa 1 la DPA din 2018 stabilește circumstanțele suplimentare în care pot fi utilizate date privind condamnările penale care corespund temeiurilor juridice pentru prelucrarea datelor sensibile de la articolul 9 alineatul (2) din Regulamentul (UE) 2016/679 și din RGPD al Regatului Unit (de exemplu, consimțământul persoanei vizate, interesele vitale ale unei persoane în cazul în care persoana vizată se află în imposibilitatea legală sau fizică de a-și da consimțământul, dacă datele au fost deja făcute publice în mod evident de către persoana vizată, dacă prelucrarea este necesară pentru stabilirea, exercitarea sau apărarea unui drept în instanță etc.).

2.5.3. *Limitări legate de scop, exactitate, reducerea la minimum a datelor, limitări legate de stocare și securitatea datelor*

(43) Datele cu caracter personal ar trebui să fie prelucrate într-un scop anume și să fie utilizate ulterior numai în măsura în care acest lucru nu este incompatibil cu scopul prelucrării.

(44) Acest principiu este prevăzut la articolul 5 alineatul (1) litera (b) din Regulamentul (UE) 2016/679 și a fost menținut fără modificări la articolul 5 alineatul (1) litera (b) din RGPD al Regatului Unit. Condițiile privind prelucrarea compatibilă ulterioară în temeiul articolului 6 alineatul (4) din Regulamentul (UE) 2016/679 au fost, de asemenea, menținute fără modificări semnificative la articolul 6 alineatul (4) literele (a)-(e) din RGPD al Regatului Unit.

(45) În plus, datele ar trebui să fie exacte și, dacă este necesar, actualizate. De asemenea, ar trebui să fie adecvate, relevante și neexcesive în raport cu scopurile în care sunt prelucrate și, în principiu, păstrate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele cu caracter personal.

(46) Aceste principii privind reducerea la minimum a datelor, exactitatea și limitările legate de stocare sunt prevăzute la articolul 5 alineatul (1) literele (c)-(e) din Regulamentul (UE) 2016/679 și sunt menținute fără modificări la articolul 5 alineatul (1) literele (c)-(e) din RGPD al Regatului Unit.

(47) Datele cu caracter personal ar trebui prelucrate într-un mod care să le asigure securitatea, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale. În acest scop, operatorii economici ar trebui să ia măsurile tehnice sau organizatorice adecvate pentru a proteja datele cu caracter personal împotriva eventualelor amenințări. Aceste măsuri ar trebui să fie evaluate luând în considerare cunoștințele actuale și costurile aferente.

(48) Securitatea datelor este consacrată în legislația Regatului Unit prin principiul integrității și confidențialității prevăzut la articolul 5 alineatul (1) litera (f) din RGPD al Regatului Unit și la articolul 32 din RGPD al Regatului Unit privind securitatea prelucrării. Dispozițiile menționate sunt identice cu dispozițiile corespunzătoare din Regulamentul (UE) 2016/679. În plus, în aceleași condiții ca cele prevăzute la articolele 33 și 34 din Regulamentul (UE) 2016/679, RGPD al Regatului Unit prevede notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal (articolul 33 din RGPD al Regatului Unit) și informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal (articolul 34 din RGPD al Regatului Unit).

2.5.4. *Transparența*

(49) Persoanele vizate ar trebui să fie informate cu privire la principalele caracteristici ale prelucrării datelor lor cu caracter personal.

(50) Acest lucru este garantat prin articolele 13 și 14 din RGPD al Regatului Unit, care, pe lângă un principiu general al transparenței, prevăd norme privind informațiile care trebuie furnizate persoanei vizate ([42]). RGPD al Regatului Unit nu introduce nicio modificare substanțială a acestor norme în comparație cu articolele corespunzătoare din Regulamentul (UE) 2016/679. Cu toate acestea, la fel ca în Regulamentul (UE) 2016/679, cerințele de transparență prevăzute la articolele respective fac obiectul mai multor excepții prevăzute în DPA din 2018 (a se vedea considerentele 55-72).

([42]) La articolul 13 alineatul (1) litera (f) și la articolul 14 alineatul (1) litera (f), trimiterile la deciziile Comisiei privind caracterul adecvat al nivelului de protecție au fost înlocuite cu trimiteri la un instrument echivalent din Regatul Unit, și anume la regulamentele privind caracterul adecvat al nivelului de protecție din cadrul DPA din 2018. În plus, la articolul 14 alineatul (5) literele (c)-(d), trimiterile la dreptul Uniunii sau la dreptul intern („*Member State law*") au fost înlocuite cu o trimitere la dreptul intern („*domestic law*") [ca exemple de astfel de norme de drept intern care pot intra sub incidența articolului 14 alineatul (5) litera (c), Regatul Unit a menționat secțiunea 7 din *Scrap Metal Dealers Act 2013* (Legea comercianților de deșeuri metalice din 2013) care prevede norme pentru registrul autorizațiilor pentru deșeuri metalice sau partea 35 din *Companies Act 2006* (Legea societăților comerciale din 2006) care prevede normele pentru registrul comerțului]. În mod similar, un exemplu de drept intern care poate intra sub incidența articolului 14 alineatul (5) litera (d) ar putea include o legislație care să stabilească norme privind secretul profesional sau obligații care reies din contractele de muncă sau obligația de confidențialitate prevăzută de common law (cum ar fi datele cu caracter personal prelucrate de cadrele medicale, resursele umane, asistenții sociali etc.).

2.5.5. *Drepturi individuale*

(51) Persoanele vizate ar trebui să aibă anumite drepturi care pot fi impuse operatorului sau persoanei împuternicite de operator, în special dreptul de acces la date, dreptul de a se opune prelucrării și dreptul la rectificarea și ștergerea datelor. În același timp, aceste drepturi pot face obiectul unor restricții, în măsura în care aceste restricții sunt necesare și proporționale pentru a proteja securitatea publică sau alte obiective importante de interes public general.

2.5.5.1. Drepturi materiale

(52) RGPD al Regatului Unit acordă persoanelor aceleași drepturi opozabile ca Regulamentul (UE) 2016/679. Dispozițiile care prevăd drepturile persoanelor au fost menținute în RGPD al Regatului Unit fără modificări semnificative.

(53) Drepturile includ dreptul de acces al persoanei vizate (articolul 15 din RGPD al Regatului Unit), dreptul la rectificare (articolul 16 din RGPD al Regatului Unit), dreptul la ștergerea datelor (articolul 17 din RGPD al Regatului Unit), dreptul la restricționarea prelucrării (articolul 18 din RGPD al Regatului Unit), o obligație de notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării (articolul 19 din RGPD al Regatului Unit), dreptul la portabilitatea datelor (articolul 20 din RGPD al Regatului Unit) și dreptul la opoziție (articolul 21 din RGPD al Regatului Unit) ([43]). Acesta din urmă include, de asemenea, dreptul unei persoane vizate de a se opune prelucrării datelor cu caracter personal în scopul marketingului direct prevăzut la articolul 21 alineatele (2) și (3) din Regulamentul (UE) 2016/679. În plus, în temeiul secțiunii 122 din DPA din 2018, comisarul pentru informații trebuie să elaboreze un cod de bune practici în ceea ce privește realizarea marketingului direct în conformitate cu cerințele legislației privind protecția datelor [și cu *Privacy and Electronic Communications (EC Directive) Regulations 2003* – Regulamentele din 2003 privind confidențialitatea și comunicațiile electronice (Directiva CE)], precum și alte orientări pentru promovarea bunelor practici în materie de marketing direct pe care comisarul le consideră adecvate. Biroul comisarului pentru informații elaborează în prezent codul de marketing direct ([44]).

(54) Dreptul persoanei vizate de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă, astfel cum se prevede la articolul 22 din RGPD, a fost, de asemenea, menținut în RGPD al Regatului Unit fără modificări substanțiale. Cu toate acestea, a fost adăugat un nou alineat (3A) pentru a menționa că secțiunea 14 din DPA din 2018 stabilește garanții pentru drepturile, libertățile și interesele legitime ale persoanelor vizate atunci când prelucrarea este efectuată în temeiul articolului 22 alineatul (2) litera (b) din RGPD al Regatului Unit. Acesta se aplică numai atunci când temeiul unei astfel de decizii este o autorizație sau o cerință în temeiul legislației Regatului Unit și nu se aplică în cazul în care decizia este necesară în temeiul unui contract sau este luată cu consimțământul explicit al persoanei vizate. În cazul în care se aplică secțiunea 14 din DPA din 2018, operatorul trebuie să notifice în scris persoanei vizate, cât mai curând posibil din punct de vedere practic, că a fost luată o decizie bazată exclusiv pe prelucrarea automată. Persoana vizată are dreptul de a solicita operatorului – în termen de o lună de la primirea notificării – să reexamineze decizia sau să ia o nouă decizie care nu se bazează exclusiv pe prelucrarea automată. Secretarul de stat este împuternicit să adopte garanții suplimentare în ceea ce privește procesul decizional automatizat. Această competență nu a fost încă exercitată.

2.5.5.2. Restricții privind drepturile individuale și alte dispoziții

(55) DPA din 2018 stabilește o serie de restricții privind drepturile individuale, în conformitate cu articolul 23 din RGPD al Regatului Unit. În acest cadru nu sunt introduse restricții în ceea ce privește dreptul de a se opune marketingului direct, astfel cum se prevede la articolul 21 alineatele (2) și (3) din RGPD al Regatului Unit, sau dreptul de a nu face obiectul procesului decizional automatizat, astfel cum se prevede la articolul 22 din RGPD al Regatului Unit.

(56) Restricțiile sunt detaliate în anexele 2-4 la DPA din 2018. Autoritățile Regatului Unit au explicat că sunt ghidate de două principii: principiul specificității (adoptarea unei abordări granulare, împărțirea restricțiilor ample în dispoziții multiple, mai specifice) și principiul condiționalității (fiecare dispoziție este completată de garanții sub formă de limitări sau condiții pentru a preveni abuzurile) ([45]).

([43]) La articolul 17 alineatul (1) litera (e) și la articolul 17 alineatul (3) litera (b), trimiterile la dreptul Uniunii sau la dreptul intern („*Member State law*") au fost înlocuite cu o trimitere la dreptul intern („*domestic law*") [ca exemple de astfel de norme de drept intern în temeiul articolului 17 alineatul (1) litera (e), Regatul Unit a menționat *Education (Pupil Information) (England) Regulations 2006* – Regulamentele din 2006 privind educația (informații referitoare la elevi) (Anglia), care impune ștergerea numelor elevilor din registrele școlare după ce aceștia au ieșit din sistemul școlar, sau *Medical Act 1983* (Legea din 1983 privind activitățile medicale), secțiunea 34F, care stabilește normele privind ștergerea numelor din Registrul medicilor generaliști și din Registrul medicilor specialiști.

([44]) Proiectul de cod de bune practici poate fi consultat la următoarea adresă: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf

([45]) Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat, secțiunea E: Restricții, pagina 1, disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf

(57) Restricțiile descrise la articolul 23 alineatul (1) din RGPD al Regatului Unit sunt menite să garanteze că acestea se aplică numai în circumstanțe specifice, atunci când acest lucru este necesar într-o societate democratică și proporțional cu obiectivul legitim pe care îl urmăresc. În plus, în conformitate cu jurisprudența constantă privind interpretarea restricțiilor, o derogare de la regimul de protecție a datelor poate fi aplicată în orice caz particular numai dacă acest lucru este necesar și proporțional ([46]). Testul necesității a trebuit să fie „strict, impunând ca orice ingerință în drepturile persoanei vizate să fie proporțională cu gravitatea amenințării la adresa interesului public. Prin urmare, exercițiul implică o analiză clasică a proporționalității ([47])".

(58) Obiectivele urmărite de aceste restricții corespund celor enumerate la articolul 23 din Regulamentul (UE) 2016/679, cu excepția restricțiilor privind apărarea și securitatea națională, care sunt reglementate în schimb de secțiunea 26 din DPA din 2018, dar fac obiectul acelorași cerințe de necesitate și proporționalitate (a se vedea considerentele 63-66).

(59) Unele dintre restricții, de exemplu cele legate de prevenirea sau depistarea infracțiunilor, de arestarea sau urmărirea penală a infractorilor, precum și de stabilirea sau colectarea impozitelor sau a taxelor ([48]), permit restricționarea tuturor drepturilor individuale și a obligațiilor în materie de transparență [cu excepția drepturilor prevăzute la articolul 21 alineatul (2) și la articolul 22]. Domeniul de aplicare al altor restricții se limitează la obligațiile de transparență și la drepturile de acces, cum ar fi restricțiile referitoare la secretul profesional al avocatului ([49]), la dreptul de a nu fi supus obligației de a furniza informații care ar conduce la autoincriminare ([50]), precum și la finanțarea întreprinderilor, în special la prevenirea utilizării abuzive a informațiilor privilegiate ([51]). Puține dintre restricții permit o limitare a obligației operatorului de a informa o persoană vizată cu privire la încălcarea securității datelor și a principiilor limitărilor legate de scop, legalității, echității și transparenței prelucrării ([52]).

(60) Unele restricții se aplică automat „integral" unui anumit tip de prelucrare a datelor cu caracter personal (de exemplu, aplicarea obligațiilor de transparență și a drepturilor individuale este exclusă în cazul în care datele cu caracter personal sunt prelucrate în scopul evaluării capacității unei persoane de a ocupa o funcție judiciară sau atunci când datele cu caracter personal sunt prelucrate de către o instanță judecătorească, un tribunal sau o persoană care acționează în exercițiul unei funcții judiciare).

(61) Cu toate acestea, în majoritatea cazurilor, punctul relevant din anexa 2 la DPA din 2018 precizează că restricția se aplică numai în cazul în care (și în măsura în care) aplicarea dispozițiilor „ar putea aduce atingere" obiectivului legitim urmărit de restricția respectivă: de exemplu, dispozițiile enumerate din RGPD al Regatului Unit nu se aplică datelor cu caracter personal prelucrate în scopul prevenirii sau depistării infracțiunilor, al arestării sau urmăririi penale a infractorilor sau al stabilirii sau colectării impozitelor sau a taxelor „în măsura în care aplicarea dispozițiilor respective ar putea aduce atingere" oricăruia dintre aceste aspecte ([53]).

(62) Standardul referitor la „ar putea aduce atingere" a fost interpretat în mod consecvent de instanțele din Regatul Unit ca însemnând „o probabilitate foarte semnificativă și hotărâtoare de a aduce atingere intereselor publice identificate" ([54]). Prin urmare, o restricție care face obiectul testului prejudiciului poate fi invocată numai dacă și în măsura în care există o șansă semnificativă ca acordarea unui anumit drept să aducă atingere interesului public în cauză. Operatorul este responsabil de evaluarea de la caz la caz a îndeplinirii acestor condiții ([55]).

(63) Pe lângă restricțiile cuprinse în anexa 2 la DPA din 2018, secțiunea 26 din DPA din 2018 prevede o derogare care poate fi aplicată anumitor dispoziții din RGPD al Regatului Unit și din DPA din 2018 dacă derogarea respectivă este necesară în scopul protejării securității naționale sau în scopuri de apărare. Această derogare se aplică principiilor privind protecția datelor (cu excepția principiului legalității), obligațiilor în materie de transparență, drepturilor persoanei vizate, obligației de a notifica o încălcare a securității datelor, normelor privind transferurile

([46]) *Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor* [2019] EWHC 2562 (Admin), punctele 40 și 41.

([47]) *Guriev/Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), punctul 43. Cu privire la acest punct, a se vedea, de asemenea, *Lin/Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), punctul 80.

([48]) Punctul 2 din anexa 2 la DPA din 2018.

([49]) Punctul 19 din anexa 2 la DPA din 2018.

([50]) Punctul 20 din anexa 2 la DPA din 2018.

([51]) Punctul 21 din anexa 2 la DPA din 2018.

([52]) De exemplu, restricționarea dreptului la o notificare privind încălcarea securității datelor este permisă numai în ceea ce privește infracțiunile și impozitarea (punctul 2 din anexa 2 la DPA din 2018), privilegiul parlamentar (punctul 13 din anexa 2 la DPA din 2018) și prelucrarea în scopuri jurnalistice, academice, artistice și literare (punctul 26 din anexa 2 la DPA din 2018).

([53]) Punctul 2 din anexa 2 la DPA din 2018.

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

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

internaționale, unora dintre sarcinile și competențele comisarului pentru informații și normelor privind căile de atac, răspunderile și sancțiunile, cu excepția dispoziției privind condițiile generale pentru impunerea amenzilor administrative prevăzute la articolul 83 din RGPD al Regatului Unit și a dispoziției privind sancțiunile de la articolul 84 din RGPD al Regatului Unit. În plus, secțiunea 28 din DPA din 2018 modifică aplicarea articolului 9 alineatul (1) pentru a permite prelucrarea categoriilor speciale de date de la articolul 9 alineatul (1) din RGPD al Regatului Unit, în măsura în care prelucrarea este efectuată pentru apărarea securității naționale sau în scopuri de apărare, precum și cu garanții adecvate pentru drepturile și libertățile persoanelor vizate ([56]).

(64) Derogarea poate fi aplicată numai în măsura în care este necesară pentru a proteja securitatea națională sau apărarea. La fel ca și în cazul celorlalte derogări prevăzute de DPA din 2018, aceasta trebuie luată în considerare și invocată de operator de la caz la caz. În plus, orice aplicare a derogării trebuie să fie în conformitate cu standardele privind drepturile omului (bazate pe Legea privind drepturile omului din 1998), conform cărora orice ingerință în viața privată ar trebui să fie necesară și proporțională într-o societate democratică ([57]).

(65) Această interpretare a derogării este confirmată de ICO care a emis orientări detaliate privind aplicarea derogării în materie de securitate națională și apărare, clarificând faptul că aceasta trebuie luată în considerare și aplicată de către operator de la caz la caz ([58]). În special, orientările subliniază că „aceasta nu este o derogare generală" și că, pentru a o invoca, „nu este suficient ca datele să fie prelucrate în scopuri de securitate națională". În schimb, operatorul care se bazează pe aceasta trebuie „să demonstreze că există o posibilitate reală de a avea un efect negativ asupra securității naționale" și, atunci când este necesar, operatorul trebuie să „furnizeze [ICO] dovezi cu privire la motivele pentru care a utilizat această derogare". Orientările conțin o listă de verificare și o serie de exemple pentru a clarifica mai bine condițiile în care poate fi invocată această derogare.

(66) Prin urmare, faptul că datele sunt prelucrate în scopuri de securitate națională sau de apărare nu este suficient în sine pentru ca derogarea să fie aplicată. Un operator trebuie să ia în considerare consecințele reale pentru securitatea națională dacă ar trebui să respecte dispoziția specifică privind protecția datelor. Derogarea poate fi aplicată numai acelor dispoziții specifice care au fost identificate ca prezentând riscul respectiv și trebuie să fie aplicată cât mai restrictiv posibil ([59]).

(67) Această abordare a fost confirmată de Information Tribunal ([60]). În cauza *Baker/Secretary of State for the Home Department* („Baker/Secretary of State"), s-a stabilit că este ilegal să se aplice derogarea referitoare la securitatea națională ca derogare generală pentru cererile de acces primite de serviciile de informații. În schimb, derogarea a trebuit să fie aplicată de la caz la caz, analizând fiecare cerere pe fond și având în vedere dreptul persoanelor la respectarea vieții lor private ([61]).

([56]) Potrivit informațiilor furnizate de autoritățile din Regatul Unit, în cazul în care prelucrarea se efectuează în contextul securității naționale, operatorii vor aplica, de regulă, garanții și măsuri de securitate sporite în cazul prelucrării, care să reflecte natura sensibilă a prelucrării. Tipul de garanții adecvate va depinde de riscurile pe care le prezintă prelucrarea efectuată. Acest lucru ar putea include restricții privind accesul la date, astfel încât acestea să poată fi accesate numai de către persoane autorizate care să dețină o autorizare de securitate adecvată, restricții stricte privind schimbul de date și standardul ridicat de securitate aplicat procedurilor de stocare și de gestionare.

([57]) A se vedea, de asemenea, *Guriev/Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), punctul 45; *Lin/Commissioner of the Police for the Metropolis* [2015] EWHC 2484 (QB), punctul 80.

([58]) A se vedea orientările ICO privind derogarea în materie de securitate națională și apărare, disponibile la următoarea adresă: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence

([59]) Conform unui exemplu furnizat de autoritățile Regatului Unit, în cazul în care un terorist suspectat care face obiectul unei investigații active a MI5 a prezentat Ministerului de Interne o cerere de acces (de exemplu, deoarece este implicat într-un litigiu cu Ministerul de Interne cu privire la aspecte legate de imigrație), ar fi necesar să se protejeze împotriva divulgării către persoana vizată orice date pe care este posibil ca MI5 să le fi comunicat Ministerului de Interne cu privire la investigații în curs, care ar putea prejudicia sursele, metodele sau tehnicile sensibile și/sau ar putea conduce la o creștere a amenințării pe care o reprezintă persoana respectivă. În astfel de circumstanțe, este probabil ca pragul de aplicare a derogării prevăzute la secțiunea 26 să fi fost atins și să fie necesară o derogare de la divulgarea informațiilor pentru a proteja securitatea națională. Cu toate acestea, în cazul în care Ministerul de Interne ar deține, de asemenea, date cu caracter personal cu privire la persoana respectivă, care nu au legătură cu investigația MI5, iar informațiile respective ar putea fi furnizate fără riscul de a aduce atingere securității naționale, derogarea privind securitatea națională nu ar fi aplicabilă atunci când se are în vedere divulgarea de informații către persoana respectivă. ICO elaborează în prezent orientări cu privire la modul în care operatorii ar trebui să abordeze utilizarea derogării din secțiunea 26. Se preconizează că aceste orientări vor fi publicate până la sfârșitul lunii martie 2021.

([60]) Information Tribunal a fost înființat pentru a soluționa căile de atac în materie de protecție a datelor în temeiul Legii privind protecția datelor din 1984. În 2010, Information Tribunal a devenit parte din General Regulatory Chamber din cadrul First Tier Tribunal (Tribunalul de Primă Instanță), în cadrul reformei structurii sistemului de tribunale din Regatul Unit.

([61]) A se vedea *Baker/Secretary of State for the Home Department* [2001] UKIT NSA2 („Baker/Secretary of State").

2.5.6. *Restricții privind datele cu caracter personal prelucrate în scopuri jurnalistice, artistice, academice și literare, precum și în scopuri de arhivare și cercetare*

(68) Articolul 85 alineatul (2) din RGPD al Regatului Unit permite ca datele cu caracter personal prelucrate în scopuri jurnalistice, artistice, academice și literare să fie exceptate de la aplicarea mai multor dispoziții din RGPD al Regatului Unit. Partea 5 din anexa 2 la DPA din 2018 stabilește derogările pentru prelucrarea în aceste scopuri. Aceasta prevede derogări de la principiile privind protecția datelor (cu excepția principiului integrității și confidențialității), temeiurile juridice pentru prelucrare (inclusiv categoriile speciale de date și date privind condamnări penale etc.), condițiile pentru consimțământ, obligațiile în materie de transparență, drepturile persoanelor vizate, obligația de a notifica încălcarea securității datelor, cerința de a consulta comisarul pentru informații înainte de prelucrarea cu risc ridicat și normele privind transferurile internaționale ([62]). În această privință, RGPD al Regatului Unit nu se abate în mod substanțial de la Regulamentul (UE) 2016/679 care, la articolul 85, prevede, de asemenea, posibilitatea de a excepta prelucrarea efectuată în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare de la o serie de cerințe ale Regulamentului (UE) 2016/679. Dispozițiile DPA din 2018, în special partea 5 din anexa 2 , sunt compatibile cu RGPD al Regatului Unit.

(69) Principalul exercițiu de echilibru care trebuie efectuat în temeiul articolului 85 din RGPD al Regatului Unit se referă la întrebarea dacă o derogare de la normele de protecție a datelor menționate în considerentul 68 este „necesară pentru a asigura un echilibru între dreptul la protecția datelor cu caracter personal și libertatea de exprimare și de informare" ([63]). În conformitate cu punctul 26 subpunctele 2 și 3 din anexa 2 la DPA din 2018, Regatul Unit aplică un test al „convingerii rezonabile" pentru a se ajunge la acest echilibru. Pentru ca o derogare să fie justificată, operatorul trebuie să considere în mod rezonabil (i) că publicarea este în interes public; și (ii) aplicarea dispoziției relevante din RGPD ar fi incompatibilă cu scopurile jurnalistice, academice, artistice sau literare. Astfel cum este confirmat de jurisprudență ([64]), testul „convingerii rezonabile" are atât o componentă subiectivă, cât și una obiectivă: este insuficient ca operatorul să demonstreze că el însuși a considerat conformitatea ca fiind incompatibilă. Convingerea sa trebuie să fie rezonabilă, și anume ar putea fi crezută de o persoană rezonabilă, cunoscând faptele relevante. Prin urmare, pentru a putea demonstra caracterul rezonabil, operatorul trebuie să depună diligența necesară atunci când își formează convingerea. Conform explicațiilor furnizate de autoritățile din Regatul Unit, testul „convingerii rezonabile" trebuie să fie efectuat de la derogare la derogare ([65]). În cazul în care condițiile sunt îndeplinite, derogarea este considerată necesară și proporțională în temeiul legislației Regatului Unit.

(70) În conformitate cu secțiunea 124 din DPA din 2018, ICO trebuie să elaboreze un cod de bune practici privind protecția datelor și jurnalismul. Lucrările cu privire la acest cod sunt în curs de desfășurare. Au fost emise orientări cu privire la această chestiune în temeiul Legii privind protecția datelor din 1998, care subliniază în special faptul că, pentru a se prevala de această derogare, nu este suficient să se afirme doar că respectarea ar reprezenta un inconvenient pentru activitățile jurnalistice, ci trebuie să existe un argument clar potrivit căruia

([62]) A se vedea articolul 85 din RGPD al Regatului Unit și partea 5 punctul 26 subpunctul 9 din anexa 2 la DPA din 2018.

([63]) În conformitate cu partea 5 punctul 26 subpunctul 2 din anexa 2 la DPA din 2018, excepția se aplică prelucrării datelor cu caracter personal efectuate în scopuri speciale (scopuri jurnalistice, academice, artistice și literare), dacă prelucrarea este efectuată în vederea publicării de către o persoană a unor materiale jurnalistice, academice, artistice sau literare, iar operatorul are convingerea rezonabilă că publicarea acestui material ar servi unui interes public. Pentru a stabili dacă o publicare ar servi unui interes public, operatorul trebuie să țină seama de importanța deosebită a interesului public în ceea ce privește libertatea de exprimare și de informare. În plus, operatorul trebuie să aibă în vedere codurile de bune practici sau orientările relevante pentru publicarea în cauză [*BBC Editorial Guidelines* (liniile directoare editoriale BBC), *Ofcom Broadcasting Code* (codul de radiodifuziune Ofcom) și *Editors' Code of Practice* (codul de bune practici al editorilor)]. De asemenea, pentru ca o derogare să se aplice, operatorul trebuie să aibă convingerea rezonabilă că respectarea dispoziției relevante ar fi incompatibilă cu scopurile speciale (punctul 26 subpunctul 3 din anexa 2 la DPA din 2018).

([64]) Hotărârea pronunțată în cauza NT1/Google [2018] EWHC 799 (QB), punctul 102, a abordat o discuție cu privire la faptul dacă operatorul de date a avut convingerea rezonabilă că publicarea servește interesului public și că respectarea dispozițiilor relevante este incompatibilă cu scopurile speciale. Instanța a precizat că secțiunea 32 punctul 1 literele (b) și (c) din Legea privind protecția datelor din 1998 are un element subiectiv și unul obiectiv: operatorul de date trebuie să demonstreze că a avut convingerea că publicarea ar servi interesului public și că această convingere este rezonabilă din punct de vedere obiectiv; acesta trebuie să demonstreze o convingere subiectivă potrivit căreia respectarea dispoziției de la care solicită derogarea ar fi incompatibilă cu scopul special în cauză.

([65]) Un exemplu al modului în care se aplică testul „convingerii rezonabile" este inclus în decizia ICO de a amenda *True Visions Productions*, care a fost adoptată în temeiul Legii privind protecția datelor din 1998. ICO a acceptat faptul că operatorul mass-media a avut convingerea subiectivă că respectarea primului principiu privind protecția datelor (echitate și legalitate) este incompatibilă cu scopurile jurnalistice. Cu toate acestea, ICO nu a acceptat faptul că această convingere a fost rezonabilă din punct de vedere obiectiv. Decizia ICO este disponibilă la următoarea adresă: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf

dispoziția în cauză reprezintă un obstacol în calea jurnalismului responsabil ([66]). Orientări privind aplicarea testului privind interesul public și asigurarea unui echilibru între interesul public și interesul unei persoane față de viața privată au fost, de asemenea, publicate de autoritatea de reglementare în domeniul telecomunicațiilor din Regatul Unit, OFCOM, și BBC în liniile sale directoare editoriale ([67]). Liniile directoare oferă în special exemple de informații care pot fi considerate a fi în interesul public și explică necesitatea de a putea demonstra că interesul public prevalează asupra drepturilor la viață privată în circumstanțele specifice ale cazului.

(71) În mod similar cu ceea ce se prevede la articolul 89 din RGPD, datele cu caracter personal prelucrate în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice pot fi, de asemenea, exceptate de la o serie de dispoziții enumerate în RGPD al Regatului Unit ([68]). În ceea ce privește cercetarea și statisticile, sunt posibile derogări de la dispozițiile RGPD al Regatului Unit referitoare la confirmarea prelucrării, accesul la date și garanții pentru transferurile către țări terțe; dreptul la rectificare; restricționarea prelucrării și opoziția la prelucrare. În ceea ce privește arhivarea în interes public, sunt, de asemenea, posibile derogări de la obligația de notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării și de la dreptul la portabilitatea datelor.

(72) În conformitate cu punctul 27 subpunctul 1 și cu punctul 28 subpunctul 1 din anexa 2 la DPA din 2018, derogările de la dispozițiile enumerate din RGPD al Regatului Unit sunt posibile în cazul în care aplicarea dispozițiilor ar „împiedica sau ar afecta în mod grav realizarea" scopurilor în cauză ([69]).

(73) Având în vedere relevanța acestora pentru exercitarea efectivă a drepturilor individuale, orice evoluție relevantă în ceea ce privește interpretarea și aplicarea în practică a derogărilor menționate anterior (în plus față de cea referitoare la menținerea unui control eficace al imigrației, astfel cum se explică în considerentul 6), inclusiv orice evoluție ulterioară a jurisprudenței, a orientărilor ICO și a măsurilor de asigurare a respectării legii, va fi luată în considerare în mod corespunzător în contextul monitorizării continue a prezentei decizii ([70]).

2.5.7. *Restricții privind transferurile ulterioare de date*

(74) Nivelul de protecție oferit datelor cu caracter personal transferate din Uniunea Europeană către operatorii sau persoanele împuternicite de operatori din Regatul Unit nu trebuie să fie subminat de transferul suplimentar al acestor date către destinatari dintr-o țară terță. Astfel de „transferuri ulterioare", care, din perspectiva operatorului sau al persoanei împuternicite de operator din Regatul Unit, constituie transferuri internaționale din Regatul Unit, ar trebui să fie permise numai în cazul în care destinatarul suplimentar din afara Regatului Unit intră el însuși sub incidența unor norme care asigură un nivel de protecție similar cu cel garantat în cadrul ordinii juridice a Regatului Unit. Din acest motiv, aplicarea normelor din RGPD al Regatului Unit și din DPA din 2018 privind transferurile internaționale de date cu caracter personal este un factor important pentru a asigura continuitatea protecției în cazul datelor cu caracter personal transferate din Uniunea Europeană către Regatul Unit în temeiul prezentei decizii.

([66]) Conform orientărilor, organizațiile trebuie să fie în măsură să explice de ce respectarea dispoziției relevante din Legea privind protecția datelor din 1998 este incompatibilă cu scopurile jurnalismului. În special, operatorii trebuie să stabilească un echilibru între efectul negativ pe care respectarea l-ar avea asupra jurnalismului și efectul negativ pe care nerespectarea l-ar avea asupra drepturilor persoanei vizate. Dacă un jurnalist își poate atinge în mod rezonabil obiectivele editoriale într-un mod care respectă dispozițiile standard ale DPA, atunci acesta trebuie să acționeze astfel. Organizațiile trebuie să fie în măsură să își justifice utilizarea restricției în ceea ce privește toate dispozițiile pe care nu le-au respectat. *Data protection and journalism: a guide for the media* („Protecția datelor și jurnalismul: ghid pentru mass-media"), disponibil la următoarea adresă: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf

([67]) Printre exemplele de interes public s-ar număra dezvăluirea sau depistarea infracțiunilor, protejarea sănătății sau a siguranței publice, expunerea afirmațiilor înșelătoare făcute de persoane sau organizații sau divulgarea incompetenței care afectează publicul. A se vedea orientările OFCOM la următoarea adresă: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf și liniile directoare editoriale ale BBC la următoarea adresă: https://www.bbc.com/editorialguidelines/guidelines/privacy

([68]) A se vedea articolul 89 din RGPD al Regatului Unit și punctul 27 subpunctul 2 și punctul 28 subpunctul 2 din partea 6 din anexa 2 la DPA din 2018.

([69]) Acest lucru este supus cerinței ca datele cu caracter personal să fie prelucrate în conformitate cu articolul 89 alineatul (1) din RGPD al Regatului Unit, astfel cum a fost completat de secțiunea 19 din DPA din 2018.

([70]) A se vedea considerentele 281-287.

(75) Regimul transferurilor internaționale de date cu caracter personal din Regatul Unit este prevăzut la articolele 44-49 din RGPD al Regatului Unit, completat de DPA din 2018, și este în esență identic cu normele prevăzute în capitolul V din Regulamentul (UE) 2016/679 ([71]). Transferurile de date cu caracter personal către o țară terță sau o organizație internațională pot avea loc numai în baza regulamentelor privind caracterul adecvat al nivelului de protecție [echivalentul din Regatul Unit al unei decizii privind caracterul adecvat al nivelului de protecție în temeiul Regulamentului (UE) 2016/679] sau, în absența unor regulamente privind caracterul adecvat al nivelului de protecție, în cazul în care operatorul sau persoana împuternicită de operator a oferit garanții adecvate în conformitate cu articolul 46 din RGPD al Regatului Unit. În absența unor regulamente privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate, un transfer poate avea loc numai pe baza derogărilor prevăzute la articolul 49 din RGPD al Regatului Unit.

(76) Regulamentele privind caracterul adecvat al nivelului de protecție adoptate de secretarul de stat pot stipula ca o țară terță (sau un teritoriu sau un sector dintr-o țară terță), o organizație internațională sau o descriere ([72]) a țării, teritoriului, sectorului sau organizației respective să asigure un nivel adecvat de protecție a datelor cu caracter personal. Atunci când evaluează caracterul adecvat al nivelului de protecție, secretarul de stat trebuie să ia în considerare aceleași elemente pe care Comisia trebuie să le evalueze în temeiul articolului 45 alineatul (2) literele (a)-(c) din Regulamentul (UE) 2016/679, interpretat împreună cu considerentul 104 din Regulamentul (UE) 2016/679 și cu jurisprudența menținută a Uniunii. Aceasta înseamnă că, atunci când se evaluează nivelul adecvat de protecție al unei țări terțe, standardul relevant va fi dacă țara terță în cauză asigură un nivel de protecție „echivalent în esență" cu cel garantat în Regatul Unit.

(77) În ceea ce privește procedura, regulamentele privind caracterul adecvat al nivelului de protecție fac obiectul cerințelor de procedură „generale" prevăzute în secțiunea 182 din DPA din 2018. În cadrul acestei proceduri, secretarul de stat trebuie să consulte comisarul pentru informații atunci când propune adoptarea unor regulamente ale Regatului Unit privind caracterul adecvat al nivelului de protecție ([73]). Odată adoptate de secretarul de stat, aceste regulamente sunt prezentate Parlamentului și fac obiectul procedurii de „rezoluție negativă", în cadrul căreia ambele camere ale Parlamentului pot examina regulamentele și pot adopta o propunere de anulare a regulamentelor în termen de 40 de zile ([74]).

(78) În conformitate cu secțiunea 17B punctul 1 din DPA din 2018, regulamentele privind caracterul adecvat al nivelului de protecție trebuie revizuite la intervale de cel mult patru ani, iar secretarul de stat trebuie să monitorizeze în permanență evoluțiile din țările terțe și la nivelul organizațiilor internaționale, care ar putea afecta deciziile de adoptare a unor regulamente privind caracterul adecvat al nivelului de protecție sau de modificare sau de revocare a unor astfel de regulamente. În cazul în care secretarul de stat constată că o țară sau o organizație specificată nu mai asigură un nivel adecvat de protecție a datelor cu caracter personal, acesta trebuie, în măsura în care este necesar, să modifice sau să revoce regulamentele și să inițieze consultări cu țara terță sau cu organizația internațională în cauză pentru a remedia lipsa unui nivel adecvat de protecție. Aceste aspecte procedurale reflectă, de asemenea, cerințele corespunzătoare din Regulamentul (UE) 2016/679.

([71]) Cu excepția articolului 48 din Regulamentul (UE) 2016/679, pe care Regatul Unit a decis să nu îl includă în RGPD al Regatului Unit. În această privință, ar trebui reamintit, în primul rând, că standardul care trebuie considerat ca oferind un nivel adecvat de protecție este mai degrabă un standard de „echivalență substanțială" decât unul de identitatea, astfel cum a fost clarificat de CJUE (*Schrems I*, punctele 73 și 74) și recunoscut de CEPD (Criterii de referință privind caracterul adecvat al nivelului de protecție, pagina 3). Prin urmare, astfel cum a explicat CEPD în criteriile sale de referință privind caracterul adecvat al nivelului de protecție, „obiectivul nu este de a reflecta punct cu punct legislația europeană, ci de a stabili cerințele esențiale ale legislației respective". În acest sens, este important de remarcat faptul că, deși ordinea juridică a Regatului Unit nu conține în mod formal o dispoziție identică cu cea de la articolul 48, același efect este garantat de alte dispoziții și principii juridice, și anume că, în urma unei cereri de date cu caracter personal din partea unei instanțe judecătorești sau a unei autorități administrative dintr-o țară terță, datele cu caracter personal pot fi transferate către țara terță respectivă numai dacă există un acord internațional în vigoare – pe baza căruia hotărârea judecătorească sau decizia administrativă a țării terțe în cauză este recunoscută sau executată în Regatul Unit – sau dacă se bazează pe unul dintre mecanismele de transfer prevăzut la capitolul V din RGPD al Regatului Unit. Mai precis, pentru a executa o hotărâre judecătorească străină, instanțele din Regatul Unit trebuie să poată invoca common law sau un statut care permite forța executorie a acesteia. Cu toate acestea, nici common law (a se vedea *Adams și alții/Cape Industries Plc.*, [1990] 2 W.L.R. 657), nici statutul nu prevăd executarea hotărârilor judecătorești străine care impun transferul de date fără un acord internațional în vigoare. În consecință, cererile de date nu sunt executorii în temeiul legislației Regatului Unit, în absența unui astfel de acord internațional. În plus, orice transfer de date cu caracter personal către țări terțe – inclusiv la cererea unei instanțe judecătorești sau a unei autorități administrative străine – face în continuare obiectul restricțiilor prevăzute la capitolul V din RGPD al Regatului Unit, care sunt identice cu dispozițiile corespunzătoare din Regulamentul (UE) 2016/679 și, prin urmare, trebuie să se bazeze pe unul dintre motivele de transfer disponibile în temeiul capitolului V, în conformitate cu condițiile specifice cărora trebuie să li se supună în temeiul capitolului respectiv.

([72]) Autoritățile Regatului Unit au explicat că descrierea unei țări sau a unei organizații internaționale se referă la o situație în care ar fi necesar să se efectueze o determinare specifică și parțială a caracterului adecvat cu restricții specifice (de exemplu, regulamente privind caracterul adecvat al nivelului de protecție în ceea ce privește numai anumite tipuri de transferuri de date).

([73]) A se vedea Memorandumul de înțelegere dintre secretarul de stat al Ministerului pentru Digitalizare, Cultură, Mass-Media și Sport și Biroul comisarului pentru informații privind rolul ICO în legătură cu noua evaluare privind caracterul adecvat al nivelului de protecție din Regatul Unit, disponibil la următoarea adresă: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments

([74]) În cazul în care se adoptă un astfel de vot, regulamentele vor înceta, în cele din urmă, să mai producă efecte juridice.

(79) În absența unor regulamente privind caracterul adecvat al nivelului de protecție, transferurile internaționale pot avea loc în cazul în care operatorul sau persoana împuternicită de operator a oferit garanții adecvate în conformitate cu articolul 46 din RGPD al Regatului Unit. Aceste garanții sunt similare celor prevăzute la articolul 46 din Regulamentul (UE) 2016/679. Garanțiile includ instrumente obligatorii din punct de vedere juridic și executorii între autoritățile sau organismele publice, reguli corporatiste obligatorii ([75]), clauze standard de protecție a datelor, coduri de conduită aprobate, mecanisme de certificare aprobate și cu autorizarea comisarului pentru informații, clauze contractuale între operatori (sau persoane împuternicite de operatori) sau acorduri administrative între autoritățile publice. Cu toate acestea, normele au fost modificate, din punct de vedere procedural, pentru a funcționa în cadrul Regatului Unit, în special clauzele standard de protecție a datelor pot fi adoptate de secretarul de stat (secțiunea 17C) sau de comisarul pentru informații (secțiunea 119A) în conformitate cu DPA din 2018.

(80) În absența unei decizii privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate, un transfer poate avea loc numai pe baza derogărilor prevăzute la articolul 49 din RGPD al Regatului Unit ([76]). RGPD al Regatului Unit nu introduce nicio modificare semnificativă a derogărilor în comparație cu normele corespunzătoare din Regulamentul (UE) 2016/679. În temeiul RGPD al Regatului Unit, la fel ca în cazul Regulamentului (UE) 2016/679, anumite derogări pot fi invocate numai dacă transferul este ocazional ([77]). În plus, în orientările sale privind transferurile internaționale, ICO clarifică următoarele aspecte: „Ar trebui să le utilizați doar ca «excepții» reale de la regula generală conform căreia nu ar trebui să efectuați un transfer restricționat decât dacă acesta face obiectul unei decizii privind caracterul adecvat al nivelului de protecție sau dacă există garanții adecvate în vigoare” ([78]). În ceea ce privește transferurile care sunt necesare din motive importante de interes public [articolul 49 alineatul (1) litera (d)], secretarul de stat poate adopta regulamente pentru a preciza circumstanțele în care un transfer de date cu caracter personal către o țară terță sau o organizație internațională nu este necesar din motive importante de interes public. În plus, secretarul de stat poate, prin regulamente, să restricționeze transferul unei categorii de date cu caracter personal către o țară terță sau către o organizație internațională în cazul în care transferul nu poate avea loc pe baza unor regulamente privind caracterul adecvat al nivelului de protecție, iar secretarul de stat consideră că restricția este necesară din motive importante de interes public. Până în prezent nu au fost adoptate astfel de regulamente.

(81) Acest cadru pentru transferurile internaționale a devenit aplicabil la sfârșitul perioadei de tranziție ([79]). Cu toate acestea, punctul 4 din anexa 21 la DPA din 2018 (introdus prin regulamentele DPPEC) prevede că, la sfârșitul perioadei de tranziție, anumite transferuri de date cu caracter personal sunt tratate ca și cum s-ar baza pe regulamente privind caracterul adecvat al nivelului de protecție. Aceste transferuri includ transferurile către un stat SEE, teritoriul Gibraltarului, o instituție, un organism, un oficiu sau o agenție a(l) Uniunii înființat(ă) prin Tratatul UE sau în temeiul acestuia, precum și către țări terțe care au făcut obiectul unei decizii a UE privind

([75]) RGPD al Regatului Unit menține normele de la articolul 47 din Regulamentul (UE) 2016/679, sub rezerva doar a unor modificări pentru încadrarea normelor în contextul intern, de exemplu prin înlocuirea trimiterilor la autoritatea de supraveghere competentă cu trimiteri la comisarul pentru informații, eliminarea trimiterii la mecanismul pentru asigurarea coerenței de la alineatul (1) și eliminarea întregului alineat (3).

([76]) În temeiul articolului 49 din RGPD al Regatului Unit, transferurile sunt posibile dacă este îndeplinită una dintre următoarele condiții: (a) persoana vizată și-a exprimat în mod explicit acordul cu privire la transferul propus, după ce a fost informată asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru persoana vizată ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protecție și a unor garanții adecvate; (b) transferul este necesar pentru executarea unui contract între persoana vizată și operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate; (c) transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică; (d) transferul este necesar din considerente importante de interes public; (e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță; (f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul; (g) transferul se realizează dintr-un registru care, potrivit dreptului intern, are scopul de a furniza informații publicului și care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în măsura în care sunt îndeplinite condițiile cu privire la consultare prevăzute de dreptul intern în acel caz specific. În plus, în cazul în care niciuna dintre condițiile de mai sus nu este aplicabilă, un transfer poate avea loc numai dacă nu este repetitiv, se referă doar la un număr limitat de persoane vizate, este necesar în scopul realizării intereselor legitime majore urmărite de operator asupra căruia nu prevalează interesele sau drepturile și libertățile persoanei vizate și operatorul a evaluat toate circumstanțele aferente transferului de date și, pe baza acestei evaluări, a prezentat garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal.

([77]) Considerentul 111 din RGPD al Regatului Unit precizează că transferurile în legătură cu un contract sau cu o acțiune în justiție pot avea loc numai în cazul în care sunt ocazionale.

([78]) Orientările ICO privind transferurile internaționale, disponibile la următoarea adresă: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7

([79]) În cursul unei perioade de maximum șase luni care se încheie cel târziu la 30 iunie 2021, aplicabilitatea acestui nou cadru trebuie interpretată în lumina articolului 782 din Acordul comercial și de cooperare între Uniunea Europeană și Comunitatea Europeană a Energiei Atomice, pe de o parte, și Regatul Unit al Marii Britanii și Irlandei de Nord, pe de altă parte (L 444/14 din 31.12.2020) („TCA UE-UK”), disponibil la următoarea adresă: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:22020A1231(01)&from=RO

caracterul adecvat al nivelului de protecție la încheierea perioadei de tranziție. În consecință, transferurile către aceste țări pot continua la fel ca înainte de retragerea Regatului Unit din UE. După încheierea perioadei de tranziție, secretarul de stat trebuie să efectueze o revizuire a acestor constatări privind caracterul adecvat al nivelului de protecție pe o perioadă de patru ani, și anume până la sfârșitul lunii decembrie 2024. Potrivit explicației furnizate de autoritățile Regatului Unit, deși secretarul de stat trebuie să efectueze o astfel de revizuire până la sfârșitul lunii decembrie 2024, dispozițiile tranzitorii nu includ o dispoziție de caducitate, iar dispozițiile tranzitorii relevante nu vor înceta în mod automat să producă efecte dacă revizuirea nu este finalizată până la sfârșitul lunii decembrie 2024.

(82) În cele din urmă, în ceea ce privește evoluția viitoare a regimului transferurilor internaționale al Regatului Unit – prin adoptarea unor noi regulamente privind caracterul adecvat al nivelului de protecție, încheierea de acorduri internaționale sau dezvoltarea altor mecanisme de transfer – Comisia va monitoriza îndeaproape situația, va evalua dacă diferitele mecanisme de transfer sunt utilizate într-un mod care să asigure continuitatea protecției și, dacă este necesar, va lua măsurile adecvate pentru a aborda posibilele efecte negative asupra acestei continuități (a se vedea considerentele 278-287). Întrucât UE și Regatul Unit au norme similare privind transferurile internaționale, se preconizează că divergențele problematice ar putea fi, de asemenea, evitate prin cooperare, schimb de informații și schimb de experiență, inclusiv între ICO și CEPD.

2.5.8. *Responsabilitate*

(83) Conform principiului responsabilității, entităților care prelucrează date li se solicită să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a-și respecta în mod efectiv obligațiile în materie de protecție a datelor și pentru a putea demonstra această conformitate, în special autorității de supraveghere competente.

(84) Principiul responsabilității prevăzut în Regulamentul (UE) 2016/679 a fost menținut la articolul 5 alineatul (2) din RGPD al Regatului Unit fără modificări substanțiale și același lucru se aplică articolului 24 privind responsabilitatea operatorului, articolului 25 privind protecția datelor începând cu momentul conceperii și în mod implicit și articolului 30 privind evidențele activităților de prelucrare. Articolele 35 și 36 privind evaluarea impactului asupra protecției datelor și consultarea prealabilă a autorității de supraveghere au fost, de asemenea, menținute. Articolele 37-39 din Regulamentul (UE) 2016/679 privind desemnarea și sarcinile responsabililor cu protecția datelor au fost menținute în RGPD al Regatului Unit fără modificări semnificative. În plus, dispozițiile articolelor 40 și 42 din Regulamentul (UE) 2016/679 privind codurile de conduită și certificarea au fost menținute în RGPD al Regatului Unit ([80]).

2.6. **Supraveghere și asigurarea respectării normelor**

2.6.1. *Supravegherea independentă*

(85) Pentru a garanta în practică un nivel adecvat de protecție a datelor, ar trebui instituită o autoritate de supraveghere independentă care să aibă competența de a monitoriza și de a asigura respectarea normelor de protecție a datelor. Această autoritate ar trebui să acționeze cu deplină independență și imparțialitate în îndeplinirea sarcinilor sale și în exercitarea competențelor sale.

(86) În Regatul Unit, supravegherea și asigurarea respectării RGPD al Regatului Unit și a DPA din 2018 sunt efectuate de comisarul pentru informații. Comisarul pentru informații este o „întreprindere individuală” (Corporation Sole): o entitate juridică separată constituită dintr-o singură persoană. Comisarul pentru informații este sprijinit în activitatea sa de un birou. La 31 martie 2020, Biroul comisarului pentru informații avea 768 de angajați permanenți ([81]). Ministerul finanțator al comisarului pentru informații este Ministerul pentru Digitalizare, Cultură, Mass-Media și Sport ([82]).

(87) Independența comisarului este stabilită în mod explicit la articolul 52 din RGPD al Regatului Unit, care nu aduce nicio modificare de fond articolului 52 alineatele (1)-(3) din RGPD. Comisarul trebuie să beneficieze de independență deplină în îndeplinirea sarcinilor sale și exercitarea competențelor sale în conformitate cu RGPD al Regatului Unit, să rămână independent de orice influență externă directă sau indirectă în legătură cu aceste sarcini și

([80]) Dacă este necesar, aceste trimiteri se înlocuiesc cu trimiteri la autoritățile din Regatul Unit. De exemplu, în temeiul secțiunii 17 din DPA din 2018, comisarul pentru informații sau organismul național de acreditare din Regatul Unit poate acredita o persoană care îndeplinește cerințele prevăzute la articolul 43 din RGPD al Regatului Unit pentru a monitoriza conformitatea cu o certificare.

([81]) Raportul anual și situațiile financiare pe 2019-2020 ale comisarului pentru informații, disponibile la următoarea adresă: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf

([82]) Un acord de gestionare reglementează relația dintre cele două entități. Responsabilitățile principale ale DCMS, în calitate de minister finanțator, includ în special: asigurarea faptului că comisarul pentru informații dispune de finanțare și resurse adecvate; reprezentarea intereselor comisarului pentru informații în fața Parlamentului și a altor departamente guvernamentale; asigurarea existenței unui cadru național solid de protecție a datelor; și furnizarea de orientări și sprijin Biroului comisarului pentru informații cu privire la aspecte legate de întreprinderi, cum ar fi aspecte imobiliare, contracte de leasing și achiziții publice (Acordul de gestionare 2018-2021, disponibil la următoarea adresă: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

competențe și să nu solicite, nici să nu accepte instrucțiuni de la o parte externă. De asemenea, comisarul trebuie să se abțină de la a întreprinde acțiuni incompatibile cu atribuțiile sale, iar pe durata mandatului, nu desfășoară activități incompatibile, remunerate sau nu.

(88) Condițiile pentru numirea și revocarea comisarului pentru informații sunt prevăzute în anexa 12 la DPA din 2018. Comisarul pentru informații este numit de Majestatea Sa la recomandarea Guvernului, în urma unui concurs general echitabil. Candidatul trebuie să dețină calificările, aptitudinile și competențele corespunzătoare. În conformitate cu Codul de guvernanță privind numirile publice ([83]), o listă de candidați care pot fi numiți este întocmită de un comitet consultativ de evaluare. Înainte ca secretarul de stat din cadrul Ministerului pentru Digitalizare, Cultură, Mass-Media și Sport să ia o decizie finală, comisia specială competentă din cadrul Parlamentului trebuie să efectueze un control prealabil numirii. Poziția Comitetului este făcută publică ([84]).

(89) Comisarul pentru informații are un mandat de până la șapte ani. O persoană nu poate fi numită în calitate de comisar pentru informații de mai multe ori. Comisarul pentru informații poate fi revocat din funcție de Majestatea Sa în urma unei propuneri („address") formulate de ambele camere ale Parlamentului ([85]). Nicio cerere de revocare a comisarului pentru informații nu poate fi prezentată nici unei camere a Parlamentului decât în cazul în care un ministru a prezentat un raport în care afirmă că este convins că comisarul pentru informații este vinovat de comiterea unei abateri grave și/sau comisarul nu mai îndeplinește condițiile necesare pentru exercitarea funcțiilor sale ([86]).

(90) Finanțarea comisarului pentru informații provine din trei surse: (i) taxele pentru protecția datelor plătite de operatori, care sunt stabilite prin regulamentele secretarului de stat ([87]) [Regulamentele din 2018 privind protecția datelor (taxe și informații)] și se ridică la 85-90 % din bugetul anual al Biroului ([88]); (ii) grant sub formă de ajutor plătit de Guvern comisarului pentru informații. Grantul sub formă de ajutor este utilizat în principal pentru finanțarea cheltuielilor de funcționare ale comisarului pentru informații în ceea ce privește sarcinile care nu au legătură cu protecția datelor ([89]) și (iii) taxele percepute pentru servicii ([90]). În prezent, nu se percep astfel de taxe.

(91) Funcțiile generale ale comisarului pentru informații în ceea ce privește prelucrarea datelor cu caracter personal cărora li se aplică RGPD al Regatului Unit sunt prevăzute la articolul 57 din RGPD al Regatului Unit, reflectând îndeaproape normele corespunzătoare din Regulamentul (UE) 2016/679. Printre funcțiile sale se numără monitorizarea și asigurarea respectării RGPD al Regatului Unit, promovarea acțiunilor de sensibilizare în rândul publicului, tratarea plângerilor depuse de persoanele vizate, desfășurarea de investigații etc. În plus, secțiunea 115 din DPA din 2018 stabilește alte funcții generale ale comisarului, printre care se numără obligația de a oferi consiliere Parlamentului, Guvernului și altor instituții și organisme cu privire la măsurile legislative și administrative referitoare la protecția drepturilor și libertăților persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, precum și competența de a emite, din proprie inițiativă sau la cerere, avize adresate Parlamentului, guvernului sau altor instituții și organisme, precum și publicului cu privire la orice aspect legat de protecția datelor cu caracter personal. Pentru a menține independența sistemului judiciar, comisarul pentru informații nu este

([83]) Codul de guvernanță privind numirile publice, disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf

([84]) Al doilea raport al sesiunii 2015-2016 a Comisiei pentru cultură, mass-media și sport a Camerei Comunelor, disponibil la următoarea adresă: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf

([85]) „Address" este o propunere prezentată Parlamentului prin care se urmărește informarea monarhului cu privire la opiniile Parlamentului referitoare la o anumită chestiune.

([86]) Punctul 3 subpunctul (3) din anexa 12 la DPA din 2018.

([87]) Secțiunea 137 din DPA din 2018, a se vedea considerentul 17.

([88]) Secțiunile 137 și 138 din DPA din 2018 conțin o serie de garanții pentru a se asigura că taxele sunt stabilite la un nivel corespunzător. În special secțiunea 137 punctul 4 enumeră aspectele pe care secretarul de stat trebuie să le ia în considerare atunci când elaborează regulamente care precizează suma pe care trebuie să o plătească diferitele organizații; În al doilea rând, secțiunea 138 punctul 1 și secțiunea 182 din DPA din 2018 conțin de asemenea o cerință legală potrivit căreia secretarul de stat trebuie să se consulte cu comisarul pentru informații și cu alți reprezentanți ai persoanelor care pot fi afectate de regulamentele în cauză, înainte ca acestea să fie adoptate, astfel încât opiniile lor să poată fi luate în considerare. În plus, în temeiul secțiunii 138 punctul 2 din DPA din 2018, comisarul pentru informații are obligația de a monitoriza funcționarea regulamentelor privind taxele și poate prezenta secretarului de stat propuneri de modificare a regulamentelor. În cele din urmă, cu excepția cazului în care regulamentele sunt adoptate doar pentru a lua în considerare o creștere a indicelui prețurilor cu amănuntul (caz în care vor face obiectul procedurii de rezoluție negativă), regulamentele fac obiectul procedurii de rezoluție afirmativă și nu pot fi adoptate decât după ce au fost aprobate prin rezoluția fiecărei camere a Parlamentului.

([89]) Acordul de gestionare a clarificat următoarele: „Secretarul de stat poate efectua plăți către CI din banii furnizați de Parlament în temeiul punctului 9 din anexa 12 la DPA din 2018. După consultarea CI, DCMS va plăti către CI sumele corespunzătoare (grantul sub formă de ajutor) pentru costurile administrative ale ICO și pentru exercitarea funcțiilor CI în legătură cu o serie de funcții specifice, inclusiv libertatea de informare" (Acordul de gestiune 2018-2021, punctul 1.12, a se vedea nota de subsol 82).

([90]) A se vedea secțiunea 134 din DPA din 2018.

autorizat să își exercite funcțiile în legătură cu prelucrarea datelor cu caracter personal de către o persoană care acționează în exercițiul unei funcții judiciare sau de către o instanță sau tribunal care acționează în exercițiul funcției sale judiciare. Cu toate acestea, supravegherea sistemului judiciar este asigurată de organisme specializate (a se vedea considerentele 99-103).

2.6.2. *Asigurarea respectării normelor, inclusiv sancțiuni*

(92) Competențele comisarului pentru informații sunt prevăzute la articolul 58 din RGPD al Regatului Unit, care nu introduce nicio modificare substanțială a articolului corespunzător din Regulamentul (UE) 2016/679. DPA din 2018 stabilește norme suplimentare privind modul în care pot fi exercitate aceste competențe. În special, comisarul are competența de: (a) a ordona operatorului și persoanei împuternicite de operator (și, în anumite circumstanțe, oricărei alte persoane) să furnizeze informațiile necesare prin transmiterea unei notificări de informare („notificare de informare") ([91]); (b) a efectua investigații și audituri prin transmiterea unei notificări de evaluare, care poate impune operatorului sau persoanei împuternicite de operator să permită comisarului să intre în incinte specificate, să inspecteze sau să examineze documente sau echipamente, să intervieveze persoane care prelucrează date cu caracter personal în numele operatorului etc. („notificare de evaluare") ([92]); (c) a obține în alt mod acces la documente etc. ale operatorilor și ale persoanelor împuternicite de operatori și acces la sediile acestora în conformitate cu secțiunea 154 din DPA din 2018 („competențe de intrare și de inspecție"); (d) a exercita competențe corective, inclusiv prin avertismente și mustrări sau a emite ordine prin intermediul unei notificări de executare, care impune operatorilor/persoanelor împuternicite de operatori să întreprindă sau să se abțină de la a întreprinde anumite măsuri, inclusiv obligarea operatorului sau a persoanei împuternicite de operator să întreprindă orice acțiune prevăzută la articolul 58 alineatul (2) literele (c)-(g) și (j) din RGPD al Regatului Unit („notificare de executare") ([93]); (e) și a emite amenzi administrative sub forma unei notificări de sancționare („notificare de sancționare") ([94]). Aceasta din urmă poate fi emisă și în cazul în care o autoritate publică nu a respectat dispozițiile RGPD al Regatului Unit ([95]).

(93) Politica ICO privind acțiunile de reglementare stabilește circumstanțele în care acesta va emite o notificare de informare, de evaluare, de executare sau de sancționare ([96]). O notificare de executare transmisă ca răspuns la o neîndeplinire a obligațiilor de către un operator sau o persoană împuternicită de operator poate impune numai cerințele pe care comisarul le consideră adecvate în scopul remedierii neîndeplinirii obligațiilor. Notificarea de executare și cea de sancționare pot fi emise unui operator sau unei persoane împuternicite de operator în legătură cu încălcări ale capitolului II din RGPD al Regatului Unit (principiile prelucrării), ale articolelor 12-22 (drepturile persoanei vizate), ale articolelor 25-39 (obligațiile operatorilor și ale persoanelor împuternicite de operatori) și ale articolelor 44-49 (transferurile internaționale) din RGPD al Regatului Unit. De asemenea, se poate emite o notificare de executare în cazul în care un operator nu a respectat cerința de a plăti o taxă prevăzută în reglementările adoptate în temeiul articolului 137 din DPA din 2018. În plus, un organism de monitorizare prevăzut la articolul 41 sau un furnizor de certificare poate primi o notificare de executare în cazul în care nu își respectă obligațiile care îi revin în temeiul RGPD al Regatului Unit. O notificare de sancționare poate fi transmisă, de asemenea, unei persoane care nu a respectat o notificare de informare, o notificare de evaluare sau o notificare de executare.

(94) Notificarea de sancționare impune persoanei în cauză să plătească Comisarului pentru informații o sumă specificată în notificare. Pentru a decide dacă să transmită o notificare de sancționare unei persoane și pentru a stabili cuantumul sancțiunii, comisarul pentru informații trebuie să aibă în vedere aspectele enumerate la articolul 83 alineatele (1) și (2) din RGPD al Regatului Unit, care sunt identice cu normele corespunzătoare din Regulamentul (UE) 2016/679 ([97]). În conformitate cu articolul 83 alineatele (4) și (5), cuantumurile maxime ale amenzilor administrative în cazul nerespectării obligațiilor menționate în aceste dispoziții sunt de 8 700 000 GBP sau, respectiv, 17 500 000 GBP. În cazul unei întreprinderi, comisarul pentru informații poate, de asemenea, să impună

([91]) Secțiunea 142 din DPA din 2018 (sub rezerva restricțiilor prevăzute în secțiunea 143 din DPA din 2018).

([92]) Secțiunea 146 din DPA din 2018 (sub rezerva restricțiilor prevăzute în secțiunea 147 din DPA din 2018).

([93]) Secțiunile 149-151 din DPA din 2018 (sub rezerva restricțiilor prevăzute în secțiunea 152 din DPA din 2018).

([94]) Secțiunea 155 din DPA din 2018 și articolul 83 din RGPD al Regatului Unit.

([95]) Acest lucru rezultă din articolul 155 alineatul (1) din DPA din 2018 coroborat cu secțiunea 149 punctele 2 și 5 din DPA din 2018 și din secțiunea 156 punctul 4 din DPA din 2018, care restricționează emiterea de notificări de sancționare numai în ceea ce privește comisarii patrimoniului Coroanei (Crown Estate Commissioners) și controlorii casei regale (controllers for the Royal Household) în temeiul secțiunii 209 punctul 4 din DPA din 2018.

([96]) Politica privind acțiunile de reglementare, disponibilă la următoarea adresă: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf0

([97]) Inclusiv natura și gravitatea încălcării (ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea), dacă încălcarea a fost comisă intenționat sau din neglijență, orice acțiuni întreprinse de operator pentru a reduce prejudiciile suferite de persoanele vizate, gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator (ținându-se seama de măsurile tehnice și organizatorice puse în aplicare de operator sau de persoana împuternicită de operator), eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator; gradul de cooperare cu comisarul, categoriile de date cu caracter personal afectate de neîndeplinire, orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

amenzi ca procent din cifra de afaceri mondială anuală, dacă are valoare mai mare. La fel ca în dispozițiile echivalente din Regulamentul (UE) 2016/679, aceste sume sunt stabilite la 2 % și, respectiv, 4 % la articolul 83 alineatele (4) și (5). În cazul nerespectării unei notificări de informare, a unei notificări de evaluare sau a unei notificări de executare, cuantumul maxim al sancțiunii care poate fi impusă printr-o notificare de sancționare este valoarea mai mare dintre 17 500 000 GBP sau, în cazul unei întreprinderi, 4 % din cifra de afaceri mondială anuală.

(95) RGPD al Regatului Unit, împreună cu DPA din 2018, au consolidat și alte competențe ale comisarului pentru informații. De exemplu, în prezent, comisarul poate efectua audituri obligatorii cu privire la toți operatorii și persoanele împuternicite de operatori prin utilizarea notificărilor de evaluare, în timp ce, în temeiul legislației anterioare, Legea privind protecția datelor din 1998, comisarul avea această competență doar în ceea ce privește administrația centrală și organizațiile din domeniul sănătății, fiind necesar ca alte entități să își dea acordul cu privire la efectuarea unui audit.

(96) De la introducerea Regulamentului (UE) 2016/679, ICO tratează anual aproximativ 40 000 de plângeri din partea persoanelor vizate ([98]) și, în plus, efectuează aproximativ 2 000 de investigații din oficiu ([99]). Majoritatea plângerilor se referă la drepturile de acces la date și de divulgare a acestora. În urma investigațiilor efectuate, comisarul ia măsuri de aplicare a legii într-o gamă largă de sectoare. Mai precis, în conformitate cu cel mai recent raport anual al comisarului pentru informații (2019-2020) ([100]), acesta a emis 54 de notificări de informare, 8 notificări de evaluare, 7 notificări de executare, 4 avertismente, 8 urmăriri penale și 15 amenzi în cursul perioadei de raportare ([101]).

(97) Printre acestea se numără mai multe sancțiuni financiare semnificative impuse în temeiul Regulamentului (UE) 2016/679 și al DPA din 2018. În special, în octombrie 2020, comisarul pentru informații a amendat o companie aeriană britanică cu 20 de milioane GBP pentru o încălcare a securității datelor care afectează peste 400 000 de clienți. La sfârșitul lunii octombrie 2020, un lanț hotelier internațional a fost amendat cu 18,4 milioane GBP pentru că nu a păstrat securitatea datelor cu caracter personal ale milioane de clienți, iar în noiembrie 2020 un furnizor britanic de servicii care vinde bilete pentru evenimente online a fost amendat cu 1,25 milioane GBP pentru că nu a protejat detaliile de plată ale clienților ([102]).

(98) Pe lângă competențele comisarului pentru informații în materie de asigurare a respectării aplicării descrise în considerentul 92, anumite încălcări ale legislației privind protecția datelor constituie infracțiuni și, prin urmare, pot face obiectul unor sancțiuni penale (secțiunea 196 din DPA din 2018). Acest lucru este valabil, de exemplu, pentru obținerea sau divulgarea în cunoștință de cauză sau din neglijență a datelor cu caracter personal fără consimțământul operatorului, cauzarea divulgării de date cu caracter personal unei alte persoane fără consimțământul operatorului ([103]), reidentificarea informațiilor care sunt date cu caracter personal anonimizate fără consimțământul operatorului responsabil de anonimizarea datelor cu caracter personal ([104]), obstrucționarea intenționată a competenței comisarului de a-și exercita competențele în ceea ce privește examinarea datelor cu caracter personal în conformitate cu obligațiile internaționale ([105]), prezentarea de declarații false ca răspuns la o notificare de informare sau distrugerea informațiilor în legătură cu notificările de informare și de evaluare ([106]).

([98]) Potrivit informațiilor furnizate de autoritățile din Regatul Unit, în perioada acoperită de Raportul anual pe 2019-2020 al comisarului pentru informații, nu s-a constatat nicio încălcare în aproximativ 25 % din cazuri, în aproximativ 29 % din cazuri persoana vizată fie a fost invitată să își exprime preocuparea față de operatorul de date pentru prima dată, să aștepte răspunsul operatorului, fie să continue dialogul în curs cu operatorul de date, în aproximativ 17 % din cazuri nu s-a constatat nicio încălcare, dar s-a furnizat consiliere operatorului de date, în aproximativ 25 % din cazuri comisarul pentru informații a constatat o încălcare și fie a furnizat consiliere operatorului de date, fie operatorului de date i s-a solicitat să întreprindă anumite acțiuni, în aproximativ 3 % din cazuri s-a stabilit că plângerea nu intră sub incidența Regulamentului (UE) 2016/679, iar aproximativ 1 % din cazuri au fost trimise unei alte autorități pentru protecția datelor în cadrul Comitetului european pentru protecția datelor.

([99]) ICO poate iniția aceste investigații pe baza informațiilor primite din diverse surse, inclusiv notificări privind încălcarea securității datelor cu caracter personal, sesizări din partea altor autorități publice ale Regatului Unit sau de la autorități străine pentru protecția datelor, precum și plângeri primite de la persoane sau organizații ale societății civile.

([100]) Raportul anual și Situațiile financiare pe 2019-2020 ale comisarului pentru informații (a se vedea nota de subsol 81).

([101]) Conform raportului anual anterior referitor la perioada 2018-2019, comisarul pentru informații a emis 22 de notificări de sancționare în temeiul DPA din 1998 în cursul perioadei de raportare, cu amenzi în valoare totală de 3 010 610 GBP, inclusiv două amenzi în valoare de 500 000 GBP (limita maximă permisă în temeiul DPA din 1998). În 2018, comisarul pentru informații a efectuat, în special, o investigație privind utilizarea analizei datelor în scopuri politice în urma dezvăluirilor Cambridge Analytica. Investigația a avut ca rezultat un raport referitor la politici, un set de recomandări, o amendă de 500 000 GBP aplicată Facebook și o notificare de executare adresată Aggregate IQ, un broker de date din Canada, prin care societății i se solicita să șteargă datele cu caracter personal pe care le deținea cu privire la cetățenii și rezidenții Regatului Unit (a se vedea Raportul anual și Situațiile financiare pe 2018-2019 ale comisarului pentru informații, disponibile la următoarea adresă: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf).

([102]) Pentru un rezumat al acțiunilor de aplicare a legii care au fost întreprinse, a se vedea site-ul web al ICO, disponibil la următoarea adresă: https://ico.org.uk/action-weve-taken/enforcement

([103]) Secțiunea 170 din DPA din 2018.

([104]) Secțiunea 171 din DPA din 2018.

([105]) Secțiunea 119 din DPA din 2018.

([106]) Secțiunile 144 și 148 din DPA din 2018.

2.6.3. *Supravegherea sistemului judiciar*

(99) Supravegherea prelucrării datelor cu caracter personal de către instanțe și sistemul judiciar este dublă. În cazul în care un titular al unei funcții judiciare sau o instanță nu acționează în exercițiul unei funcții judiciare, supravegherea este asigurată de ICO. În cazul în care operatorul își desfășoară activitatea în exercițiul unei funcții judiciare, ICO nu își poate exercita funcțiile de supraveghere ([107]), iar supravegherea este efectuată de organisme speciale. Aceasta reflectă abordarea adoptată în Regulamentul (UE) 2016/679 [articolul 55 alineatul (3)].

(100) În special, în cel de al doilea scenariu, pentru instanțele din Anglia și Țara Galilor, precum și pentru Tribunalul de Primă Instanță și Tribunalul Superior din Anglia și Țara Galilor, această supraveghere este asigurată de Grupul pentru protecția datelor judiciare ([108]). În plus, președintele Curții Supreme (Lord Chief Justice) și președintele sistemului de tribunale (Senior President of Tribunals) au emis o declarație de confidențialitate ([109]) care stabilește modul în care instanțele din Anglia și Țara Galilor prelucrează datele cu caracter personal pentru o funcție judiciară. O declarație similară a fost emisă de autoritățile judiciare din Irlanda de Nord ([110]) și de cele din Scoția ([111]).

(101) În plus, în Irlanda de Nord, președintele Curții Supreme din Irlanda de Nord a numit un judecător din cadrul Înaltei Curți în calitate de judecător în materie de supraveghere a datelor (DSJ – Data Supervisory Judge) ([112]). Aceștia au emis, de asemenea, orientări pentru sistemul judiciar din Irlanda de Nord cu privire la acțiunile care trebuie întreprinse în cazul unei pierderi sau potențiale pierderi de date și la procesul de abordare a oricăror probleme care decurg din acest fapt ([113]).

(102) În Scoția, președintele Curții Supreme (Lord President) a numit un judecător în materie de supraveghere a datelor pentru a investiga orice plângeri pe motive de protecție a datelor. Acest fapt este prevăzut în normele privind plângerile judiciare, care le reflectă pe cele stabilite pentru Anglia și Țara Galilor ([114]).

(103) În cele din urmă, în cadrul Curții Supreme, unul dintre judecătorii Curții Supreme este desemnat să supravegheze protecția datelor.

2.6.4. *Căi de atac*

(104) Pentru a asigura o protecție adecvată și, în special, asigurarea respectării drepturilor individuale, persoanei vizate ar trebui să i se ofere căi de atac administrative și judiciare eficace, inclusiv despăgubiri pentru prejudiciile suferite.

([107]) Secțiunea 117 din DPA din 2018.

([108]) Grupul este responsabil de furnizarea de orientări și formare pentru sistemul judiciar. Acesta tratează, de asemenea, plângerile persoanelor vizate cu privire la prelucrarea datelor cu caracter personal de către instanțe, tribunale și persoane care acționează în exercițiul unei funcții judiciare. Grupul urmărește să ofere mijloacele prin care orice plângere ar putea fi soluționată. În cazul în care un reclamant nu a fost mulțumit de o decizie a grupului și a furnizat dovezi suplimentare, grupul ar putea să își reexamineze decizia. Deși grupul în sine nu impune sancțiuni financiare, în cazul în care grupul consideră că există o încălcare suficient de gravă a DPA din 2018, acesta o poate adresa Biroului de investigare a conduitei judiciare (JCIO – *Judicial Conduct Investigation Office*), care va investiga plângerea. În cazul în care plângerea este admisă, este de competența Lordului Cancelar (Lord Chancellor) și a președintelui Curții Supreme (sau a unui judecător de rang înalt delegat să acționeze în numele său) să decidă ce măsuri ar trebui luate împotriva titularului funcției. Acestea ar putea include, în ordinea gravității: recomandare formală, avertisment formal, mustrare și, în cele din urmă, revocare din funcție. În cazul în care o persoană este nemulțumită de modul în care JCIO a investigat plângerea, aceasta poate depune o plângere mai departe la Ombudsmanul pentru numiri și conduită judiciară (*Judicial Appointments and Conduct Ombudsman*) (a se vedea https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Ombudsmanul are competența de a solicita JCIO să investigheze din nou o plângere și poate propune ca reclamantului să i se plătească despăgubiri în cazul în care consideră că a suferit prejudicii ca urmare a administrării defectuoase.

([109]) Declarația de confidențialitate a președintelui Curții Supreme și a președintelui sistemului de tribunale este disponibilă la următoarea adresă: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([110]) Declarația de confidențialitate emisă de președintele Curții Supreme din Irlanda de Nord este disponibilă la următoarea adresă: https://judiciaryni.uk/data-privacy

([111]) Declarația de confidențialitate pentru instanțele și tribunalele din Scoția este disponibilă la următoarea adresă: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([112]) DSJ furnizează îndrumări sistemului judiciar și investighează încălcările și/sau plângerile referitoare la prelucrarea datelor cu caracter personal de către instanțe sau persoane care acționează în exercițiul unei funcții judiciare.

([113]) În cazul în care plângerea sau încălcarea este considerată gravă, aceasta este înaintată responsabilului cu tratarea plângerilor judiciare (Judicial Complaints Officer) pentru investigații suplimentare în conformitate cu Codul de bune practici în materie de plângeri al președintelui Curții Supreme din Irlanda de Nord. Rezultatul unei astfel de plângeri ar putea include următoarele: clasarea plângerii, recomandare, formare sau mentorat, avertisment informal, avertisment formal, avertisment final, restricții de practică sau sesizarea unui tribunal statutar. Codul de bune practici în materie de plângeri emis de președintele Curții Supreme din Irlanda de Nord este disponibil la următoarea adresă: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf

([114]) Orice plângere întemeiată este investigată de judecătorul în materie de supraveghere a datelor și înaintată președintelui Curții Supreme care are competența de a emite o recomandare, un avertisment formal sau o mustrare în cazul în care consideră că este necesar (există norme echivalente pentru membrii tribunalului, disponibile la următoarea adresă: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

(105) În primul rând, o persoană vizată are dreptul de a depune o plângere la comisarul pentru informații, în cazul în care consideră că, în ceea ce privește datele cu caracter personal care o vizează, există o încălcare a RGPD al Regatului Unit ([115]). RGPD al Regatului Unit menține normele prevăzute la articolul 77 din Regulamentul (UE) 2016/679 cu privire la acest drept, fără modificări substanțiale. Același lucru este valabil și pentru articolul 57 alineatul (1) litera (f) și alineatul (2), care stabilesc sarcinile comisarului în ceea ce privește tratarea plângerilor. Astfel cum se descrie în considerentele 92-98, comisarul pentru informații are competența de a evalua respectarea de către operator și persoana împuternicită de operator a RGPD al Regatului Unit și a DPA din 2018, de a le impune să întreprindă sau să se abțină de la a întreprinde măsurile necesare în caz de nerespectare și de a aplica amenzi.

(106) În al doilea rând, RGPD al Regatului Unit și DPA din 2018 prevăd dreptul la o cale de atac împotriva comisarului pentru informații. În temeiul articolului 78 alineatul (1) din RGPD al Regatului Unit, o persoană are dreptul de a exercita o cale de atac judiciară eficientă împotriva unei decizii obligatorii din punct de vedere juridic a comisarului care o vizează. În contextul controlului jurisdicțional, judecătorul examinează decizia contestată în cerere și analizează dacă acțiunile comisarului pentru informații au fost legale. În plus, în temeiul articolului 78 alineatul (2) din RGPD al Regatului Unit, în cazul în care comisarul nu tratează în mod corespunzător o plângere depusă de persoana vizată, ([116]) reclamantul are acces la o cale de atac judiciară. Acesta se poate adresa unui tribunal de primă instanță care să îl oblige pe comisar să ia măsurile necesare pentru a răspunde plângerii sau să îl informeze pe reclamant cu privire la evoluția plângerii ([117]). În plus, orice persoană căreia comisarul îi comunică una dintre notificările menționate mai sus (notificare de informare, de evaluare, de executare sau de sancționare) poate introduce o cale de atac în fața unui tribunal de primă instanță ([118]). În cazul în care tribunalul consideră că decizia comisarului nu este conformă cu legea sau că, în ceea ce privește comisarul pentru informații, acesta ar fi trebuit să își exercite puterea de apreciere în mod diferit, tribunalul trebuie să admită calea de atac sau să înlocuiască decizia comisarului cu o altă notificare sau decizie pe care comisarul pentru informații ar fi putut să o emită sau să o adopte.

(107) În al treilea rând, persoanele fizice pot introduce o cale de atac împotriva operatorilor și a persoanelor împuternicite de operatori direct în fața instanțelor în temeiul articolului 79 din RGPD al Regatului Unit și al secțiunii 167 din DPA din 2018. În cazul în care, la cererea unei persoane vizate, o instanță constată că a avut loc o încălcare a drepturilor persoanei vizate în temeiul legislației privind protecția datelor, instanța poate obliga operatorul în ceea ce privește prelucrarea, sau persoana împuternicită de operator care acționează în numele operatorului respectiv, să ia măsurile specificate în ordonanță sau să se abțină de la luarea măsurilor specificate în ordonanță.

(108) În plus, în temeiul articolului 82 din RGPD al Regatului Unit și al secțiunii 168 din DPA din 2018, orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a RGPD al Regatului Unit are dreptul să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit. Normele privind despăgubirile și răspunderea prevăzute la articolul 82 alineatele (1)-(5) din RGPD al Regatului Unit sunt identice cu normele corespunzătoare din Regulamentul (UE) 2016/679. În temeiul secțiunii 168 din DPA din 2018, prejudiciile morale includ, de asemenea, suferințele clinice. În temeiul articolului 80 din RGPD al Regatului Unit, persoana vizată are, de asemenea, dreptul de a mandata un organism sau o organizație reprezentativ(ă) să depună plângerea la comisar în numele său (în temeiul articolului 77 din RGPD al Regatului Unit) și să exercite în numele său drepturile menționate la articolele 78 (dreptul la o cale de atac judiciară eficientă împotriva comisarului), 79 (dreptul la o cale de atac judiciară eficientă împotriva unui operator sau unei persoane împuternicite de operator) și 82 (dreptul la despăgubiri și răspunderea) din RGPD al Regatului Unit.

(109) În al patrulea rând, pe lângă căile de atac descrise mai sus, orice persoană care consideră că drepturile sale, inclusiv dreptul la viață privată și la protecția datelor, au fost încălcate de autoritățile publice, poate obține reparații în fața instanțelor din Regatul Unit în temeiul Legii privind drepturile omului din 1998 ([119]). O persoană care susține că o autoritate publică a acționat (sau propune să acționeze) într-un mod care este incompatibil cu un drept conferit prin convenție și, prin urmare, ilegal în temeiul secțiunii 6 punctul 1 din Legea privind drepturile omului din 1998 poate introduce o acțiune împotriva autorității respective în fața instanței sau a tribunalului competent(e) sau poate invoca drepturile în cauză în cadrul oricărei proceduri judiciare, atunci când este (sau ar fi) victimă a actului ilegal.

(110) În cazul în care constată că un act al unei autorități publice este ilegal, instanța poate admite o astfel de reparație sau cale de atac sau poate dispune, în limitele competențelor sale, după cum consideră corect și adecvat ([120]). Instanța poate, de asemenea, să declare o dispoziție din legislația primară ca fiind incompatibilă cu un drept conferit prin convenție.

([115]) Articolul 77 din RGPD al Regatului Unit.

([116]) Secțiunea 166 din DPA din 2018 se referă în mod specific la următoarele situații: (a) comisarul nu ia măsurile adecvate pentru a răspunde plângerii, (b) comisarul nu furnizează reclamantului informații cu privire la evoluția plângerii sau la rezultatul acesteia înainte de sfârșitul perioadei de trei luni care începe în momentul în care comisarul a primit plângerea sau (c) în cazul în care examinarea plângerii de către comisar nu este finalizată în perioada respectivă, acesta nu furnizează reclamantului astfel de informații în cursul unei perioade ulterioare de trei luni.

([117]) Articolul 78 alineatul (2) din RGPD al Regatului Unit și secțiunea 166 din DPA din 2018.

([118]) Articolul 78 alineatul (1) din RGPD al Regatului Unit și secțiunea 162 din DPA din 2018.

([119]) Secțiunea 7 punctul 1 din Legea privind drepturile omului din 1998. Potrivit secțiunii 7 punctul 7, o persoană este victima unui act ilegal numai dacă ar fi victimă în sensul articolului 34 din Convenția europeană a drepturilor omului dacă ar fi introdusă o acțiune în fața Curții Europene a Drepturilor Omului cu privire la actul în cauză.

([120]) Secțiunea 8 punctul 1 din Legea privind drepturile omului din 1998.

(111) În cele din urmă, după epuizarea căilor de atac naționale, o persoană poate obține reparații în fața Curții Europene a Drepturilor Omului pentru încălcarea drepturilor garantate de Convenția europeană a drepturilor omului.

3. ACCESAREA ȘI UTILIZAREA DE CĂTRE AUTORITĂȚILE PUBLICE DIN REGATUL UNIT A DATELOR CU CARACTER PERSONAL TRANSFERATE DIN UNIUNEA EUROPEANĂ

(112) Comisia a evaluat, de asemenea, cadrul juridic al Regatului Unit pentru colectarea și utilizarea ulterioară a datelor cu caracter personal transferate operatorilor economici din Regatul Unit de către autoritățile publice din Regatul Unit din motive de interes public, în special în scopul asigurării respectării dreptului penal și în scopuri de asigurare a securității naționale (denumit în continuare „accesul administrației publice"). Pentru a evalua dacă condițiile în care accesul administrației publice la datele transferate către Regatul Unit în temeiul prezentei decizii ar îndeplini criteriul „echivalenței substanțiale" în temeiul articolului 45 alineatul (1) din Regulamentul (UE) 2016/679, astfel cum a fost interpretat de Curtea de Justiție a Uniunii Europene în lumina Cartei drepturilor fundamentale, Comisia a luat în considerare în special următoarele criterii.

(113) În primul rând, orice restrângere a dreptului la protecția datelor cu caracter personal trebuie să fie prevăzută de lege, iar temeiul juridic care permite ingerința în acest drept trebuie să definească el însuși întinderea restrângerii exercitării dreptului vizat ([121]).

(114) În al doilea rând, pentru a îndeplini cerința proporționalității potrivit căreia derogările de la protecția datelor cu caracter personal și restrângerile acesteia trebuie să fie efectuate în limitele strictului necesar într-o societate democratică pentru a îndeplini obiective specifice de interes general echivalente cu cele recunoscute de Uniune, legislația țării terțe în cauză care permite o ingerință trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurilor respective și să impună o serie de cerințe minime, astfel încât persoanele ale căror date au fost transferate să dispună de garanții suficiente care să permită protejarea în mod eficient a datelor lor cu caracter personal împotriva riscurilor de abuz ([122]). Legislația trebuie în special să indice în ce împrejurări și în ce condiții poate fi luată o măsură care prevede prelucrarea unor asemenea date ([123]), precum și să supună îndeplinirea acestor cerințe unei supravegheri independente ([124]).

(115) În al treilea rând, legislația respectivă trebuie să fie obligatorie din punct de vedere juridic în temeiul dreptului intern, iar aceste cerințe legale trebuie să fie nu numai obligatorii pentru autorități, ci și opozabile autorităților din țara terță în cauză în fața instanțelor judecătorești ([125]). În special, persoanele vizate trebuie să dispună de posibilitatea de a exercita căi legale în fața unei instanțe judecătorești independente și imparțiale pentru a avea acces la date cu caracter personal care le privesc sau de a obține rectificarea sau ștergerea unor astfel de date ([126]).

3.1. **Cadrul juridic general**

(116) Ca exercitare a puterii de către o autoritate publică, accesul administrației publice în Regatul Unit trebuie să se realizeze cu respectarea deplină a legii. Regatul Unit a ratificat Convenția europeană a drepturilor omului (a se vedea considerentul 9) și toate autoritățile publice din Regatul Unit au obligația de a acționa în conformitate cu convenția ([127]). Articolul 8 din convenție prevede că orice ingerință în viața privată trebuie să fie în conformitate cu legea, în interesul unuia dintre obiectivele stabilite la articolul 8 alineatul (2) și proporțională în raport cu acest obiectiv. Articolul 8 impune, de asemenea, ca ingerința să fie „previzibilă", și anume să aibă un temei juridic clar și accesibil și ca legea să conțină garanții adecvate pentru a preveni abuzurile.

(117) În plus, în jurisprudența sa, Curtea Europeană a Drepturilor Omului a precizat că orice ingerință în dreptul la viață privată și la protecția datelor ar trebui să facă obiectul unui sistem de supraveghere eficace, independent și imparțial, care trebuie să fie asigurat fie de un judecător, fie de un alt organism independent ([128]) (de exemplu, o autoritate administrativă sau un organ parlamentar).

([121]) A se vedea *Schrems II*, punctele 174-175 și jurisprudența citată. A se vedea, de asemenea, în ceea ce privește accesul autorităților publice ale statelor membre, cauza C-623/17, *Privacy International*, ECLI:EU:C:2020:790, punctul 65, și cauzele conexate C-511/18, C-512/18 și C-520/18, *La Quadrature du Net și alții*, ECLI:EU:C:2020:791, punctul 175.

([122]) A se vedea *Schrems II*, punctele 176 și 181, precum și jurisprudența citată. A se vedea, de asemenea, în ceea ce privește accesul autorităților publice ale statelor membre, *Privacy International*, punctul 68, și *La Quadrature du Net și alții*, punctul 132.

([123]) A se vedea *Schrems II*, punctul 176. A se vedea, de asemenea, în ceea ce privește accesul autorităților publice ale statelor membre, *Privacy International*, punctul 68, și *La Quadrature du Net și alții*, punctul 132.

([124]) A se vedea *Schrems II*, punctul 179.

([125]) A se vedea *Schrems II*, punctele 181-182.

([126]) A se vedea *Schrems I*, punctul 95 și *Schrems II*, punctul 194. În acest sens, CJUE a subliniat în special faptul că respectarea articolului 47 din Carta drepturilor fundamentale, care garantează dreptul la o cale de atac eficientă în fața unei instanțe judecătorești independente și imparțiale, „participă de asemenea la nivelul de protecție impus în cadrul Uniunii [și] trebuie să fie constatată de Comisie înainte ca aceasta să adopte o decizie privind caracterul adecvat al nivelului de protecție în temeiul articolului 45 alineatul (1) din Regulamentul (UE) 2016/679" (*Schrems II*, punctul 186).

([127]) Secțiunea 6 din Legea privind drepturile omului din 1998.

([128]) Curtea Europeană a Drepturilor Omului, *Klass și alții/Germania*, cererea nr. 5029/71, punctele 17-51.

(118) În plus, persoanelor trebuie să li se furnizeze o cale de atac eficientă, iar Curtea Europeană a Drepturilor Omului a clarificat faptul că această cale de atac trebuie oferită de un organism independent și imparțial care și-a adoptat propriul regulament de procedură, alcătuit din membri care trebuie să dețină sau să fi deținut o funcție judiciară de înalt nivel sau să fie avocați experimentați, și că nu trebuie să existe nicio sarcină a probei care trebuie îndeplinită pentru a depune o cerere la aceasta. Atunci când examinează plângerile depuse de persoane, organismul independent și imparțial ar trebui să aibă acces la toate informațiile relevante, inclusiv la materialele confidențiale. În cele din urmă, acesta ar trebui să aibă competența de a remedia cazurile de neconformitate ([129]).

(119) Regatul Unit a ratificat, de asemenea, Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108) și a semnat Protocolul de modificare a Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (cunoscută sub denumirea de „Convenția 108+") în 2018 ([130]). Articolul 9 din Convenția 108 prevede că derogările de la principiile generale privind protecția datelor (articolul 5 Calitatea datelor), de la normele care reglementează categoriile speciale de date (articolul 6 Categorii speciale de date) și de la drepturile persoanelor vizate (articolul 8 Garanții suplimentare pentru persoana vizată) sunt permise numai în cazul în care o astfel de derogare este prevăzută de legislația părții și constituie o măsură necesară într-o societate democratică în interesul protejării siguranței statului, a siguranței publice, a intereselor monetare ale statului sau în interesul eliminării infracțiunilor, ori pentru protejarea persoanei vizate sau a drepturilor și libertăților altora ([131]).

(120) Prin urmare, prin calitatea de membru al Consiliului Europei, aderarea la Convenția europeană a drepturilor omului și recunoașterea competenței Curții Europene a Drepturilor Omului, Regatul Unit este supus unei serii de obligații, consacrate în dreptul internațional public, care încadrează sistemul său de acces al administrației publice pe baza unor principii, garanții și drepturi individuale similare cu cele garantate de dreptul Uniunii și aplicabile statelor membre. Astfel cum se subliniază în considerentul 19, aderarea continuă la astfel de instrumente este, prin urmare, un element deosebit de important al evaluării pe care se întemeiază prezenta decizie.

(121) În plus, DPA din 2018 prevede garanții și drepturi specifice în materie de protecție a datelor atunci când datele sunt prelucrate de autorități publice, inclusiv de autoritățile de asigurare a respectării legii și de organismele de asigurare a securității naționale.

(122) În special, regimul de prelucrare a datelor cu caracter personal în contextul asigurării respectării dreptului penal este prevăzut în partea 3 din DPA din 2018 care a fost adoptată pentru a transpune Directiva (UE) 2016/680. Partea 3 din DPA din 2018 se aplică prelucrării datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora ([132]).

(123) Conceptul de „autoritate competentă" este definit în secțiunea 30 din DPA ca fiind o persoană prevăzută în anexa 7 la DPA din 2018, precum și orice altă persoană, în măsura în care persoana are funcții statutare în oricare dintre scopurile de asigurare a respectării legii ([133]). Astfel cum se explică mai jos (a se vedea considerentul 139), anumite autorități competente (de exemplu, Agenția Națională pentru Combaterea Criminalității) pot face uz, în anumite condiții, de competențele conferite de Legea din 2016 de reglementare a competențelor de investigare (IPA din 2016). În acest caz, garanțiile prevăzute de IPA din 2016 se vor aplica în plus față de cele prevăzute în partea 3 din DPA din 2018. Serviciile de informații (Serviciul Secret de Informații, Serviciul de Securitate și Cartierul General pentru Comunicații) nu sunt „autorități competente" ([134]) care intră sun incidența părții 3 din DPA din 2018 și, prin urmare, normele prevăzute de aceasta nu se aplică niciuneia dintre activitățile lor. O parte specifică din DPA din 2018 (partea 4) este dedicată prelucrării datelor cu caracter personal de către serviciile de informații (pentru mai multe detalii, a se vedea considerentul 125).

([129]) Curtea Europeană a Drepturilor Omului, *Kennedy/Regatul Unit*, cererea nr. 26839/05 („Kennedy"), punctele 167 și 190.

([130]) Pentru mai multe informații cu privire la Convenția europeană a drepturilor omului și încorporarea acesteia în dreptul Regatului Unit prin Legea privind drepturile omului din 1998, precum și cu privire la Convenția 108, a se vedea considerentul 9.

([131]) În mod similar, în temeiul articolului 11 din Convenția 108+, restricțiile de la exercitarea anumitor drepturi și obligații specifice din convenție în scopul securității naționale sau al prevenirii, investigării și urmăririi penale a infracțiunilor și al executării sancțiunilor penale sunt permise numai în cazul în care o astfel de restricție este prevăzută de lege, respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică. Activitățile de prelucrare în scopuri de securitate națională și apărare trebuie, de asemenea, să facă obiectul unui control și al unei supravegheri independente și efective în temeiul legislației interne a părții respective la convenție.

([132]) Secțiunea 31 din DPA din 2018.

([133]) Printre autoritățile competente enumerate în anexa 7 se numără nu numai forțele de poliție, ci și toate departamentele ministeriale ale guvernului Regatului Unit, precum și alte autorități cu atribuții de investigare (de exemplu, Comisarul Administrației Fiscale și Vamale din Regatul Unit – *Commissioner for Her Majesty's Revenue and Customs*, Agenția Națională pentru Combaterea Criminalității – National Crime Agency, Autoritatea Fiscală din Țara Galilor, Autoritatea pentru Concurență și Piețe sau Registrul funciar al Majestății Sale – *Her Majesty's Land Register*), agenții de urmărire penală, alte agenții de justiție penală și alți deținători sau organizații care desfășoară activități de asigurare a respectării legii (printre acestea, anexa 7 la DPA din 2018 enumeră directorii procurorilor, directorul procurorilor din Irlanda de Nord sau comisarul pentru informații).

([134]) Secțiunea 30 punctul 2 din DPA din 2018.

(124) În mod similar Directivei (UE) 2016/680, partea 3 din DPA din 2018 stabilește principiile legalității și echității ([135]), limitărilor legate de scop ([136]), reducerii la minimum a datelor ([137]), exactității ([138]), limitărilor legate de stocare ([139]) și securității ([140]). Legislația impune obligații specifice în materie de transparență ([141]) și oferă persoanelor dreptul de acces ([142]), rectificare și ștergere ([143]), precum și dreptul de a nu face obiectul procesului decizional automatizat ([144]). Autoritățile competente au, de asemenea, obligația de a pune în aplicare protecția datelor începând cu momentul conceperii și în mod implicit, de a ține evidențe ale activităților de prelucrare și, pentru anumite operațiuni de prelucrare, de a efectua evaluări ale impactului asupra protecției datelor și de a consulta în prealabil comisarul pentru informații ([145]). În conformitate cu secțiunea 56 din DPA din 2018, acestea trebuie să demonstreze conformitatea. În plus, autoritățile trebuie să instituie măsuri adecvate pentru a asigura securitatea prelucrării ([146]) și sunt supuse unor obligații specifice în cazul unei încălcări a securității datelor, inclusiv notificarea comisarului pentru informații și persoanelor vizate cu privire la aceste încălcări ([147]). La fel ca în cazul Directivei (UE) 2016/680, există, de asemenea, o cerință ca un operator (cu excepția cazului în care acesta este o instanță sau o altă autoritate judiciară care acționează în exercițiul unei funcții judiciare) să desemneze un responsabil cu protecția datelor ([148]) care asistă operatorul în îndeplinirea obligațiilor sale, precum și în monitorizarea conformității menționate ([149]). În plus, legislația impune cerințe specifice pentru transferurile internaționale de date cu caracter personal în scopul asigurării respectării legii către țări terțe sau organizații internaționale pentru a asigura continuitatea protecției ([150]). La aceeași dată cu prezenta decizie, Comisia a adoptat o decizie privind caracterul adecvat al nivelului de protecție în temeiul articolului 36 alineatul (3) din Directiva (UE) 2016/680, prin care constata că regimul de protecție a datelor aplicabil prelucrării de către autoritățile de aplicare a dreptului penal din Regatul Unit asigură un nivel de protecție echivalent în esență cu cel garantat de Directiva (UE) 2016/680.

(125) Partea 4 din DPA din 2018 se aplică tuturor prelucrărilor efectuate de serviciile de informații sau în numele acestora. În special, aceasta stabilește principalele principii privind protecția datelor (legalitate, echitate și transparență ([151]); limitări legate de scop ([152]); reducerea la minimum a datelor ([153]); exactitate ([154]); limitări legate de stocare ([155]) și securitate ([156]), impune condiții pentru prelucrarea categoriilor speciale de date ([157]), prevede drepturi ale persoanelor vizate ([158]), impune

([135]) Secțiunea 35 din DPA din 2018.
([136]) Secțiunea 36 din DPA din 2018.
([137]) Secțiunea 37 din DPA din 2018.
([138]) Secțiunea 38 din DPA din 2018.
([139]) Secțiunea 39 din DPA din 2018.
([140]) Secțiunea 40 din DPA din 2018.
([141]) Secțiunea 44 din DPA din 2018.
([142]) Secțiunea 45 din DPA din 2018.
([143]) Secțiunile 46 și 47 din DPA din 2018.
([144]) Secțiunile 49 și 50 din DPA din 2018.
([145]) Secțiunile 56-65 din DPA din 2018.
([146]) Secțiunea 66 din DPA din 2018.
([147]) Secțiunile 67-68 din DPA din 2018.
([148]) Secțiunile 69-71 din DPA din 2018.
([149]) Secțiunile 67-68 din DPA din 2018.
([150]) Partea 3 capitolul 5 din DPA din 2018.
([151]) În temeiul secțiunii 86 punctul 6 din DPA din 2018, pentru a stabili echitatea și transparența prelucrării, trebuie să se ia în considerare metoda prin care aceasta este obținută. În acest sens, cerința de echitate și transparență este îndeplinită dacă datele sunt obținute de la o persoană care este autorizată sau obligată în mod legal să le furnizeze.
([152]) În conformitate cu secțiunea 87 din DPA din 2018, scopurile prelucrării trebuie să fie determinate, explicite și legitime. Datele nu trebuie prelucrate într-un mod incompatibil cu scopurile pentru care sunt colectate. În temeiul secțiunii 87 punctul 3 din DPA din 2018, o prelucrare suplimentară compatibilă a datelor cu caracter personal poate fi permisă numai dacă operatorul este autorizat prin lege să prelucreze datele în acest scop, iar prelucrarea este necesară și proporțională cu scopul secundar respectiv. Prelucrarea ar trebui considerată compatibilă în cazul în care aceasta constă în prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice și face obiectul unor garanții adecvate (secțiunea 87 punctul 4 din DPA din 2018).
([153]) Datele cu caracter personal trebuie să fie adecvate, relevante și neexcesive (secțiunea 88 din DPA din 2018).
([154]) Datele cu caracter personal trebuie să fie exacte și actualizate (secțiunea 89 din DPA din 2018).
([155]) Datele cu caracter personal nu trebuie păstrate mai mult decât este necesar (secțiunea 90 din DPA din 2018).
([156]) Al șaselea principiu privind protecția datelor este că datele cu caracter personal trebuie prelucrate într-un mod care să includă luarea unor măsuri de securitate adecvate în ceea ce privește riscurile care decurg din prelucrarea datelor cu caracter personal. Riscurile includ (dar nu se limitează la) accesul accidental sau neautorizat la datele cu caracter personal sau distrugerea, pierderea, utilizarea, modificarea sau divulgarea acestora (secțiunea 91 din DPA din 2018). Secțiunea 107 prevede, de asemenea, că: 1. fiecare operator trebuie să pună în aplicare măsuri de securitate adecvate pentru riscurile care decurg din prelucrarea datelor cu caracter personal; și 2. în cazul prelucrării automate, fiecare operator și fiecare persoană împuternicită de operator pun în aplicare măsuri preventive sau de atenuare pe baza unei evaluări a riscurilor.
([157]) Secțiunea 86 punctul 2 litera (b) și anexa 10 la DPA din 2018.
([158]) Partea 4 capitolul 3 din DPA din 2018, în special drepturile: de acces, rectificare și ștergere, de a se opune prelucrării și de a nu face obiectul procesului decizional automatizat, de a interveni în procesul decizional automatizat și de a fi informat cu privire la procesul decizional. În plus, operatorul trebuie să ofere persoanei vizate informații cu privire la prelucrarea datelor sale cu caracter personal. Astfel cum se explică în orientările ICO privind prelucrarea de către serviciile de informații, persoanele fizice își pot exercita toate drepturile (inclusiv o cerere de rectificare) prin depunerea unei plângeri la ICO sau prin introducerea de acțiuni în instanță (a se vedea Orientările ICO privind prelucrarea de către serviciile de informații, disponibil la următoarea adresă: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing).

protecția datelor începând cu momentul conceperii ([159]) și reglementează transferurile internaționale de date cu caracter personal ([160]). ICO a emis recent orientări detaliate privind prelucrarea de către serviciile de informații în temeiul părții 4 din DPA din 2018 ([161]).

(126) În același timp, secțiunea 110 din DPA din 2018 prevede o derogare de la dispozițiile specificate în partea 4 din DPA din 2018 ([162]), în cazul în care o astfel de derogare este necesară pentru protejarea securității naționale. Această derogare poate fi invocată pe baza unei analize de la caz la caz ([163]). Astfel cum au explicat autoritățile Regatului Unit și după cum este confirmat de jurisprudență, un „operator trebuie să ia în considerare consecințele reale pentru securitatea națională sau apărare dacă ar trebui să respecte dispoziția specifică privind protecția datelor și dacă ar putea respecta în mod rezonabil regula obișnuită fără a afecta securitatea națională sau apărarea" ([164]). Utilizarea corespunzătoare sau necorespunzătoare a derogării face obiectul supravegherii ICO ([165]).

(127) În plus, în ceea ce privește posibilitatea de a restricționa, pentru protecția „securității naționale", aplicarea dispozițiilor specificate mai sus, în conformitate cu secțiunea 111 din DPA din 2018, un operator poate solicita un certificat semnat de un ministru din cadrul Cabinetului sau de procurorul general, care să ateste că restricționarea acestor drepturi este o măsură necesară și proporțională pentru protecția securității naționale ([166]).

(128) Guvernul Regatului Unit a emis orientări pentru a ajuta operatorii atunci când analizează dacă să solicite un certificat de securitate națională în temeiul DPA din 2018, care subliniază în special că orice limitare a drepturilor persoanelor vizate în ceea ce privește protejarea securității naționale trebuie să fie proporțională și necesară ([167]). Toate certificatele de securitate națională trebuie publicate pe site-ul internet al ICO ([168]).

([159]) Secțiunea 103 din DPA din 2018.

([160]) Secțiunea 109 din DPA din 2018. Transferurile de date cu caracter personal către organizații internaționale sau țări din afara Regatului Unit sunt posibile dacă transferul este o măsură necesară și proporțională întreprinsă în scopul îndeplinirii funcțiilor legale ale operatorului sau în alte scopuri prevăzute în anumite secțiuni din Legea privind serviciul de securitate din 1989 (*Security Service Act 1989*) și din Legea privind serviciile de informații din 1994 (*Intelligence Services Act 1994*).

([161]) Orientările ICO, a se vedea nota de subsol158
Secțiunea 30 din DPA din 2018 și anexa 7 la DPA din 2018.

([162]) Secțiunea 110 punctul 2 din DPA din 2018 enumeră dispozițiile de la care se permite o derogare. Aceasta include principiile privind protecția datelor (cu excepția principiului legalității), drepturile persoanei vizate, obligația de a informa comisarul pentru informații cu privire la o încălcare a securității datelor, competențele de inspecție ale comisarului pentru informații în conformitate cu obligațiile internaționale, anumite competențe ale comisarului pentru informații în materie de asigurare a respectării legii, dispozițiile care fac din anumite încălcări ale protecției datelor o infracțiune, precum și dispozițiile referitoare la scopurile speciale ale prelucrării, cum ar fi scopurile jurnalistice, academice sau artistice.

([163]) A se vedea *Baker/Secretary of State*, a se vedea nota de subsol 61.

([164]) Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat, secțiunea H: Cadrul privind protecția datelor în materie de securitate națională și competențele de investigare, paginile 15-16 (a se vedea nota de subsol 31). A se vedea, de asemenea, *Baker/Secretary of State* (a se vedea nota de subsol 61), în care instanța a casat un certificat de securitate națională emis de ministrul de interne și prin care se confirma aplicarea excepției privind securitatea națională, considerând că nu există niciun motiv pentru a prevedea o excepție generală de la obligația de a răspunde cererilor de acces și că permiterea unei astfel de excepții în toate circumstanțele, fără o analiză de la caz la caz, ar depăși ceea ce este necesar și proporțional pentru protecția securității naționale.

([165]) A se vedea memorandumul de înțelegere dintre ICO și UKIC, conform căruia „La primirea unei plângeri din partea unei persoane vizate, ICO va dori să se asigure că problema a fost tratată corect și, după caz, că aplicarea oricărei derogări a fost utilizată în mod corespunzător". Memorandumul de înțelegere dintre Biroul comisarului pentru informații și serviciile de informații din Regatul Unit, punctul 16, disponibil la următoarea adresă: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf

([166]) DPA din 2018 a abrogat posibilitatea de a elibera certificate în temeiul secțiunii 28 punctul 2 din Legea privind protecția datelor din 1998. Cu toate acestea, posibilitatea de a emite „certificate vechi" există în continuare în măsura în care există o provocare istorică în temeiul Legii din 1998 [a se vedea punctul 17 din partea 5 a anexei 20 la DPA din 2018]. Totuși, această posibilitate pare foarte rară și se va aplica numai în cazuri limitate, cum ar fi, de exemplu, în cazul în care o persoană vizată formulează o cale de atac în ceea ce privește utilizarea derogării în materie de securitate națională în legătură cu prelucrarea de către o autoritate publică care a efectuat prelucrarea în temeiul Legii din 1998. Trebuie remarcat faptul că, în aceste cazuri, secțiunea 28 din DPA din 1998 se va aplica în întregime, incluzând, prin urmare, posibilitatea ca persoana vizată să conteste certificatul în instanță.

([167]) Orientările Guvernului Regatului Unit privind certificatele de securitate națională în temeiul Legii privind protecția datelor din 2018, disponibile la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf. Potrivit explicației furnizate de autoritățile Regatului Unit, deși un certificat este o dovadă concludentă a faptului că, în ceea ce privește datele sau prelucrarea descrise în certificat, derogarea este aplicabilă, acesta nu elimină cerința ca operatorul să analizeze, de la caz la caz, dacă este necesar să invoce derogarea.

([168]) În conformitate cu secțiunea 130 din DPA din 2018, ICO poate decide să nu publice textul sau o parte a textului certificatului, în cazul în care acest lucru ar fi contrar interesului securității naționale sau ar fi contrar interesului public sau ar putea pune în pericol siguranța oricărei persoane. În aceste cazuri, ICO va publica totuși faptul că certificatul a fost eliberat.

(129) Certificatul ar trebui să fie emis pe o durată determinată de maximum cinci ani, astfel încât să fie revizuit periodic de către executiv ([169]). Certificatul identifică datele cu caracter personal sau categoriile de date cu caracter personal care fac obiectul derogării, precum și dispozițiile DPA din 2018 cărora li se aplică derogarea ([170]).

(130) Este important de remarcat faptul că certificatele de securitate națională nu oferă un temei suplimentar pentru restricționarea drepturilor privind protecția datelor din motive de securitate națională. Cu alte cuvinte, operatorul sau persoana împuternicită de operator poate invoca un certificat numai atunci când a ajuns la concluzia că este necesar să invoce derogarea în materie de securitate națională care, astfel cum s-a explicat mai sus, trebuie aplicată de la caz la caz ([171]). Chiar dacă un certificat de securitate națională se aplică chestiunii în cauză, ICO poate investiga dacă invocarea derogării în materie de securitate națională a fost sau nu justificată într-un caz specific ([172]).

(131) Orice persoană direct afectată de emiterea certificatului poate introduce o cale de atac la Tribunalul Superior ([173]) împotriva certificatului ([174]) sau, în cazul în care certificatul identifică date prin intermediul unei descrieri generale, poate contesta aplicarea certificatului la o serie de date specifice ([175]). Tribunalul va examina decizia de emitere a certificatului și va decide dacă au existat motive întemeiate pentru emiterea certificatului ([176]). Acesta poate lua în considerare o gamă largă de aspecte, printre care se numără și necesitatea, proporționalitatea și legalitatea, având în vedere impactul asupra drepturilor persoanelor vizate și punând în balanță necesitatea de a proteja securitatea națională. În consecință, tribunalul poate stabili că certificatul nu se aplică datelor cu caracter personal specifice care fac obiectul căii de atac ([177]).

(132) Un set diferit de restricții posibile se referă la cele care se aplică, în temeiul anexei 11 la DPA din 2018, anumitor dispoziții ale părții 4 din DPA din 2018 ([178]) pentru a proteja alte obiective importante de interes public general sau interese protejate, cum ar fi, de exemplu, privilegiul parlamentar, secretul profesional al avocatului, desfășurarea procedurilor judiciare sau eficacitatea de luptă a forțelor armate ([179]). Aplicarea acestor dispoziții fie este exceptată pentru anumite categorii de informații („bazată pe categorii"), fie este exceptată în măsura în care aplicarea acestor dispoziții ar putea aduce atingere interesului protejat („bazată pe prejudicii") ([180]). Derogările bazate pe prejudicii pot

([169]) Orientările Guvernului Regatului Unit privind certificatele de securitate națională, punctul 15, a se vedea nota de subsol 167.

([170]) Orientările Guvernului Regatului Unit privind certificatele de securitate națională, punctul 5, a se vedea nota de subsol 167.

([171]) A se vedea nota de subsol 164.

([172]) Secțiunea 102 din DPA din 2018 prevede că operatorul trebuie să fie în măsură să demonstreze că s-a conformat DPA din 2018. Aceasta implică faptul că un serviciu de informații ar trebui să demonstreze ICO faptul că, atunci când invocă derogarea, a luat în considerare circumstanțele specifice ale cazului. ICO publică, de asemenea, o evidență a certificatelor de securitate națională, care este disponibilă la următoarea adresă: este disponibilă la următoarea adresă: https://ico.org.uk/about-the-ico/our-information/national-security-certificates

([173]) Tribunalul Superior este instanța competentă să soluționeze căile de atac împotriva hotărârilor pronunțate de tribunalele administrative inferioare și are competențe specifice pentru soluționarea căilor de atac directe introduse împotriva deciziilor anumitor organisme guvernamentale.

([174]) Secțiunea 111 punctul 3 din DPA din 2018.

([175]) Secțiunea 111 punctul 5 din DPA din 2018.

([176]) În cauza *Baker/Secretary of State* (a se vedea nota de subsol 61), Information Tribunal a anulat un certificat de securitate națională emis de ministrul de interne, considerând că nu există niciun motiv pentru a prevedea o excepție generală de la obligația de a răspunde cererilor de acces și că permiterea unei astfel de excepții în toate circumstanțele, fără o analiză de la caz la caz, ar depăși ceea ce este necesar și proporțional pentru protecția securității naționale.

([177]) Orientările Guvernului Regatului Unit privind certificatele de securitate națională, punctul 25, a se vedea nota de subsol 167.

([178]) Printre acestea se numără: (i) principiile privind protecția datelor prevăzute în partea 4, cu excepția legalității cerinței de prelucrare în temeiul primului principiu și a faptului că prelucrarea trebuie să îndeplinească una dintre condițiile relevante prevăzute în anexele 9 și 10; (ii) drepturile persoanelor vizate; și (iii) obligațiile legate de raportarea încălcărilor către ICO.

([179]) Partea 4 din DPA din 2018 prevede cadrul juridic care se aplică tuturor tipurilor de prelucrare a datelor cu caracter personal efectuate de serviciile de informații (și nu numai în scopul exercitării sarcinilor lor în materie de securitate națională). Prin urmare, partea 4 se aplică și atunci când agențiile de informații prelucrează date, de exemplu în scopul gestionării resurselor umane, în contextul litigiilor sau în contextul achizițiilor publice. Restricțiile enumerate în anexa 11 sunt destinate în principal aplicării în aceste alte contexte. De exemplu, în contextul litigiilor cu un angajat, poate fi invocată restricția în scopul „procedurilor judiciare" sau, în contextul achizițiilor publice, poate fi invocată restricția în scopul „negocierii" etc. Acest lucru se reflectă în orientările ICO privind prelucrarea de către serviciile de informații, care menționează negocierea unei înțelegeri între o agenție de informații și un fost angajat care depune o creanță legată de raporturile de muncă ca exemplu pentru aplicarea restricțiilor din anexa 11 (a se vedea nota de subsol 161). De asemenea, trebuie remarcat faptul că aceleași restricții sunt disponibile pentru alte autorități publice în conformitate cu anexa 2 la partea 2 din DPA din 2018.

([180]) Conform Cadrului explicativ al Regatului Unit, excepțiile „bazate pe categorii" sunt: (i) informații cu privire la acordarea de distincții și demnități ale Coroanei; (ii) secretul profesional al avocatului; (iii) referințe confidențiale privind angajarea, formarea sau educația; și (iv) foi de examinare și note la examene. Excepțiile „bazate pe prejudicii" se referă la următoarele aspecte: (i) prevenirea sau depistarea infracțiunilor; arestarea și urmărirea penală a infractorilor; (ii) privilegiul parlamentar; (iii) proceduri judiciare; (iv) eficacitatea de luptă a forțelor armate ale Coroanei; (v) bunăstarea economică a Regatului Unit; (vi) negocierile cu persoana vizată; (vii) scopuri de cercetare științifică sau istorică ori scopuri statistice; (viii) arhivarea în interes public. Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat, secțiunea H: Securitatea națională, pagina 13, a se vedea nota de subsol 31.

fi invocate numai în măsura în care aplicarea dispoziției enumerate privind protecția datelor ar putea aduce atingere interesului specific în cauză. Prin urmare, utilizarea unei derogări trebuie să fie întotdeauna justificată prin trimiterea la prejudiciul relevant care ar putea apărea în fiecare caz în parte. Derogările bazate pe categorii pot fi invocate numai în ceea ce privește categoria specifică, definită în mod strict, de informații pentru care se acordă derogarea. Acestea sunt similare, în ceea ce privește scopul și efectul, mai multor excepții de la RGPD al Regatului Unit (în temeiul anexei 2 la DPA din 2018) care, la rândul lor, reflectă cele prevăzute la articolul 23 din RGPD.

(133) Din cele de mai sus rezultă că există limitări și condiții în temeiul dispozițiilor legale aplicabile din Regatul Unit, astfel cum sunt interpretate, de asemenea, de instanțe și de comisarul pentru informații, pentru a se asigura că aceste derogări și restricții rămân în limitele a ceea ce este necesar și proporțional pentru protejarea securității naționale.

3.2. **Accesul și utilizarea de către autoritățile publice din Regatul Unit în scopuri de asigurare a respectării dreptului penal**

(134) Legislația Regatului Unit impune o serie de limitări privind accesul la datele cu caracter personal și utilizarea acestora în scopul asigurării respectării dreptului penal și prevede mecanisme de supraveghere și de exercitare a unei căi de atac în acest domeniu, care sunt în conformitate cu cerințele menționate în considerentele 113-115 din prezenta decizie. Condițiile în care poate avea loc un astfel de acces și garanțiile aplicabile utilizării acestor competențe sunt evaluate în detaliu în secțiunile următoare.

3.2.1. *Temeiurile juridice și limitările/garanțiile aplicabile*

(135) Potrivit principiului legalității garantat în temeiul secțiunii 35 din DPA din 2018, prelucrarea datelor cu caracter personal în oricare dintre scopurile de asigurare a respectării legii este legală numai dacă se întemeiază pe lege și fie persoana vizată și-a dat consimțământul pentru prelucrare în acest scop ([181]), fie prelucrarea este necesară pentru îndeplinirea unei sarcini în acest scop de către o autoritate competentă.

3.2.1.1. Mandate de percheziție și ordine de divulgare

(136) În cadrul juridic al Regatului Unit, colectarea datelor cu caracter personal de la operatorii economici, inclusiv de la cei care ar prelucra date transferate din UE în temeiul prezentei decizii privind caracterul adecvat al nivelului de protecție, în scopul asigurării respectării dreptului penal, este permisă pe baza mandatelor de percheziție ([182]) și a ordinelor de divulgare ([183]).

(137) Mandatele de percheziție sunt emise de o instanță, de obicei la cererea anchetatorului. Acestea permit unui anchetator să intre în incinte pentru a căuta materiale sau persoane relevante pentru ancheta pe care o desfășoară și să rețină orice element pentru care a fost autorizată efectuarea percheziției, inclusiv orice documente sau materiale relevante care conțin date cu caracter personal ([184]). Un ordin de divulgare, care trebuie, de asemenea, să fie emis de o instanță, impune persoanei menționate în acesta să prezinte sau să permită accesul la materialul pe care îl deține sau îl controlează. Solicitantul trebuie să justifice în fața instanței de ce este necesar mandatul sau

([181]) Utilizarea consimțământului nu pare relevantă într-un scenariu privind caracterul adecvat, deoarece într-o situație de transfer, datele nu vor fi fost colectate direct de la o persoană vizată din UE de către o autoritate de aplicare a legii din Regatul Unit pe baza consimțământului.

([182]) Pentru temeiul juridic relevant, a se vedea secțiunea 8 și următoarele din PACE din 1984 (pentru Anglia și Țara Galilor), secțiunea 10 și următoarele din *Police and Criminal Evidence Order (Northern Ireland)* (Ordinul privind competențele polițienești și probele în materie penală) (Irlanda de Nord) din 1989, iar pentru Scoția, acesta este obținut în temeiul common law [a se vedea secțiunea 46 din *Criminal Justice (Scotland) Act* – Legea privind justiția penală (Scoția) din 2016 și secțiunea 23B din *Criminal Law (Consolidation) (Scotland)* – Codul penal (consolidare) (Scoția)]. Pentru mandatul de percheziție emis după arestare, temeiul juridic este secțiunea 18 din PACE din 1984 (pentru Anglia și Țara Galilor), secțiunea 20 și următoarele din Ordinul privind competențele polițienești și probele în materie penală (Irlanda de Nord) din 1989, iar pentru Scoția, acesta este obținut în temeiul common law [a se vedea secțiunea 46 din Legea privind justiția penală (Scoția) din 2016]. Autoritățile Regatului Unit au clarificat faptul că mandatele de percheziție sunt emise de o instanță, la cererea anchetatorului. Acestea permit unui anchetator să intre în incinte pentru a căuta materiale sau persoane relevante pentru ancheta pe care o desfășoară; executarea mandatului va necesita adesea asistența unui agent de poliție.

([183]) Atunci când ancheta se referă la spălarea banilor (inclusiv confiscare și proceduri civile de recuperare), temeiul juridic relevant pentru solicitarea unui ordin de divulgare este secțiunea 345 și următoarele pentru Anglia, Țara Galilor și Irlanda de Nord și secțiunea 380 și următoarele din *Proceeds of Crime Act* (Legea privind produsele infracțiunii) din 2002 pentru Scoția. Atunci când ancheta se referă la alte aspecte decât spălarea banilor, se poate depune o cerere de emitere a unui ordin de divulgare în temeiul secțiunii 9 și al anexei 1 la PACE din 1984 pentru Anglia și Țara Galilor și al secțiunii 10 și următoarele din Ordinul privind competențele polițienești și probele în materie penală (Irlanda de Nord) din 1989 pentru Irlanda de Nord. Pentru Scoția, acesta se obține în temeiul common law [a se vedea secțiunea 46 din Legea privind justiția penală (Scoția) din 2016 și secțiunea 23B din Codul penal (consolidare) (Scoția)]. Autoritățile din Regatul Unit au clarificat faptul că un ordin de divulgare impune persoanei menționate în acesta să prezinte sau să permită accesul la materialul pe care îl deține sau îl controlează (a se vedea punctul 4 din anexa 1 la PACE din 1984).

([184]) De exemplu, PACE din 1984 prevede, în secțiunile 8 și 18, competențe de a confisca și a reține orice element pentru care a fost autorizată o percheziție.

ordinul, precum și de ce este în interes public. Există mai multe competențe legale care permit emiterea de mandate de percheziție și de ordine de divulgare. Fiecare dispoziție are propriul set de condiții legale care trebuie îndeplinite pentru emiterea unui mandat ([185]) sau a unui ordin de divulgare ([186]).

(138) Ordinele de divulgare și mandatele de percheziție pot fi contestate prin control jurisdicțional ([187]). În ceea ce

([185]) De exemplu, secțiunile 8 și 18 din PACE reglementează competența unui judecător de pace de a autoriza un mandat și, respectiv, a unui agent de poliție de a percheziționa o proprietate. În primul caz (secțiunea 8), înainte de a emite un mandat, un judecător de pace trebuie să se asigure în prealabil că există motive întemeiate pentru a considera că: (i) a fost comisă o infracțiune pedepsibilă; (ii) în incinte există materiale care ar putea avea o valoare substanțială (fie ele însele, fie împreună cu alte materiale) pentru anchetarea infracțiunii; (iii) este probabil ca materialele să constituie probe relevante; (iv) nu constau în sau nu includ elemente supuse secretului profesional al avocatului, materiale excluse sau materiale pentru proceduri speciale; și (v) nu ar fi posibil să se obțină intrarea fără utilizarea unui mandat. În al doilea caz, articolul 18 permite unui agent de poliție să efectueze o percheziție la locuința unei persoane arestate pentru o infracțiune pedepsibilă pentru alte materiale decât cele supuse secretului profesional al avocatului, în cazul în care are motive întemeiate să suspecteze că în locuință există probe care se referă la infracțiunea respectivă sau la o altă infracțiune similară sau conexă. O astfel de percheziție trebuie să se limiteze la descoperirea materialelor respective și trebuie să fie autorizată în scris de un funcționar al poliției având cel puțin gradul de inspector, cu excepția cazului în care acest lucru este necesar pentru anchetarea infracțiunii. În acest caz, un funcționar având cel puțin gradul de inspector trebuie să fie informat cât mai curând posibil după efectuarea acesteia. Motivele percheziției și natura probelor căutate trebuie să fie înregistrate. În plus, secțiunile 15 și 16 din PACE din 1984 prevăd garanții legale care trebuie respectate atunci când se solicită un mandat de percheziție. Secțiunea 15 specifică cerințele aplicabile pentru obținerea unui mandat de percheziție (inclusiv conținutul cererii formulate de agentul de poliție și faptul că mandatul trebuie să specifice, printre altele, legea în temeiul căreia este emis și să identifice, pe cât posibil, articolele și persoanele care trebuie căutate și incintele la care trebuie efectuată percheziția). Secțiunea 16 reglementează modul în care trebuie efectuată o percheziție în temeiul unui mandat (de exemplu: secțiunea 16 punctul 5 prevede că funcționarul care execută mandatul furnizează ocupantului o copie a mandatului; secțiunea 16 punctul 11 prevede ca mandatul, odată executat, să fie păstrat pe o perioadă de 12 luni; secțiunea 16 punctul 12 conferă ocupantului dreptul de a verifica mandatul în această perioadă, dacă dorește acest lucru). Aceste secțiuni contribuie la asigurarea conformității cu articolul 8 din Convenția europeană a drepturilor omului [a se vedea, de exemplu, Kent Pharmaceuticals/Director of the Serious Fraud Office [2002] EWHC 3023 (QB) la [30] de Lord Woolf CJ]. Nerespectarea acestor garanții poate duce la declararea percheziției drept ilegală [de exemplu, R (Brook)/Preston Crown Court [2018] EWHC 2024 (Admin), [2018] ACD 95; R (Superior Import/Export Ltd)/Revenue and Customs Commissioners [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115; și R (F)/Blackfriars Crown Court [2014] EWHC 1541 (Admin)]. Secțiunile 15 și 16 din PACE din 1984 sunt completate de Codul B din PACE, un cod de bune practici elaborat pentru a reglementa exercitarea competențelor polițienești de a efectua percheziții în incinte.

([186]) De exemplu, atunci când se emite un ordin de divulgare în temeiul Legii privind produsele infracțiunii din 2002, pe lângă necesitatea de a avea motive întemeiate pentru a îndeplini condițiile prevăzute la articolul 346 alineatul (2) din Legea privind produsele infracțiunii, ar trebui să existe dovezi satisfăcătoare din care să rezulte că persoana în cauză se află în posesia materialului astfel specificat sau deține controlul asupra acestuia și că este probabil ca materialul să aibă o valoare substanțială. În plus, o altă cerință pentru emiterea unui ordin de divulgare este faptul că trebuie să existe motive întemeiate pentru a considera că este în interes public ca materialul să fie divulgat sau accesul la acesta să fie acordat, având în vedere (a) beneficiul care ar putea rezulta pentru anchetă în cazul în care materialul este obținut; și (b) circumstanțele referitoare la persoana despre care cererea precizează că pare să se afle în posesia materialului care conține informațiile sale sau să dețină controlul asupra acestuia. În mod similar, o instanță care examinează o cerere de emitere a unui ordin de divulgare în temeiul anexei 1 la PACE din 1984 trebuie să se asigure că sunt îndeplinite anumite condiții. În special, anexa 1 la PACE stabilește două seturi separate de condiții alternative, dintre care unul trebuie îndeplinit înainte ca un judecător să poată emite un ordin de divulgare. Primul set impune ca judecătorul să aibă motive întemeiate să considere: (i) că a fost săvârșită o infracțiune pedepsibilă; (ii) materialele căutate în incintă constau în sau includ materiale pentru proceduri speciale, dar nu materiale excluse; (iii) materialele ar putea avea o valoare substanțială, fie ele însele, fie împreună cu alte materiale, pentru anchetă; (iv) și că este probabil ca acestea să constituie probe relevante; (v) alte metode de obținere a materialelor fie au fost încercate, fie nu au fost încercate deoarece ar fi sortite eșecului; și (vi) luând în considerare beneficiul pentru anchetă și circumstanțele în care persoana în cauză le deține, este în interes public ca materialele să fie divulgate sau ca accesul la acestea să fie furnizat. Al doilea set de condiții impune: (i) ca în incintă să existe materiale care constau în materiale pentru proceduri speciale sau materiale excluse; (ii) dacă nu ar fi existat interzicerea perchezițiilor efectuate în temeiul legislației adoptate înainte de PACE pentru materiale pentru proceduri speciale, materiale excluse sau materiale supuse secretului profesional al avocatului, ar fi putut fi emis un mandat de percheziție pentru materiale; și (iii) ar fi fost oportun să se procedeze astfel.

([187]) Controlul jurisdicțional este procedura legală prin care deciziile unui organism public pot fi contestate la Înalta Curte. Instanțele „reexaminează" decizia contestată și decid dacă se poate susține că decizia este eronată din punct de vedere juridic, având în vedere conceptele/principiile de drept public. Motivele principale ale controlului jurisdicțional sunt: ilegalitatea, iraționalitatea, viciile de formă, încrederea legitimă și drepturile omului. În urma unei admiteri în cadrul unei proceduri de control jurisdicțional, o instanță poate dispune o serie de căi de atac diferite; cea mai frecventă este un ordin de casare (care ar anula sau ar casa decizia inițială – și anume decizia de emitere a unui mandat de percheziție), în anumite circumstanțe, aceasta putând include, de asemenea, acordarea de compensații financiare. Detalii suplimentare privind controlul jurisdicțional în Regatul Unit sunt disponibile în publicația Departamentului juridic al Guvernului, intitulată *Judge Over Your Shoulder – a guide to good decision-making*, disponibilă la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf

privește garanțiile, toate autoritățile de aplicare a dreptului penal care intră în domeniul de aplicare al părții 3 din DPA din 2018, pot accesa datele cu caracter personal – care reprezintă o formă de prelucrare – numai înconformitate cu principiile și cerințele stabilite în DPA din 2018 (a se vedea considerentele 122 și 124). Prin urmare, o cerere formulată de orice autoritate de aplicare a legii ar trebui să respecte principiul conform căruia scopurile prelucrării trebuie să fie determinate, explicite și legitime ([188]), iar datele cu caracter personal prelucrate de o autoritate competentă trebuie să fie relevante în acest scop și neexcesive ([189]).

3.2.1.2. Competențe de investigare în scopuri de asigurare a respectării legii

(139) În scopul prevenirii sau depistării exclusiv al infracțiunilor grave ([190]), anumite autorități de aplicare a legii, de exemplu Agenția Națională pentru Combaterea Criminalității sau Chief of Police (șeful poliției) ([191]), pot utiliza competențe de investigare specifice în temeiul IPA din 2016. În acest caz, garanțiile prevăzute de IPA din 2016 se vor aplica în plus față de cele prevăzute în partea 3 din DPA din 2018. Competențele specifice de investigare pe care se pot baza aceste autorități de aplicare a legii sunt: interceptările țintite (partea 2 din IPA din 2016), achiziția datelor comunicațiilor (partea 3 din IPA din 2016), păstrarea datelor comunicațiilor (partea 4 din IPA din 2016) și intervenția țintită asupra echipamentelor (partea 5 din IPA din 2016). Interceptarea se referă la achiziția conținutului unei comunicații ([192]), în timp ce achiziția și păstrarea datelor comunicațiilor nu vizează obținerea conținutului comunicației, ci informațiile legate de „cine", „când", „unde" și „cum" referitoare la comunicație. Aceasta acoperă, de exemplu, ora și durata unei comunicații, numărul de telefon sau adresa de e-mail a inițiatorului și a destinatarului comunicației și, uneori, localizarea dispozitivelor de la care a fost efectuată comunicația, abonatul la un furnizor de servicii telefonice sau o factură detaliată ([193]). Intervenția asupra echipamentelor reprezintă un set de tehnici utilizate pentru a obține o varietate de date de la echipamente, care includ calculatoare, tablete și telefoane inteligente, precum și cabluri, fire și dispozitive de stocare ([194]).

(140) Competențele de interceptare țintită pot fi, de asemenea, utilizate atunci când acest lucru este „necesar în scopul punerii în aplicare a dispozițiilor unui instrument de asistență reciprocă al UE sau ale unui acord internațional de asistență reciprocă" (așa-numitul „mandat de asistență reciprocă" ([195])). Mandatele de asistență reciprocă sunt furnizate numai în ceea ce privește interceptarea, nu și achiziția de date ale comunicațiilor sau intervenția asupra echipamentelor. Aceste competențe țintite sunt reglementate în *Investigatory Powers Act 2016* (Legea din 2016 privind competențele de investigare) (IPA din 2016) ([196]) care, împreună cu *Regulation of Investigatory Powers Act 2000* (Legea din 2000 de reglementare a competențelor de investigare) (RIPA) pentru Anglia, Țara Galilor și Irlanda de Nord și cu *Regulation of Investigatory Powers (Scotland) Act 2000* [Legea din 2000 de reglementare a competențelor de investigare (Scoția)] (RIPSA) pentru Scoția, prevăd temeiul juridic și stabilesc limitările și garanțiile aplicabile pentru utilizarea acestor competențe. IPA din 2016 prevede, de asemenea, regimul pentru utilizarea competențelor de investigare în masă, deși acestea nu sunt la dispoziția autorităților de aplicare a legii (numai serviciile de informații le pot utiliza) ([197]).

([188]) Secțiunea 36 punctul 1 din DPA din 2018 al Regatului Unit.

([189]) Secțiunea 37 din DPA din 2018 al Regatului Unit.

([190]) Potrivit secțiunii 263 punctul 1 din IPA 2016, „infracțiune gravă" înseamnă o infracțiune pentru care se poate aștepta în mod rezonabil ca un adult, care nu a mai avut condamnări, să fie condamnat la pedeapsa cu închisoarea pentru o perioadă de cel puțin trei ani sau al cărui comportament implică utilizarea violenței, are ca rezultat un câștig financiar substanțial sau este un comportament al unui număr mare de persoane. În plus, în scopul achiziției de date ale comunicațiilor în temeiul părții 4 din IPA 2016, secțiunea 87 punctul 10B prevede că „infracțiune gravă" înseamnă o infracțiune pentru care poate fi impusă o pedeapsă cu închisoarea de cel puțin 12 luni sau o infracțiune săvârșită de o persoană care nu este persoană fizică, sau care implică, în cadrul acesteia, transmiterea unei comunicări sau încălcarea vieții private a unei persoane.

([191]) În special, următoarele autorități de aplicare a legii pot solicita un mandat de interceptare țintită: directorul general al Agenției Naționale pentru Combaterea Criminalității, Serviciul de poliție metropolitană, șeful Serviciului de poliție din Irlanda de Nord, șeful Serviciului de poliție din Scoția, Comisarul Administrației Fiscale și Vamale din Regatul Unit, șeful serviciului de informații în materie de apărare și o persoană care este o autoritate competentă a unei țări sau a unui teritoriu din afara Regatului Unit în sensul unui instrument de asistență reciprocă al UE sau al unui acord internațional de asistență reciprocă (secțiunea 18 punctul 1 din IPA din 2016).

([192]) A se vedea secțiunea 4 din IPA din 2016.

([193]) A se vedea secțiunea 261 punctul 5 din IPA din 2016 și Codul de bune practici privind achiziția în masă a datelor comunicațiilor, disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, punctul 2.9.

([194]) Codul de bune practici privind intervenția asupra echipamentelor (*Code of Practice on Equipment Interference*), disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, punctul 2.2.

([195]) Un mandat de asistență reciprocă autorizează o autoritate din Regatul Unit să ofere asistență unei autorități din afara teritoriului Regatului Unit pentru interceptarea și divulgarea materialelor interceptate către această autoritate, în conformitate cu un instrument internațional de asistență reciprocă (secțiunea 15 punctul 4 din IPA din 2016).

([196]) Legea din 2016 privind competențele de investigare (a se vedea: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) a înlocuit o legislație diferită privind interceptarea comunicațiilor, intervenția asupra echipamentelor și achiziția de date ale comunicațiilor, în special partea I din RIPA din 2000, care prevedea cadrul legislativ general anterior pentru utilizarea competențelor de investigare de către autoritățile de aplicare a legii și de securitate națională.

([197]) Secțiunea 138 punctul 1, secțiunea 158 punctul 1, secțiunea 178 punctul 1, secțiunea 199 punctul 1 din IPA din 2016.

(141) Pentru a exercita aceste competențe, autoritățile trebuie să obțină un mandat ([198]) emis de o autoritate competentă ([199]) și aprobat de un comisar judiciar independent ([200]) (așa-numita procedură de protecție dublă – „double-lock"). Obținerea unui astfel de mandat este supusă unui test de necesitate și proporționalitate ([201]). Întrucât aceste competențe de investigare țintite conferite de IPA din 2016 sunt identice celor de care dispun agențiile de securitate națională, condițiile, limitările și garanțiile aplicabile acestor competențe sunt abordate în detaliu în secțiunea privind accesul și utilizarea datelor cu caracter personal de către autoritățile publice ale Regatului Unit în scopuri de securitate națională (a se vedea considerentul 177 și următoarele).

3.2.2. *Utilizarea ulterioară a informațiilor colectate*

(142) Schimbul de date dintre o autoritate de aplicare a legii și o autoritate diferită în alte scopuri decât cele pentru care au fost colectate inițial (așa-numita „comunicare ulterioară") este supus anumitor condiții.

(143) În mod similar prevederilor de la articolul 4 alineatul (2) din Directiva (UE) 2016/680, secțiunea 36 punctul 3 din DPA din 2018 permite ca datele cu caracter personal colectate de o autoritate competentă în scopul asigurării respectării legii să poată fi prelucrate în continuare (fie de către operatorul inițial, fie de către un alt operator) în orice alt scop de asigurare a respectării legii, cu condiția ca operatorul să fie autorizat prin lege să prelucreze date în celălalt scop, iar prelucrarea să fie necesară și proporțională cu scopul respectiv ([202]). În acest caz, toate garanțiile prevăzute în partea 3 din DPA din 2018, menționate în considerentele 122 și 124, se aplică prelucrării efectuate de autoritatea destinatară.

(144) În ordinea juridică a Regatului Unit, diferite legi permit în mod explicit un astfel de transfer ulterior. În special: (i) Legea privind economia digitală din 2017 permite schimbul de informații între autoritățile publice în mai multe scopuri, de exemplu în cazul oricărei fraude asupra sectorului public care ar implica pierderi sau un risc de pierdere pentru autoritățile publice ([203]) sau în cazul unei datorii către o autoritate publică sau către Coroană ([204]); (ii) Legea privind criminalitatea și instanțele din 2013, care permite schimbul de informații cu Agenția Națională pentru Combaterea Criminalității (NCA – *National Crime Agency*) ([205]) pentru combaterea, investigarea și urmărirea penală a infracțiunilor grave și a criminalității organizate; (iii) Legea privind formele grave de criminalitate din 2007, care permite autorităților publice să divulge informații organizațiilor antifraudă în scopul prevenirii fraudei ([206]).

(145) Aceste legi prevăd în mod explicit că schimbul de informații ar trebui să fie în conformitate cu principiile stabilite în DPA din 2018. În plus, Colegiul de Poliție (*College of Policing*) a emis practici profesionale autorizate privind schimbul de informații (*Authorised Professional Practice on Information Sharing*) ([207]) pentru a ajuta poliția să își respecte obligațiile în materie de protecție a datelor în

([198]) Partea 2 capitolul 2 din IPA din 2016 prevede un număr limitat de cazuri în care interceptările pot fi efectuate fără mandat. Printre acestea se numără: interceptarea cu consimțământul expeditorului sau al destinatarului, interceptarea în scopuri administrative sau de asigurare a respectării legii, interceptarea care are loc în anumite instituții (închisori, spitale psihiatrice și centre de detenție pentru imigranți), precum și interceptarea efectuată în conformitate cu un acord internațional relevant.

([199]) În majoritatea cazurilor, secretarul de stat este autoritatea care emite mandatele în temeiul IPA din 2016, în timp ce miniștrii din Scoția sunt împuterniciți să emită mandate de interceptare țintită, mandate de asistență reciprocă și mandate pentru intervenția țintită asupra echipamentelor atunci când persoanele sau incintele care urmează să fie interceptate și echipamentele care urmează să fie exploatate sunt situate în Scoția (a se vedea secțiunile 22 și 103 din IPA din 2016). În cazul unei intervenții țintite asupra echipamentelor, un șef al autorității de aplicare a legii (descris în părțile 1 și 2 din anexa 6 la IPA din 2016) poate emite mandatul în condițiile prevăzute în secțiunea 106 din IPA din 2016.

([200]) Comisarii judiciari acordă asistență comisarului pentru competențe de investigare (IPC – *Investigatory Powers Commissioner*), un organism independent care exercită funcții de supraveghere a utilizării competențelor de investigare de către serviciile de informații (pentru mai multe detalii, a se vedea considerentul 162 și următoarele).

([201]) A se vedea, în special, secțiunile 19 și 23 din IPA din 2016.

([202]) Secțiunea 36 punctul 3 din DPA din 2018.

([203]) Secțiunea 56 din Legea privind economia digitală din 2017, disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2017/30/section/56

([204]) Secțiunea 48 din Digital Economy Act 2017 (Legea privind economia digitală din 2017).

([205]) Secțiunea 7 din Crime and Courts Act 2013 (Legea privind criminalitatea și instanțele din 2013), disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2013/22/section/7

([206]) Secțiunea 68 din *Serious Crime Act 2007* (Legea privind formele grave de criminalitate din 2007), disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2007/27/contents

([207]) Practici profesionale autorizate privind schimbul de informații, disponibile la următoarea adresă: https://www.app.college.police.uk/app-content/information-management/sharing-police-information

temeiul RGPD al Regatului Unit, al DPA și al Legii privind drepturile omului din 1998. Conformitatea schimbului de informații cu cadrul juridic aplicabil în materie de protecție a datelor este, desigur, supusă controlului jurisdicțional ([208]).

(146) În plus, în mod similar prevederilor de la articolul 9 din Directiva (UE) 2016/680, DPA din 2018 prevede că datele cu caracter personal colectate în orice scop de asigurare a respectării legii pot fi prelucrate într-un scop care nu este unul de asigurare a respectării legii atunci când prelucrarea este autorizată prin lege ([209]).

(147) Acest tip de schimb de informații se referă la două scenarii: 1. atunci când o autoritate de asigurare a respectării dreptului penal face schimb de date cu o autoritate de asigurare a respectării dreptului nepenal, alta decât o agenție de informații (cum ar fi, de exemplu, o autoritate financiară sau fiscală, o autoritate de concurență, un oficiu de asistență pentru bunăstarea tinerilor etc.); și 2. atunci când o autoritate de asigurare a respectării dreptului penal face schimb de date cu o agenție de informații. În primul scenariu, prelucrarea datelor cu caracter personal va intra sub incidența RGPD al Regatului Unit, precum și a părții 2 din DPA din 2018. Comisia a evaluat garanțiile prevăzute în RGPD al Regatului Unit și în partea 2 din DPA din 2018 în considerentele 12-111 și a ajuns la concluzia că Regatul Unit asigură un nivel adecvat de protecție a datelor cu caracter personal transferate în cadrul domeniului de aplicare al Regulamentului (UE) 2016/679 din Uniunea Europeană către Regatul Unit.

(148) În al doilea scenariu, în ceea ce privește schimbul de date colectate între o autoritate de asigurare a respectării dreptului penal și o agenție de informații în scopuri de securitate națională, temeiul juridic care autorizează un astfel de schimb este secțiunea 19 din *Counter Terrorism Act 2008* (Legea privind combaterea terorismului din 2008) (CTA din 2008) ([210]). În temeiul acestei legi, orice persoană poate furniza informații oricărui serviciu de informații în scopul îndeplinirii oricăreia dintre funcțiile serviciului respectiv, inclusiv „securitatea națională".

(149) În ceea ce privește condițiile în care datele pot fi partajate în scopuri de securitate națională, *Intelligence Services Act* (Legea privind serviciile de informații) ([211]) și *Security Service Act* (Legea privind serviciul de securitate) ([212]) limitează capacitatea serviciilor de informații de a obține date la ceea ce este necesar pentru îndeplinirea funcțiilor lor legale. Agențiile de aplicare a legii care doresc să facă schimb de date cu serviciile de informații vor trebui să ia în considerare o serie de factori/limitări, pe lângă funcțiile statutare ale agențiilor prevăzute în Legea privind serviciile de informații și în Legea privind serviciul de securitate ([213]). Secțiunea 20 din CTA din 2008 clarifică faptul că orice schimb de date în temeiul secțiunii 19 trebuie să respecte în continuare legislația privind protecția datelor; ceea ce înseamnă că se aplică toate limitările și cerințele prevăzute în partea 3 din DPA din 2018. În plus, întrucât autoritățile competente sunt autorități publice în sensul Legii privind drepturile omului din 1998, acestea trebuie să se asigure că acționează în conformitate cu drepturile conferite prin convenție, inclusiv cu articolul 8 din Convenția europeană a drepturilor omului. Aceste limite garantează faptul că toate schimburile de date dintre agențiile de aplicare a legii și serviciile de informații respectă legislația privind protecția datelor și Convenția europeană a drepturilor omului.

([208]) A se vedea, de exemplu, cauza *M, R/Chief Constable of Sussex Police* [2019] EWHC 975 (Admin), în care Înaltei Curți i s-a solicitat să analizeze schimbul de date dintre poliție și un parteneriat de reducere a criminalității din sectorul afacerilor (BCRP – *Business Crime Reduction Partnership*), o organizație abilitată să gestioneze sistemele de notificare de excludere, interzicând persoanelor să intre în spațiile comerciale ale membrilor săi. Instanța a examinat schimbul de date, care a avut loc pe baza unui acord având ca scop protejarea publicului și prevenirea criminalității și, în cele din urmă, a concluzionat că majoritatea aspectelor legate de schimbul de date sunt legale, cu excepția unor informații sensibile partajate între poliție și BCRP. Un alt exemplu este cauza *Cooper/NCA* [2019] EWCA Civ 16, în care Curtea de Apel a admis schimbul de date dintre poliție și Agenția pentru combaterea formelor grave de criminalitate organizată (SOCA – *Serious Organised Crime Agency*), o agenție de aplicare a legii care face parte în prezent din NCA.

([209]) Secțiunea 36 punctul 4 din DPA din 2018.

([210]) Legea din 2008 privind combaterea terorismului, disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2008/28/section/19

([211]) Legea privind serviciile de informații din 1994, disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/1994/13/contents

([212]) Legea privind serviciul de securitate din 1989, disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/1989/5/contents

([213]) Secțiunea 2 punctul 2 din Legea privind serviciile de informații din 1994 prevede următoarele: „Șeful Serviciului de Informații este responsabil de eficiența acestui serviciu, având datoria de a se asigura: (a) că există mecanisme pentru a garanta că Serviciul de Informații nu obține informații decât în măsura în care acest lucru este necesar pentru îndeplinirea corespunzătoare a funcțiilor sale și că nicio informație nu este divulgată de către acesta decât în măsura în care este necesar: (i) în acest scop; (ii) în interesul securității naționale; (iii) în scopul prevenirii sau depistării infracțiunilor grave; sau (iv) în scopul oricăror proceduri penale; și (b) că Serviciul de Informații nu ia nicio măsură pentru a promova interesele niciunui partid politic din Regatul Unit", în timp ce secțiunea 2 punctul 2 din Legea privind serviciile de securitate din 1989 prevede următoarele: „Directorul general este responsabil de eficiența Serviciului, având datoria de a se asigura: (a) că există mecanisme pentru a garanta că Serviciul nu obține informații decât în măsura în care acest lucru este necesar pentru îndeplinirea corespunzătoare a funcțiilor sale și că nicio informație nu este divulgată de către acesta decât în măsura în care este necesar în acest scop sau în scopul prevenirii sau depistării infracțiunilor grave sau în scopul oricăror proceduri penale; și (b) că Serviciul nu ia nicio măsură pentru a promova interesele niciunui partid politic; și (c) că există mecanisme, convenite cu directorul general al Agenției Naționale pentru Combaterea Criminalității, pentru coordonarea activităților Serviciului în temeiul secțiunii 1 punctul 4 din această lege cu activitățile forțelor de poliție, ale Agenției Naționale pentru Combaterea Criminalității și ale altor agenții de aplicare a legii".

(150) Atunci când o autoritate competentă intenționează să facă schimb de date cu caracter personal prelucrate în temeiul părții 3 din DPA din 2018 cu autoritățile de aplicare a legii dintr-o țară terță, se aplică anumite cerințe ([214]). În special, astfel de transferuri pot avea loc atunci când se bazează pe regulamentele privind caracterul adecvat al nivelului de protecție adoptate de secretarul de stat sau, în absența unor astfel de regulamente, trebuie asigurate garanții adecvate. Secțiunea 75 din DPA din 2018 prevede existența unor garanții adecvate în cazul în care sunt instituite printr-un instrument juridic obligatoriu pentru destinatarul vizat sau în cazul în care operatorul, după ce a evaluat toate circumstanțele legate de transferurile acestui tip de date cu caracter personal către țara terță sau către organizația internațională, concluzionează că există garanții adecvate pentru protejarea datelor.

(151) În cazul în care un transfer nu se bazează pe un regulament privind caracterul adecvat al nivelului de protecție sau pe garanții adecvate, acesta poate avea loc numai în anumite circumstanțe specificate, denumite „circumstanțe speciale" ([215]). Acest lucru este valabil atunci când transferul este necesar: (a) pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane; (b) pentru protejarea intereselor legitime ale persoanei vizate; (c) pentru prevenirea unei amenințări imediate și grave la adresa securității publice a unui stat membru sau a unei țări terțe; (d) în cazuri individuale, în oricare dintre scopurile de asigurare a respectării legii; sau (e) în cazuri individuale, în scopuri juridice (de exemplu, în legătură cu proceduri judiciare sau pentru obținerea de consultanță juridică). Se poate observa că literele (d) și (e) nu se aplică dacă drepturile și libertățile persoanei vizate prevalează asupra interesului public în ceea ce privește transferul. Acest set de circumstanțe corespunde situațiilor și condițiilor specifice care se califică drept „derogări" în temeiul articolului 38 din Directiva (UE) 2016/680.

(152) În plus, atunci când materialele obținute de autoritățile de aplicare a legii în temeiul unui mandat de autorizare a utilizării interceptării sau a intervențiilor asupra echipamentelor sunt predate unei țări terțe, IPA din 2016 impune garanții suplimentare. În special, o astfel de divulgare, definită ca „divulgare în străinătate", este permisă numai în cazul în care autoritatea emitentă consideră că există mecanisme specifice adecvate care limitează numărul de persoane cărora le sunt divulgate datele, măsura în care orice material este divulgat sau pus la dispoziție, precum și măsura în care oricare dintre materiale este copiat și numărul de copii realizate. În plus, autoritatea emitentă poate considera că sunt necesare mecanisme adecvate pentru a se asigura că fiecare copie a oricărei părți a materialelor respective este distrusă de îndată ce nu mai există motive relevante pentru păstrarea acesteia (dacă nu a fost distrusă mai devreme) ([216]).

(153) În cele din urmă, forme specifice de transferuri ulterioare din Regatul Unit către Statele Unite ar putea avea loc în viitor pe baza „Acordului dintre Guvernul Regatului Unit al Marii Britanii și Irlandei de Nord și Guvernul Statelor Unite ale Americii privind accesul la datele electronice în scopul combaterii formelor grave de criminalitate" („Acordul dintre Regatul Unit și SUA" sau „acordul") ([217]), încheiat în luna octombrie 2019 ([218]). Deși Acordul dintre Regatul Unit și SUA nu a intrat încă în vigoare la momentul adoptării prezentei decizii, intrarea sa previzibilă în vigoare poate afecta transferurile ulterioare către SUA de date transferate inițial către Regatul Unit în temeiul deciziei. Mai precis, datele transferate din UE către furnizorii de servicii din Regatul Unit ar putea face obiectul unor ordine de prezentare de probe electronice emise de autoritățile competente de aplicare a legii din SUA și puse în aplicare în Regatul Unit în temeiul acestui acord odată intrat în vigoare. Din aceste motive, evaluarea condițiilor și a garanțiilor în temeiul cărora pot fi emise și executate asemenea ordine este relevantă pentru prezenta decizie.

([214]) A se vedea partea 3 capitolul 5 din DPA din 2018.

([215]) Secțiunea 76 din DPA din 2018.

([216]) Secțiunile 54 și 130 din IPA din 2016. Autoritățile emitente trebuie să ia în considerare necesitatea de a impune garanții specifice materialelor predate autorităților străine, pentru a se asigura că datele fac obiectul unor garanții în ceea ce privește păstrarea, distrugerea și divulgarea datelor similare celor impuse în secțiunile 53 și 129 din IPA din 2016.

([217]) Acord între Guvernul Regatului Unit al Marii Britanii și Irlandei de Nord și Guvernul Statelor Unite ale Americii privind accesul la datele electronice în scopul combaterii formelor grave de criminalitate, disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

([218]) Acesta este primul acord încheiat în temeiul *US Clarifying Lawful Overseas Use of Data (CLOUD) Act* [Legea SUA privind clarificarea utilizării legale a datelor în străinătate (CLOUD)]. Legea CLOUD din Statele Unite este o lege federală a SUA care a fost adoptată la 23 martie 2018 și care precizează printr-o modificare a *Stored Communications Act* (Legea privind comunicațiile stocate) din 1986 că prestatorii de servicii din SUA au obligația de a da curs ordinelor SUA de divulgare a datelor referitoare la conținut și a datelor care nu se referă la conținut, indiferent de locul în care sunt stocate aceste date. De asemenea, Legea CLOUD permite încheierea de acorduri executive cu guvernele străine, în baza cărora prestatorii de servicii din Statele Unite să poată să furnizeze datele referitoare la conținut direct acestor guverne străine (textul Legii CLOUD este disponibil la următoarea adresă: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

(154) În acest sens, ar trebui remarcat faptul că, în primul rând, în ceea ce privește domeniul său de aplicare material, acordul se aplică numai infracțiunilor care sunt pasibile de sancțiuni privative de libertate având o durată maximă de cel puțin trei ani (definite drept „infracțiuni grave") ([219]), inclusiv „activitate teroristă". În al doilea rând, datele prelucrate în cealaltă jurisdicție pot fi obținute în temeiul acestui acord numai în urma unui „ordin [...] supus revizuirii sau supravegherii în temeiul dreptului intern al părții emitente de către o instanță, un judecător, un magistrat sau o altă autoritate independentă înainte sau în cadrul procedurilor de executare a ordinului" ([220]). În al treilea rând, orice ordin trebuie „să se bazeze pe cerințe privind o justificare rezonabilă bazată pe fapte concrete și credibile, pe particularitate, legalitate și gravitate în ceea ce privește comportamentul care face obiectul investigației" ([221]) și „să vizeze conturi specifice, precum și să identifice o anumită persoană, un anumit cont, o anumită adresă sau un anumit dispozitiv personal sau orice alt element de identificare specific" ([222]). În al patrulea rând, datele obținute în temeiul acestui acord beneficiază de măsuri de protecție echivalente cu garanțiile specifice prevăzute de așa-numitul „Acord-cadru UE-SUA" ([223]) – un acord cuprinzător privind protecția datelor, încheiat în decembrie 2016 între UE și SUA și care stabilește garanțiile și drepturile aplicabile transferurilor de date în domeniul cooperării în materie de asigurare a respectării legii – care sunt toate încorporate în acest acord prin trimitere, *mutatis mutandis*, pentru a ține seama în special de natura specifică a transferurilor (și anume transferurile de la operatorii privați către o autoritate de aplicare a legii, mai degrabă decât transferurile între autoritățile de aplicare a legii) ([224]). Acordul dintre Regatul Unit și SUA prevede în mod expres aplicarea de măsuri de protecție echivalente celor prevăzute de Acordul-cadru UE-SUA „tuturor informațiilor cu caracter personal furnizate în cursul executării ordinelor care fac obiectul acordului pentru a furniza măsuri de protecție echivalente" ([225]).

(155) Datele transferate autorităților din SUA în temeiul Acordului dintre Regatul Unit și SUA ar trebui, prin urmare, să beneficieze de măsurile de protecție prevăzute de un instrument legislativ al UE, cu adaptările necesare pentru a reflecta natura transferurilor în cauză. Autoritățile Regatului Unit au confirmat, de asemenea, că măsurile de protecție din acordul-cadru se vor aplica tuturor informațiilor cu caracter personal furnizate sau păstrate în temeiul acordului, indiferent de natura sau tipul organismului care formulează cererea (de exemplu, atât autoritățile federale, cât și cele statale de aplicare a legii din SUA), astfel încât trebuie să se asigure o protecție echivalentă în toate cazurile. Cu toate acestea, autoritățile Regatului Unit au explicat, de asemenea, că detaliile punerii în aplicare concrete a garanțiilor privind protecția datelor fac încă obiectul discuțiilor dintre Regatul Unit și SUA. În contextul discuțiilor cu serviciile Comisiei Europene cu privire la această decizie, autoritățile Regatului Unit au confirmat că vor permite intrarea în vigoare a acordului numai după ce se asigură că punerea sa în aplicare respectă obligațiile legale prevăzute în acesta, inclusiv claritatea în ceea ce privește respectarea standardelor de protecție a datelor pentru orice date solicitate în temeiul acestui acord. Întrucât o posibilă intrare în vigoare a acordului poate avea un impact asupra nivelului de protecție evaluat în prezenta decizie, orice informații și clarificare viitoare cu privire la modul în care SUA își va respecta obligațiile care îi revin în temeiul acordului ar trebui să fie comunicată Comisiei Europene de către Regatul Unit, de îndată ce va fi disponibilă și, în orice caz, înaintea intrării în vigoare a acordului, pentru a asigura monitorizarea corespunzătoare a acestei decizii în conformitate cu articolul 45 alineatul (4) din Regulamentul (UE) 2016/679. Se va acorda o atenție deosebită aplicării și adaptării măsurilor de protecție din acordul-cadru la tipul specific de transferuri reglementate de Acordul dintre Regatul Unit și SUA.

(156) La un nivel mai general, orice evoluție relevantă în ceea ce privește intrarea în vigoare și aplicarea acordului va fi luată în considerare în mod corespunzător în contextul monitorizării continue a prezentei decizii, inclusiv în ceea ce privește consecințele necesare care trebuie deduse în cazul în care există indicii că nu mai este asigurat un nivel de protecție echivalent în esență.

3.2.3. *Supravegherea*

(157) În funcție de competențele utilizate de autoritățile competente atunci când prelucrează date cu caracter personal în scopuri de asigurare a respectării legii (fie în temeiul DPA din 2018, fie în temeiul IPA din 2016), diferite organisme asigură supravegherea utilizării acestor competențe. În special, comisarul pentru informații supraveghează

([219]) Articolul 1 alineatul (14) din acord.
([220]) Articolul 5 alineatul (2) din acord.
([221]) Articolul 5 alineatul (1) din acord.
([222]) Articolul 4 alineatul (5) din acord. În ceea ce privește interceptarea în timp real, se aplică un standard suplimentar mai strict: ordinele trebuie să aibă o durată limitată, care să nu depășească ceea ce este în mod rezonabil necesar pentru îndeplinirea scopurilor ordinului, și se emit numai în cazul în care aceleași informații nu au putut fi obținute în mod rezonabil printr-o metodă mai puțin intruzivă [articolul 5 alineatul (3) din acord].
([223]) Acord între Statele Unite ale Americii și Uniunea Europeană privind protecția informațiilor cu caracter personal în ceea ce privește prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor, JO L 336, 10.12.2016, p. 3, disponibil la următoarea adresă: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN
([224]) Articolul 9 alineatul (1) din acord.
([225]) Articolul 9 alineatul (1) din acord.

prelucrarea de date cu caracter personal atunci când aceasta intră în domeniul de aplicare al părții 3 din DPA din 2018 ([226]). Supravegherea judiciară independentă a utilizării competențelor de investigare în temeiul IPA din 2016 este asigurată de Biroul comisarului pentru competențe de investigare (IPCO – *Investigatory Powers Commissioner's Office*) ([227]) (această parte este abordată în considerentele 250-255). În plus, o supraveghere suplimentară este garantată atât de Parlament, cât și de alte organisme.

3.2.3.1. Supravegherea părții 3 din DPA din 2018

(158) Funcțiile generale ale comisarului pentru informații – ale cărui independență și organizare sunt explicate în considerentul 87 – în ceea ce privește prelucrarea datelor cu caracter personal care intră sub incidența părții 3 din DPA din 2018 sunt prevăzute în anexa 13 la DPA din 2018. Principala sarcină a ICO este de a monitoriza și de a pune în aplicare partea 3 din DPA din 2018, precum și de a promova acțiuni de sensibilizare în rândul publicului și de a oferi consiliere Parlamentului, Guvernului și altor instituții și organisme. Pentru a menține independența sistemului judiciar, comisarul pentru informații nu este autorizat să își exercite funcțiile în legătură cu prelucrarea datelor cu caracter personal de către o persoană care acționează în exercițiul unei funcții judiciare sau de către o instanță sau tribunal care acționează în exercițiul funcției sale judiciare. În aceste circumstanțe, alte organisme ar exercita funcțiile de supraveghere, astfel cum se explică în considerentele 99-103.

(159) Comisarul are competențe generale de investigare, de corecție, de autorizare și de consiliere în ceea ce privește prelucrarea datelor cu caracter personal, cărora li se aplică partea 3. În special, comisarul are competența de a notifica operatorul sau persoana împuternicită de operator cu privire la o presupusă încălcare a părții 3 din DPA din 2018, de a emite avertismente sau o mustrare unui operator sau unei persoane împuternicite de operator care a încălcat dispozițiile părții 3 din lege, precum și de a emite, din proprie inițiativă sau la cerere, avize adresate Parlamentului, Guvernului sau altor instituții și organisme, precum și publicului cu privire la orice aspect legat de protecția datelor cu caracter personal ([228]).

(160) În plus, comisarul are competența de a emite notificări de informare ([229]), notificări de evaluare ([230]) și notificări de executare ([231]), precum și competența de a accesa documentele operatorilor și ale persoanelor împuternicite de operatori, de a avea acces la sediile acestora ([232]) și de a aplica amenzi administrative sub forma unor notificări de sancționare ([233]). Politica ICO privind acțiunile de reglementare stabilește circumstanțele în care acesta emite o notificare de informare, de evaluare, de executare sau, respectiv, de sancționare ([234]) [a se vedea, de asemenea, considerentul 93 și considerentele 101-102 din Directiva (UE) 2016/680 cu privire la decizia privind caracterul adecvat al nivelului de protecție].

(161) Conform ultimelor sale rapoarte anuale [2018-2019 ([235]), 2019-2020 ([236])], comisarul pentru informații a efectuat o serie de investigații și a luat măsuri de asigurare a respectării legii în ceea ce privește prelucrarea datelor de către autoritățile de aplicare a legii. De exemplu, comisarul a efectuat o investigație și a publicat un aviz în octombrie 2019 în ceea ce privește utilizarea de către autoritățile de aplicare a legii a tehnologiei de recunoaștere facială în locuri publice. Investigația s-a axat, în special, pe utilizarea capacităților de recunoaștere facială în direct de către poliția din sudul Țării Galilor și de către Serviciul de poliție metropolitană (MPS). Comisarul pentru informații a investigat, de asemenea, baza de date „Gangs Matrix" a MPS ([237]) și a constatat o serie de încălcări grave ale legislației privind protecția datelor, care erau de natură să submineze încrederea publicului în baza de date și în modul în care erau utilizate datele. În noiembrie 2018, comisarul pentru informații a emis o notificare de executare, iar ulterior MPS a luat măsurile necesare pentru a spori securitatea și

([226]) Secțiunea 116 din DPA din 2018.
([227]) A se vedea IPA din 2016, în special capitolul 1 partea 8.
([228]) Punctul 2 din anexa 13 la DPA din 2018.
([229]) Care obligă operatorul și persoana împuternicită de operator (și, în anumite circumstanțe, orice altă persoană) să furnizeze informațiile necesare (secțiunea 142 din DPA din 2018).
([230]) Care permite desfășurarea investigațiilor și a auditului, care pot impune operatorului sau persoanei împuternicite de operator să permită comisarului să intre în incinte specificate, să inspecteze sau să examineze documente sau echipamente, să intervieveze persoane care prelucrează date cu caracter personal în numele operatorului (secțiunea 146 din DPA din 2018).
([231]) Care permite exercitarea de competențe corective, ceea ce impune operatorilor/persoanelor împuternicite de operatori să întreprindă sau să se abțină de la a întreprinde anumite măsuri (secțiunea 149 din DPA din 2018).
([232]) Secțiunea 154 din DPA din 2018.
([233]) Secțiunea 155 din DPA din 2018.
([234]) Politica privind acțiunile de reglementare, a se vedea nota de subsol 96.
([235]) Raportul anual și Situațiile financiare pe 2018-2019 ale comisarului pentru informații, a se vedea nota de subsol 101.
([236]) Raportul anual și Situațiile financiare pe 2019-2020 ale comisarului pentru informații, a se vedea nota de subsol 82.
([237]) O bază de date care a înregistrat informații referitoare la presupuși membri ai unor grupări criminale și la victimele infracțiunilor săvârșite de grupări criminale.

responsabilitatea și pentru a se asigura că datele sunt utilizate în mod proporțional. Un alt exemplu de acțiune de asigurare a respectării legii în acest domeniu este amenda de 325 000 GBP aplicată ministerului public de către comisar în luna mai 2018, pentru pierderea unor DVD-uri necriptate care conțineau înregistrări ale interogatoriilor efectuate de poliție. Comisarul pentru informații a desfășurat, de asemenea, investigații cu privire la subiecte mai ample, de exemplu în prima jumătate a anului 2020, cu privire la utilizarea criminalisticii mobile în scopuri polițienești și la prelucrarea datelor victimelor de către poliție. În plus, comisarul investighează în prezent un caz care implică accesul autorităților de aplicare a legii la datele deținute de o entitate din sectorul privat, Clearview AI Inc. ([238]).

(162) Pe lângă competențele comisarului pentru informații în materie de asigurare a respectării legii, menționate în considerentele 160 și 161, anumite încălcări ale legislației privind protecția datelor constituie infracțiuni și, prin urmare, pot face obiectul unor sancțiuni penale (secțiunea 196 din DPA din 2018). Acest lucru se aplică, de exemplu, obținerii, divulgării sau păstrării datelor cu caracter personal fără consimțământul operatorului și cauzării divulgării datelor cu caracter personal unei alte persoane fără consimțământul operatorului ([239]); reidentificării informațiilor care sunt date cu caracter personal anonimizate fără consimțământul operatorului responsabil de anonimizarea datelor cu caracter personal ([240]); împiedicării intenționate a comisarului de a-și exercita competențele în ceea ce privește examinarea datelor cu caracter personal în conformitate cu obligațiile internaționale ([241]), prezentării de declarații false ca răspuns la o notificare de informare sau distrugerii informațiilor în legătură cu notificările de informare și de evaluare ([242]).

3.2.3.2. Alte organisme de supraveghere în domeniul asigurării respectării dreptului penal

(163) Pe lângă comisarul pentru informații, există mai multe organisme de supraveghere în domeniul asigurării respectării dreptului penal, cu mandate specifice relevante pentru aspecte legate de protecția datelor. Printre acestea se numără, de exemplu, comisarul pentru păstrarea și utilizarea materialelor biometrice (denumit în continuare „comisarul pentru biometrie") ([243]) și comisarul pentru camere de supraveghere ([244]).

3.2.3.3. Supravegherea parlamentară în domeniul asigurării respectării dreptului penal

(164) Comisia specială pentru afaceri interne (HASC – *Home Affairs Select Committee*) asigură supravegherea parlamentară în domeniul asigurării respectării legii. Această comisie este alcătuită din 11 membri ai Parlamentului, aleși din cele mai mari trei partide politice. Comisia are sarcina de a analiza cheltuielile, administrarea și politica Ministerului de Interne și ale organismelor publice asociate, și anume poliția și NCA – a căror activitate poate fi verificată în mod specific de către comisie ([245]).

([238]) A se vedea declarația ICO, disponibilă la următoarea adresă: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc

([239]) Secțiunea 170 din DPA din 2018.

([240]) Secțiunea 171 din DPA din 2018.

([241]) Secțiunea 119 punctul 6 din DPA din 2018.

([242]) În cursul exercițiului financiar care acoperă perioada cuprinsă între 1 aprilie 2019 și 31 martie 2020, investigațiile ICO au avut ca rezultat patru avertismente și opt urmăriri penale. Aceste cazuri au făcut obiectul urmăririi penale în temeiul secțiunii 55 din Legea privind protecția datelor din 1998, al secțiunii 77 din Legea din 2000 privind liberul acces la informațiile de interes public și al secțiunii 170 din Legea privind protecția datelor din 2018. În 75 % din cazuri, inculpații și-au recunoscut vinovăția, negând necesitatea unor procese prelungite cu costurile aferente. (Raportul anual și Situațiile financiare pe 2019/2020 ale comisarului pentru informații, a se vedea nota de subsol 87, pagina 40).

([243]) Comisarul pentru biometrie a fost instituit prin *Protection of Freedoms Act 2012* (Legea din 2012 privind apărarea libertăților) (a se vedea: https://www.legislation.gov.uk/ukpga/2012/9/contents). Printre alte funcții, comisarul pentru biometrie decide dacă poliția poate păstra sau nu înregistrările profilurilor ADN și amprentele digitale obținute de la persoanele arestate, dar care nu sunt acuzate de o infracțiune calificată (secțiunea 63G din PACE din 1984). În plus, comisarul pentru biometrie are responsabilitatea generală de a supraveghea păstrarea și utilizarea ADN-ului și a amprentelor digitale, precum și păstrarea din motive de securitate națională (secțiunea 20 punctul 2 din PoFA din 2012). Comisarul pentru biometrie este numit în temeiul Codului privind numirile publice (codul este disponibil la următoarea adresă: https://www.gov.uk/government/publications/governance-code-for-public-appointments), iar condițiile numirii sale indică în mod clar faptul că acesta poate fi demis din funcție de către ministrul de interne numai în anumite circumstanțe definite în mod strict; printre acestea se numără neexercitarea atribuțiilor sale pentru o perioadă de trei luni, condamnarea pentru săvârșirea unei infracțiuni sau nerespectarea condițiilor numirii sale.

([244]) Comisarul pentru camere de supraveghere a fost instituit prin Legea din 2012 privind apărarea libertăților și are rolul de a încuraja respectarea Codului de bune practici referitoare la camerele de supraveghere; de a revizui modul de funcționare a codului menționat; și de a oferi consiliere miniștrilor cu privire la necesitatea modificării acestui cod. Comisarul este numit în conformitate cu aceleași norme ca și Comisarul pentru biometrie și se bucură de aceleași competențe, resurse și protecție împotriva îndepărtării.

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

(165) În limitele competențelor sale, comisia își poate alege propria temă de anchetă, inclusiv cazurile specifice, atâta timp cât chestiunea nu este *sub judice*. Comisia poate, de asemenea, să solicite probe scrise și orale de la o gamă largă de grupuri și persoane relevante. Aceasta elaborează rapoarte cu privire la constatările sale și emite recomandări adresate Guvernului ([246]). Se așteaptă ca Guvernul să răspundă fiecărei recomandări din raport și trebuie să facă acest lucru în termen de 60 de zile ([247]).

(166) În domeniul supravegherii, comisia a elaborat, de asemenea, un raport referitor la Legea din 2000 de reglementare a competențelor de investigare) (RIPA din 2000) ([248]), în care s-a constatat că RIPA din 2000 nu este adecvată scopului. Raportul comisiei a fost luat în considerare în cadrul înlocuirii unor părți semnificative din RIPA din 2000 cu IPA din 2016. Lista completă a anchetelor poate fi consultată pe site-ul comisiei ([249]).

(167) Sarcinile HASC sunt îndeplinite în Scoția de către Subcomisia pentru justiție în domeniul polițienesc și, în Irlanda de Nord, de către Comisia pentru justiție ([250]).

3.2.4. *Căi de atac*

(168) În ceea ce privește prelucrarea datelor de către autoritățile de aplicare a legii, sunt disponibile mecanisme de exercitare a unei căi de atac în temeiul părții 3 din DPA din 2018 și al IPA din 2016, precum și în temeiul Legii privind drepturile omului din 1998.

(169) Această serie de mecanisme oferă persoanelor vizate căi de atac administrative și judiciare eficace care le permit, în special, să își asigure drepturile, inclusiv dreptul de a avea acces la datele lor cu caracter personal sau de a obține rectificarea sau ștergerea acestor date.

(170) În primul rând, în temeiul secțiunii 165 din DPA din 2018, o persoană vizată are dreptul de a depune o plângere la comisarul pentru informații în cazul în care persoana vizată consideră că, în ceea ce privește datele cu caracter personal care o privesc, există o încălcare a părții 3 din DPA din 2018 ([251]). Comisarul pentru informații are competența de a evalua conformitatea operatorului și a persoanei împuternicite de operator cu DPA din 2018, de a le solicita să ia măsurile necesare în caz de neconformitate și de a aplica amenzi.

([246]) Comisiile speciale, inclusiv Comisia specială pentru afaceri interne, fac obiectul Regulamentului de procedură al Camerei Comunelor. Regulamentul de procedură reprezintă normele, convenite de Camera Comunelor, care reglementează modul în care Parlamentul își desfășoară activitatea. Competența comisiilor speciale este extinsă, iar articolul 152 alineatul (1) din Regulamentul de procedură prevede că „se numesc comisii speciale pentru a analiza cheltuielile, administrarea și politica principalelor departamente ministeriale, astfel cum se prevede la alineatul (2) din prezentul regulament, precum și ale organismelor publice asociate". Acest lucru permite Comisiei speciale pentru afaceri interne să analizeze orice politică a Ministerului de Interne, care include politici (și legislația aferentă) privind competențele de investigare. În plus, articolul 152 alineatul (4) din Regulamentul de procedură prevede în mod clar diferitele competențe ale comisiilor, inclusiv capacitatea de a solicita persoanelor să furnizeze probe sau documente cu privire la o anumită chestiune și să elaboreze rapoarte. Anchetele actuale și anterioare ale comisiei sunt disponibile la următoarea adresă: https://committees.parliament.uk/committee/83/home-affairs-committee

([247]) Competențele Comisiei speciale pentru afaceri interne din Anglia și Țara Galilor sunt stabilite în Regulamentul de procedură al Camerei Comunelor, disponibil la următoarea adresă: https://www.parliament.uk/business/publications/commons/standing-orders-public11

([248]) Disponibil la următoarea adresă: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm

([249]) Disponibil la următoarea adresă: https://committees.parliament.uk/committee/83/home-affairs-committee

([250]) Regulamentul Subcomisiei pentru justiție în domeniul polițienesc din Scoția este disponibil la următoarea adresă: https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx, iar regulamentul Comisiei pentru justiție din Irlanda de Nord este disponibil la următoarea adresă: http://www.niassembly.gov.uk/assembly-business/standing-orders

([251]) Ultimul raport anual al ICO prezintă o defalcare a naturii plângerilor primite și clasate. În special, numărul plângerilor primite cu privire la „evidențele poliției și cazierele judiciare" se ridică la 6 % din numărul total de plângeri primite (cu o creștere de 1 % față de exercițiul financiar precedent). Raportul anual arată, de asemenea, că plângerile referitoare la cererile de acces ale persoanelor vizate reprezintă cel mai mare număr (46 % din numărul total de plângeri, cu o creștere de 8 % față de exercițiul financiar precedent) (Raportul anual al ICO pe 2019-2020, pagina 55; a se vedea nota de subsol 88).

(171) În al doilea rând, DPA din 2018 prevede dreptul la o cale de atac împotriva comisarului pentru informații dacă acesta nu tratează în mod corespunzător o plângere depusă de persoana vizată. Mai precis, în cazul în care comisarul nu „înregistrează progrese” ([252]) în ceea ce privește o plângere depusă de persoana vizată, reclamantul are acces la o cale de atac judiciară, deoarece acesta se poate adresa unui tribunal de primă instanță ([253]) pentru a obliga comisarul să ia măsurile adecvate pentru a răspunde plângerii sau pentru a informa reclamantul cu privire la progresele înregistrate cu privire la plângere ([254]). În plus, orice persoană căreia i se transmite oricare dintre notificările menționate (notificare de informare, de evaluare, de executare sau de sancționare) din partea comisarului poate introduce o cale de atac în fața unui tribunal de primă instanță. În cazul în care tribunalul consideră că decizia comisarului nu este conformă cu legea sau că, în ceea ce privește comisarul pentru informații, acesta ar fi trebuit să își exercite puterea de apreciere în mod diferit, tribunalul trebuie să admită calea de atac sau să înlocuiască o altă notificare sau decizie pe care comisarul pentru informații ar fi putut să o emită sau să o adopte ([255]).

(172) În al treilea rând, persoanele fizice pot introduce o cale de atac împotriva operatorilor și a persoanelor împuternicite de operatori direct în fața instanțelor. În special, în temeiul secțiunii 167 din DPA din 2018, o persoană vizată poate depune o cerere în fața instanței pentru încălcarea dreptului său în temeiul legislației privind protecția datelor, iar instanța poate solicita operatorului, prin intermediul unui ordin judecătoresc, să întreprindă (sau să se abțină de la a întreprinde) orice măsură în ceea ce privește prelucrarea pentru a se conforma DPA din 2018. În plus, în temeiul secțiunii 169 din DPA din 2018, orice persoană care a suferit un prejudiciu din cauza unei încălcări a unei cerințe prevăzute de legislația privind protecția datelor (inclusiv partea 3 din DPA din 2018), alta decât RGPD al Regatului Unit, are dreptul la despăgubiri din partea operatorului sau a persoanei împuternicite de operator pentru prejudiciul respectiv, cu excepția cazului în care operatorul sau persoana împuternicită de operator dovedește că operatorul sau persoana împuternicită de operator nu este responsabilă în niciun fel pentru evenimentul care a cauzat prejudiciul. Prejudiciul include atât pierderi financiare, cât și prejudicii care nu implică pierderi financiare, cum ar fi suferințele clinice.

(173) În cele din urmă, orice persoană, în măsura în care consideră că drepturile sale, inclusiv dreptul la viață privată și la protecția datelor, au fost încălcate de orice autorități publice, poate obține reparații în fața instanțelor din Regatul Unit în temeiul Legii privind drepturile omului din 1998 ([256]) și, după epuizarea căilor de atac naționale, o persoană fizică, o organizație neguvernamentală și grupuri de particulari pot obține reparații în fața Curții Europene a Drepturilor Omului pentru încălcarea drepturilor garantate în temeiul Convenției europene a drepturilor omului ([257]) (a se vedea considerentul 111).

3.2.4.1. Mecanisme de exercitare a unei căi de atac disponibile în cadrul IPA din 2016

(174) Persoanele fizice pot obține reparații pentru încălcări ale IPA din 2016 în fața Tribunalului cu competențe de investigare. Căile de atac disponibile în cadrul IPA din 2016 sunt descrise în considerentele 263-269.

([252]) Secțiunea 166 din DPA din 2018 se referă în mod specific la următoarele situații: (a) comisarul nu ia măsurile adecvate pentru a răspunde plângerii; (b) comisarul nu furnizează reclamantului informații cu privire la evoluția plângerii sau la rezultatul acesteia înainte de sfârșitul perioadei de trei luni care începe în momentul în care comisarul a primit plângerea; sau (c) în cazul în care examinarea plângerii de către comisar nu este finalizată în perioada respectivă, acesta nu furnizează reclamantului astfel de informații în cursul unei perioade ulterioare de trei luni.

([253]) Tribunalul de primă instanță este instanța competentă să soluționeze căile de atac introduse împotriva deciziilor luate de organismele de reglementare guvernamentale. În cazul deciziei comisarului pentru informații, camera competentă este „General Regulatory Chamber”, care are jurisdicție asupra întregului teritoriu al Regatului Unit.

([254]) Secțiunea 166 din DPA din 2018. Exemple de acțiuni de succes introduse împotriva ICO în fața tribunalului includ o cauză în care ICO a confirmat primirea unei plângeri din partea unei persoane vizate, dar nu a indicat ce măsuri intenționa să adopte și, prin urmare, a fost obligat să confirme, în termen de 21 de zile calendaristice, dacă va investiga plângerile și, în caz afirmativ, să informeze reclamantul cu privire la evoluția investigației cel puțin la fiecare 21 de zile calendaristice după aceea (hotărârea nu a fost încă publicată) și o cauză în care tribunalul de primă instanță a considerat că este neclar dacă răspunsul ICO adresat unui reclamant constituie în mod adecvat „rezultatul” plângerii (a se vedea *Susan Milne/The Information Commissioner* [2020], hotărâre disponibilă la următoarea adresă: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

([255]) Secțiunile 162 și 163 din DPA din 2018.

([256]) A se vedea, de exemplu, cauza *Brown/Commissioner of Police of the Metropolis & Anor* [2019] EWCA Civ 1724, în care au fost acordate despăgubiri în valoare de 9 000 GBP în temeiul DPA din 1998 și al Legii privind drepturile omului din 1998 pentru obținerea și utilizarea abuzivă ilegală a informațiilor cu caracter personal, și cauza *R (on the application of Bridges)/Chief Constable of South Wales* [2020] EWCA Civ 1058, în care Curtea de Apel a declarat ilegală implementarea unui sistem de recunoaștere facială de către poliția din Țara Galilor, întrucât acesta a încălcat articolul 8 din Convenția europeană a drepturilor omului, iar evaluarea impactului asupra protecției datelor realizată de operator nu a respectat DPA din 2018.

([257]) Articolul 34 din Convenția europeană a drepturilor omului prevede următoarele: „Curtea poate fi sesizată, printr-o cerere, de orice persoană fizică, organizație neguvernamentală sau grup de particulari care se pretind victime ale unei încălcări de către una dintre Înaltele Părți Contractante a drepturilor recunoscute în Convenție sau în Protocoalele sale. Înalta Parte Contractantă se angajează să nu împiedice prin nicio măsură exercițiul eficace al acestui drept”.

3.3. **Accesul și utilizarea de către autoritățile publice din Regatul Unit în scopuri de securitate națională**

(175) În ordinea juridică a Regatului Unit, serviciile de informații abilitate să colecteze informații electronice deținute de operatori sau de persoane împuternicite de operatori din motive de securitate națională, în situații relevante pentru un scenariu privind caracterul adecvat, sunt Serviciul de Securitate ([258]) (MI5), Serviciul Secret de Informații ([259]) (SIS) și Cartierul General pentru Comunicații ([260]) (GCHQ) ([261]).

3.3.1. *Temeiuri juridice, limitări și garanții*

(176) În Regatul Unit, competențele agențiilor de informații sunt stabilite în IPA din 2016 și în RIPA din 2000, care, împreună cu DPA din 2018, definesc domeniul de aplicare material și personal al acestor competențe, precum și limitările și garanțiile pentru utilizarea acestora. Aceste competențe, precum și limitările și garanțiile aplicabile acestora, sunt evaluate în detaliu în secțiunile următoare.

3.3.1.1. Competențe de investigare exercitate în contextul securității naționale

(177) IPA din 2016 prevede cadrul juridic pentru utilizarea competențelor de investigare, și anume competența de a intercepta, de a accesa date ale comunicațiilor și de a efectua intervenții asupra echipamentelor. IPA din 2016 introduce o interdicție generală și stabilește ca infracțiune utilizarea unor tehnici care permit accesul la conținutul comunicațiilor, accesul la datele comunicațiilor sau intervenția asupra echipamentelor fără o autorizație legală ([262]). Acest lucru se reflectă în faptul că exercitarea acestor competențe de investigare este legală numai atunci când este efectuată pe baza unui mandat sau a unei autorizații ([263]).

(178) IPA din 2016 stabilește norme detaliate care reglementează domeniul de aplicare și aplicarea fiecărei competențe de investigare, precum și limitările și garanțiile specifice ale acestora. Se aplică norme diferite în funcție de tipul de competență de investigare (interceptarea comunicațiilor, achiziția și păstrarea datelor

([258]) MI5 se află sub autoritatea ministrului de interne. Legea privind serviciul de securitate din 1989 stabilește funcțiile MI5: protejarea securității naționale (inclusiv protecția împotriva amenințărilor reprezentate de spionaj, terorism și sabotaj, de activitățile agenților puterilor străine și de acțiunile menite să răstoarne sau să submineze democrația parlamentară prin mijloace politice, industriale sau violente), protejarea bunăstării economice a Regatului Unit împotriva amenințărilor externe și sprijinirea activităților forțelor de poliție și ale altor agenții de aplicare a legii în prevenirea și depistarea infracțiunilor grave.

([259]) SIS se află sub autoritatea ministrului afacerilor externe, iar funcțiile sale sunt prevăzute în Legea privind serviciile de informații din 1994. Funcțiile sale sunt de a obține și de a furniza informații cu privire la acțiunile sau intențiile persoanelor din afara Insulelor Britanice și de a îndeplini alte sarcini legate de acțiunile sau intențiile acestor persoane. Aceste funcții pot fi exercitate numai în interesul securității naționale, în interesul bunăstării economice a Regatului Unit sau în sprijinul prevenirii sau depistării infracțiunilor grave.

([260]) GCHQ se află sub autoritatea ministrului afacerilor externe, iar funcțiile sale sunt prevăzute în Legea privind serviciile de informații din 1994. Acestea sunt: (a) să monitorizeze, să utilizeze sau să efectueze intervenții asupra emisiilor electromagnetice și de altă natură și a echipamentelor care produc astfel de emisii, să obțină și să furnizeze informații provenite din sau legate de astfel de emisii sau echipamente și din materiale criptate; (b) să ofere consiliere și asistență cu privire la limbi, inclusiv terminologia utilizată în chestiuni tehnice și criptografie, precum și la alte aspecte legate de protecția informațiilor destinate forțelor armate, guvernului sau altor organizații sau persoane considerate adecvate. Aceste funcții pot fi exercitate numai în interesul securității naționale, în interesul bunăstării economice a Regatului Unit în ceea ce privește acțiunile sau intențiile persoanelor din afara Insulelor Britanice sau în sprijinul prevenirii sau depistării infracțiunilor grave.

([261]) Alte organisme publice care exercită funcții relevante pentru securitatea națională sunt Serviciul de informații în materie de apărare (DI – *Defence Intelligence*), Consiliul și Secretariatul de securitate națională, Organizația comună de informații (*Joint Intelligence Organisation*) și Comitetul comun de informații (*Joint Intelligence Committee*). Cu toate acestea, nici JIC, nici JIO nu sunt în măsură să utilizeze competențele de investigare în temeiul IPA din 2016, în timp ce DI are un domeniu de aplicare limitat pentru a-și exercita competențele.

([262]) Interdicția se aplică atât rețelelor de comunicații publice, cât și celor private, precum și serviciului poștal public atunci când interceptarea are loc în Regatul Unit. Interdicția nu se aplică operatorului rețelei private dacă operatorul și-a dat consimțământul explicit sau implicit pentru efectuarea interceptării (secțiunea 3 din IPA din 2016).

([263]) Într-un număr limitat de cazuri, este posibilă interceptarea legală fără mandat, și anume atunci când interceptarea are loc cu consimțământul expeditorului sau al destinatarului (secțiunea 44 din IPA din 2016), în cazul unor scopuri administrative sau de aplicare a legii limitate (secțiunile 45-48 din IPA), în anumite instituții speciale (secțiunile 49-51 din IPA din 2016) și conform cererilor din străinătate (secțiunea 52 din IPA din 2016).

comunicațiilor și intervenția asupra echipamentelor) ([264]), precum și de măsura în care competența este exercitată asupra unei ținte specifice sau în masă. Detaliile privind domeniul de aplicare, garanțiile și limitările fiecărei măsuri prevăzute de IPA din 2016 sunt descrise în secțiunea specifică de mai jos.

(179) Mai mult, IPA din 2016 este completată de o serie de coduri statutare de bune practici, emise de secretarul de stat, aprobate de ambele camere ale Parlamentului ([265]) și aplicabile în întreaga țară, care furnizează orientări suplimentare cu privire la utilizarea acestor competențe ([266]). Deși persoanele vizate se pot baza în mod direct pe dispozițiile prevăzute în IPA din 2016 pentru a-și exercita drepturile, anexa 7 punctul 5 la IPA din 2016 precizează că codurile de bune practici sunt admisibile ca probe în procedurile civile și penale, iar instanța, tribunalul sau autoritatea de supraveghere poate lua în considerare orice neconformitate cu codurile atunci când stabilește un aspect relevant în cadrul procedurilor judiciare ([267]). În contextul evaluării „calității legii" cu privire la legislația anterioară a Regatului Unit în domeniul supravegherii, RIPA din 2000, Marea Cameră a Curții Europene a Drepturilor Omului a recunoscut în mod expres relevanța codurilor de bune practici din Regatul Unit și a acceptat că dispozițiile sale ar putea fi luate în considerare la evaluarea previzibilității legislației care permite supravegherea ([268]).

(180) De asemenea, ar trebui remarcat faptul că agențiile de securitate națională și anumite autorități de aplicare a legii ([269]) dispun de competențe țintite (interceptare țintită ([270]), achiziția datelor comunicațiilor ([271]), păstrarea datelor comunicațiilor ([272]) și intervenția țintită asupra echipamentelor ([273])), în timp ce numai serviciile de informații pot utiliza competențe în masă (și anume interceptarea în masă ([274]), achiziția în masă a datelor comunicațiilor ([275]), intervenția în masă asupra echipamentelor ([276]) și seturile de date cu caracter personal colectate în masă ([277])).

(181) Pentru a decide ce competențe de investigare ar trebui utilizate, agenția de informații trebuie să respecte „obligațiile generale în ceea ce privește dreptul la viață privată" enumerate în secțiunea 2 punctul 2 litera (a) din IPA din 2016, care includ un test de necesitate și de proporționalitate. Mai precis, în temeiul acestei dispoziții, o autoritate publică având intenția de a utiliza o competență de investigare trebuie să analizeze: (i) dacă ceea ce se urmărește a fi obținut prin mandat, autorizație sau notificare ar putea fi obținut în mod rezonabil prin alte mijloace mai puțin intruzive; (ii) dacă nivelul de protecție care urmează să fie aplicat în legătură cu orice obținere de informații în temeiul mandatului,

([264]) În ceea ce privește, de exemplu, domeniul de aplicare al unor astfel de măsuri, în temeiul părților 3 și 4 (păstrarea și achiziția datelor comunicațiilor), domeniul de aplicare al măsurii este strict legat de definiția „operatorilor de telecomunicații" ale căror date ale utilizatorilor fac obiectul măsurii. Un alt exemplu poate fi dat în legătură cu utilizarea competențelor „în masă". În acest caz, domeniul de aplicare al acestor competențe este limitat la „comunicările trimise sau primite de persoane fizice în afara insulei britanice".

([265]) Anexa 7 la IPA din 2016 stabilește domeniul de aplicare al codurilor, procedura care trebuie urmată la emiterea acestora, normele de revizuire a acestora și efectul codurilor.

([266]) Codurile de bune practici din cadrul IPA din 2016 sunt disponibile la următoarea adresă: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

([267]) Instanțele și tribunalele utilizează codurile de bune practici pentru a evalua legalitatea comportamentului autorităților. A se vedea, de exemplu: *Dias/Cleveland Police*, [2017] UKIPTrib15_586-CH, în care Tribunalul cu competențe de investigare a făcut trimitere la pasaje specifice din Codul de bune practici privind datele comunicațiilor pentru a înțelege definiția motivului de „prevenire sau depistare a infracțiunilor sau de prevenire a tulburărilor ordinii publice" utilizat pentru a solicita achiziția datelor comunicațiilor. Codul a fost inclus în motivare pentru a constata dacă motivul în cauză a fost utilizat în mod incorect. În continuare, potrivit concluziilor instanței, comportamentele contestate au fost nelegale. Instanțele au efectuat, de asemenea, o evaluare a nivelului garanțiilor disponibile în Coduri; a se vedea, de exemplu, *Just for Law Kids/Secretary of State for the Home Department* [2019] EWHC 1772 (Admin), în care Înalta Curte a constatat că legislația primară și secundară, împreună cu orientările interne, oferă garanții suficiente; sau *R (National Council for Civil Liberties)/Secretary of State for the Home Department și alții* [2019] EWHC 2057 (Admin), în care a constatat că atât IPA din 2016, cât și Codul de bune practici privind intervenția asupra echipamentelor conțin suficiente dispoziții cu privire la necesitatea specificității mandatelor.

([268]) În cauza Big Brother Watch, Marea Cameră a Curții Europene a Drepturilor Omului a arătat că „codul IC este un document public aprobat de ambele camere ale Parlamentului, care este publicat de guvern online și în versiune tipărită și care trebuie luat în considerare atât de persoanele care exercită funcții de interceptare, cât și de instanțe (a se vedea punctele 93-94 de mai sus). În consecință, Curtea a admis că dispozițiile sale ar putea fi luate în considerare la evaluarea previzibilității RIPA (a se vedea cauza Kennedy, citată anterior, § 157). În consecință, Curtea ar accepta ca dreptul intern ar fi «accesibil» în mod adecvat." [A se vedea Curtea Europeană a Drepturilor Omului (Marea Cameră), *Big Brother Watch și alții/Regatul Unit*, Cererile nr. 58170/13, 62322/14 și 24960/15 din 25 mai 2021, punctul 366].

([269]) Pentru lista autorităților relevante de aplicare a legii care pot aplica competențe de investigare țintite în temeiul IPA din 2016, a se vedea nota de subsol (139).

([270]) Partea 2 din IPA din 2016.

([271]) Partea 3 din IPA din 2016.

([272]) Partea 4 din IPA din 2016.

([273]) Partea 5 din IPA din 2016.

([274]) Secțiunea 136 din IPA din 2016.

([275]) Secțiunea 158 din IPA din 2016.

([276]) Secțiunea 176 din IPA din 2016.

([277]) Secțiunea 199 din IPA din 2016.

al autorizației sau al notificării este mai ridicat ca urmare a sensibilității deosebite a informațiilor respective; (iii) interesul public pentru integritatea și securitatea rețelelor de telecomunicații și a serviciilor poștale; și (iv) orice alte aspecte ale interesului public în ceea ce privește protecția vieții private ([278]).

(182) Modul în care ar trebui aplicate aceste criterii – și modul în care conformitatea lor este evaluată în cadrul autorizării utilizării acestor competențe de către secretarul de stat și de către comisarii judiciari independenți – este specificat mai în detaliu în codurile de bune practici în materie. În special, utilizarea oricăreia dintre aceste competențe de investigare trebuie să fie întotdeauna „proporțională cu ceea ce se urmărește a fi obținut, [ceea ce] implică asigurarea unui echilibru între gravitatea intruziunii în viața privată (și alte considerente prevăzute în secțiunea 2 punctul 2) și necesitatea activității din punct de vedere operațional, al investigării și al capacității". Aceasta înseamnă în special că „ar trebui să ofere o perspectivă realistă de a aduce beneficiul scontat și nu ar trebui să fie disproporțională sau arbitrară" și „[n]icio ingerință în viața privată nu ar trebui să fie considerată proporțională dacă informațiile solicitate ar putea fi obținute în mod rezonabil prin alte mijloace mai puțin intruzive" ([279]). Mai precis, respectarea principiului proporționalității trebuie apreciată în funcție de următoarele criterii: „(i) amploarea ingerinței propuse în viața privată față de ceea ce se urmărește a fi obținut; (ii) modul și motivul pentru care metodele care urmează să fie adoptate vor cauza cel mai redus grad posibil de ingerință persoanei în cauză și altor persoane; (iii) dacă activitatea este o utilizare adecvată a legii și o modalitate rezonabilă, după analizarea tuturor alternativelor rezonabile, de a obține ceea ce se urmărește a fi obținut; (iv) ce alte metode, după caz, fie nu au fost puse în aplicare, fie au fost utilizate, dar care sunt evaluate ca fiind insuficiente pentru îndeplinirea obiectivelor operaționale fără utilizarea competenței de investigare propuse" ([280]).

(183) În practică, astfel cum au explicat autoritățile Regatului Unit, acest lucru asigură faptul că o agenție de informații, în primul rând, stabilește obiectivul operațional (delimitând astfel colectarea, de exemplu un scop internațional de combatere a terorismului într-o anumită zonă geografică) și, în al doilea rând, pe baza obiectivului operațional respectiv, va trebui să ia în considerare opțiunea tehnică (de exemplu interceptarea țintită sau în masă, intervenția asupra echipamentelor, achiziția de date ale comunicațiilor) cu cel mai înalt grad de proporționalitate (și anume, cea mai puțin intruzivă în viața privată; a se vedea secțiunea 2 punctul 2 din IPA) față de ceea ce se urmărește a fi obținut și, prin urmare, poate fi autorizată în temeiul uneia dintre bazele statutare disponibile.

(184) Trebuie remarcat faptul că această recurgere la standardele de necesitate și proporționalitate a fost, de asemenea, observată și salutată de Raportorul special al ONU privind dreptul la viață privată, Joseph Cannataci, care a declarat, în ceea ce privește sistemul instituit prin IPA din 2016, că „[p]rocedurile în vigoare atât în cadrul serviciilor de informații, cât și în cadrul agențiilor de aplicare a legii par să necesite în mod sistematic luarea în considerare a necesității și a proporționalității unei măsuri sau a unei operațiuni de supraveghere înainte ca aceasta să fie recomandată pentru autorizare, precum și revizuirea acesteia din aceleași motive" ([281]). Acesta a observat, de asemenea, că, în cadrul întâlnirii cu reprezentanții autorităților de aplicare a legii și ai agențiilor de securitate națională, „[i] s-a adus la cunoștință opinia unanim acceptată potrivit căreia dreptul la viață privată trebuie să fie un considerent primordial pentru orice decizie privind măsurile de supraveghere. Cu toții au înțeles și au apreciat necesitatea și proporționalitatea ca principii fundamentale care trebuie luate în considerare".

([278]) Codul de bune practici privind interceptarea comunicațiilor precizează că alte elemente ale testului de proporționalitate sunt următoarele: „(i) amploarea ingerinței propuse în viața privată față de ceea ce se urmărește a fi obținut; (ii) modul și motivul pentru care metodele care urmează să fie adoptate vor cauza cel mai redus grad posibil de ingerință persoanei în cauză și altor persoane; (iii) dacă activitatea este o utilizare adecvată a legii și o modalitate rezonabilă, după analizarea tuturor alternativelor rezonabile, de a obține ceea ce se urmărește a fi obținut; (iv) ce alte metode, după caz, fie nu au fost puse în aplicare, fie au fost utilizate, dar care sunt evaluate ca fiind insuficiente pentru îndeplinirea obiectivelor operaționale fără utilizarea competenței de investigare propuse". Punctul 4.16 din Codul de bune practici privind interceptarea comunicațiilor, disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

([279]) A se vedea punctele 4.12 și 4.15 din Codul de bune practici privind interceptarea comunicațiilor, disponibile la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

([280]) A se vedea Codul de bune practici privind interceptarea comunicațiilor, punctul 4.16.

([281]) Declarația de sfârșit de mandat a Raportorului special privind dreptul la viață privată la încheierea misiunii sale în Regatul Unit al Marii Britanii și Irlandei de Nord, disponibilă la următoarea adresă: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, punctul 1.a.

(185) Criteriile specifice pentru emiterea diferitelor mandate, precum și limitările și garanțiile stabilite de IPA din 2016 în ceea ce privește fiecare competență de investigare sunt detaliate în considerentele 186-243.

3.3.1.1.1. Interceptare și examinare țintită

(186) Există trei tipuri de mandat de interceptare țintită: mandatul de interceptare țintită ([282]), mandatul de examinare țintită și un mandat de asistență reciprocă ([283]). Condițiile pentru obținerea acestor mandate și garanțiile relevante sunt prevăzute în partea 2 capitolul 1 din IPA din 2016.

(187) Un mandat de interceptare țintită autorizează interceptarea comunicațiilor descrise în mandat în cursul transmiterii acestora și obținerea altor date relevante pentru aceste comunicații ([284]), inclusiv a datelor secundare ([285]). Un mandat de examinare țintită autorizează o persoană să efectueze selecția pentru examinarea conținutului interceptat obținut în baza unui mandat de interceptare în masă ([286]).

(188) Orice mandat în temeiul părții 2 din IPA din 2016 poate fi emis de către secretarul de stat ([287]) și aprobat de un comisar judiciar ([288]). În toate cazurile, durata oricărui tip de mandat țintit este limitată la șase luni ([289]) și se aplică norme specifice privind modificarea ([290]) și reînnoirea ([291]) acestuia.

(189) Înainte de emiterea mandatului, secretarul de stat trebuie să efectueze o evaluare a necesității și a proporționalității ([292]). Mai precis, pentru un mandat de interceptare țintită și un mandat de examinare țintită, secretarul de stat ar trebui să verifice dacă măsura este necesară pentru unul dintre următoarele motive: interesul securității naționale; prevenirea sau depistarea unei infracțiuni grave; sau interesele bunăstării economice a Regatului Unit ([293]), în măsura în care aceste interese sunt relevante și pentru interesele de securitate națională ([294]). Pe de altă parte, un mandat de asistență reciprocă (a se vedea considerentul 139) poate fi emis numai în cazul în care secretarul de stat consideră că există circumstanțe echivalente cu cele în care ar emite un mandat în scopul prevenirii și/sau al depistării infracțiunilor grave ([295]).

(190) În plus, secretarul de stat ar trebui să evalueze dacă măsura este proporțională cu ceea ce se urmărește a fi obținut ([296]). Evaluarea proporționalității măsurilor solicitate trebuie să țină seama de obligațiile generale în ceea ce privește dreptul la viață privată prevăzute în secțiunea 2 punctul 2 din IPA din 2016, în special de necesitatea de a evalua dacă ceea ce se urmărește a fi obținut prin mandat, autorizație sau notificare ar putea fi obținut în mod

([282]) Secțiunea 15 punctul 2 din IPA din 2016.
([283]) Secțiunea 15 punctul 4 din IPA din 2016.
([284]) Secțiunea 15 punctul 2 din IPA din 2016.
([285]) Datele secundare sunt date atașate la comunicația interceptată sau asociate în mod logic acesteia, care pot fi separate în mod logic de aceasta și care, dacă ar fi separate astfel, nu ar dezvălui nicio informație din ceea ce ar putea fi considerat în mod rezonabil a fi sensul comunicației (dacă este cazul). Printre exemplele de date secundare se numără configurațiile routerelor sau firewall-urile sau perioada de timp în care un router a fost activ într-o rețea atunci când acestea fac parte din comunicația interceptată, sunt atașate la aceasta sau sunt asociate în mod logic acesteia. Pentru mai multe detalii, a se vedea definiția din secțiunea 16 din IPA din 2016 și Codul de bune practici privind interceptarea comunicațiilor, punctul 2.19, a se vedea nota de subsol 278.
([286]) Această examinare este efectuată cu titlu de excepție de la secțiunea 152 punctul 4 din IPA din 2016, care prevede interdicția încercării de identificare a comunicațiilor persoanelor care se află pe teritoriul Insulelor Britanice. A se vedea considerentul 229.
([287]) Ministrul scoțian autorizează mandatul atunci când acesta se referă la o activitate infracțională gravă din Scoția (a se vedea secțiunile 21 și 22 din IPA din 2016), în timp ce un funcționar superior poate fi desemnat de către secretarul de stat să emită un mandat de asistență reciprocă atunci când se constată că interceptarea va viza o persoană aflată sau un sediu aflat în afara Regatului Unit (secțiunea 40 din IPA din 2016).
([288]) Secțiunile 19 și 23 din IPA din 2016.
([289]) Secțiunea 32 din IPA din 2016.
([290]) Secțiunea 39 din IPA din 2016. Se pot efectua modificări limitate ale mandatelor de către persoanele prevăzute, în condițiile stabilite în IPA din 2016. Persoana care a emis mandatul poate anula un mandat în orice moment. Aceasta trebuie să procedeze astfel dacă mandatul nu mai este necesar din orice motive relevante sau în cazul în care comportamentul autorizat prin mandat nu mai este proporțional cu ceea ce se urmărește a fi obținut.
([291]) Secțiunea 33 din IPA din 2016. Decizia de reînnoire a mandatului trebuie aprobată de un comisar judiciar.
([292]) Secțiunea 19 din IPA din 2016.
([293]) În ceea ce privește noțiunea de „interese ale bunăstării economice a Regatului Unit, atunci când aceste interese sunt relevante și pentru securitatea națională”, Marea Cameră a Curții Europene a Drepturilor Omului a constatat în cauza Big Brother Watch și alții/Regatul Unit (a se vedea nota de subsol 268 de mai sus), punctul 371, că această noțiune s-a concentrat suficient pe securitatea națională. Deși constatarea Curții în această cauză a fost legată de utilizarea acestei noțiuni în RIPA din 2000, aceeași noțiune este utilizată în IPA din 2016.
([294]) Secțiunea 20 punctul 2 din IPA din 2016.
([295]) Secțiunea 20 punctul 3 din IPA din 2016.
([296]) Secțiunea 19 punctul 1 litera (b), secțiunea 19 punctul 2 litera (b) și secțiunea 19 punctul 3 litera (b) din IPA din 2016.

rezonabil prin alte mijloace mai puțin intruzive și dacă nivelul de protecție care urmează să fie aplicată în legătură cu orice obținere de informații în temeiul mandatului este mai ridicat ca urmare a sensibilității deosebite a informațiilor respective (a se vedea considerentul 181).

(191) În acest scop, secretarul de stat va trebui să ia în considerare toate elementele cererii furnizate de autoritatea care a prezentat cererea, în special cele referitoare la persoanele care urmează să fie interceptate și relevanța măsurii pentru investigație. Aceste elemente sunt enunțate în Codul de bune practici privind interceptarea comunicațiilor și trebuie descrise la un anumit nivel de specificitate ([297]). În plus, secțiunea 17 din IPA din 2016 prevede că orice mandat emis în temeiul capitolului 2 din aceasta trebuie să nominalizeze sau să descrie o anumită persoană sau un grup de persoane, organizația sau sediul care urmează să fie interceptate („ținta"). În cazul unui mandat de interceptare țintită sau al unui mandat de examinare țintită, acestea se pot referi, de asemenea, la un grup de persoane, la mai multe persoane sau organizații sau la mai multe sedii (așa-numitul „mandat tematic") ([298]). În aceste cazuri, mandatul ar trebui să descrie scopul comun sau activitatea comună a grupului de persoane sau a operațiunii/investigațiilor și să nominalizeze sau să descrie cât mai multe dintre aceste persoane/organizații sau sedii, în cazul în care acest lucru este rezonabil din punct de vedere practic ([299]). În cele din urmă, toate mandatele emise în temeiul părții 2 din IPA din 2016 trebuie să specifice adresele, numerele, aparatura, factorii sau combinația de factori care urmează să fie utilizați pentru identificarea comunicațiilor ([300]). În acest sens, Codul de bune practici privind interceptarea comunicațiilor precizează că, în cazul unui mandat de interceptare țintită și al unui mandat de examinare țintită, „mandatul trebuie să specifice (sau să descrie) factorii sau combinația de factori care urmează să fie utilizați pentru identificarea comunicațiilor. În cazul în care comunicațiile trebuie să fie identificate prin trimitere la un număr de telefon (de exemplu), numărul trebuie specificat prin redarea sa în întregime. Cu toate acestea, în cazul în care pentru identificarea comunicațiilor urmează să se utilizeze selectoare de internet foarte complexe sau în continuă schimbare, aceste selectoare ar trebui să fie descrise cât mai mult posibil" ([301]).

(192) O garanție importantă în acest context este că evaluarea efectuată de secretarul de stat pentru emiterea unui mandat trebuie să fie aprobată de un comisar judiciar ([302]) independent care va verifica în special dacă decizia de emitere a mandatului respectă principiile necesității și proporționalității ([303]) (în ceea ce privește statutul și rolul comisarilor judiciari, a se vedea considerentele 251-256). IPA din 2016 clarifică, de asemenea, faptul că, atunci când efectuează o astfel de verificare, comisarul judiciar trebuie să aplice aceleași principii ca cele care ar fi aplicate de o instanță cu privire la o cerere de control jurisdicțional ([304]). Acest lucru garantează faptul că, în fiecare caz și înainte să aibă loc accesul la date, respectarea principiului necesității și proporționalității este verificată în mod sistematic de către un organism independent.

(193) IPA din 2016 prevede câteva excepții specifice și limitate pentru efectuarea de interceptări țintite fără mandat. Cazurile limitate sunt detaliate în lege ([305]) și, cu excepția celui bazat pe „consimțământul" expeditorului/destinatarului, acestea sunt efectuate de persoane (organisme private sau publice), altele decât agențiile de securitate națională. În plus, acest tip de interceptări este efectuat în alte scopuri decât colectarea de „informații" ([306]) și, pentru unele dintre acestea, este foarte puțin probabil ca colectarea să poată avea loc în contextul unui scenariu de „transfer"

([297]) Informațiile solicitate includ detalii privind contextul (descrierea persoanelor/organizațiilor/sediilor, comunicația care urmează să fie interceptată) și modul în care obținerea acestor informații va aduce beneficii investigației, precum și o descriere a comportamentului care urmează să fie autorizat. În cazul în care nu este posibilă descrierea persoanelor/organizației/sediilor, trebuie inclusă o explicație cu privire la motivul pentru care nu a fost posibilă sau cu privire la motivul pentru care s-a realizat doar o descriere generală (Codul de bune practici privind interceptarea comunicațiilor, punctele 5.32 și 5.34, a se vedea nota de subsol 278).

([298]) Secțiunea 17 punctul 2 din IPA din 2016. A se vedea, de asemenea, Codul de bune practici privind interceptarea comunicațiilor, punctul 5.11 și următoarele, a se vedea nota de subsol 278.

([299]) Secțiunea 31 punctele 4 și 5 din IPA din 2016.

([300]) Secțiunea 31 punctul 8 din IPA din 2016.

([301]) Codul de bune practici privind interceptarea comunicațiilor, punctele 5.37 și 5.38, a se vedea nota de subsol 278.

([302]) Aprobarea de către un comisar judiciar nu este necesară atunci când secretarul de stat consideră că există o nevoie urgentă de emitere a mandatului (secțiunea 19 punctul 1 din IPA). Cu toate acestea, comisarul judiciar trebuie informat într-o perioadă scurtă de timp și trebuie să decidă dacă aprobă sau nu mandatul. În caz contrar, mandatul încetează să mai producă efecte (secțiunile 24 și 25 din IPA din 2016).

([303]) Secțiunea 23 punctul 1 din IPA din 2016.

([304]) Secțiunea 23 punctul 2 din IPA din 2016.

([305]) A se vedea secțiunile 44-51 din IPA din 2016 și secțiunea 12 din Codul de bune practici privind interceptarea comunicațiilor (a se vedea nota de subsol 278).

([306]) Acesta este cazul, de exemplu, atunci când o interceptare este necesară în închisoare sau într-un spital de psihiatrie (pentru a verifica comportamentul persoanei deținute sau al unui pacient) sau este necesară pentru ca un operator poștal sau de telecomunicații, de exemplu, să detecteze conținutul abuziv.

(de exemplu, în cazul unei interceptării desfășurate într-un spital de psihiatrie sau într-o închisoare). Având în vedere natura organismului căruia i se aplică aceste cazuri specifice (diferit de agențiile de securitate națională), se vor aplica toate garanțiile prevăzute în partea 2 din DPA din 2018 și RGPD al Regatului Unit, inclusiv supravegherea ICO și mecanismele de exercitare a unei căi de atac disponibile. În plus, pe lângă garanțiile oferite de DPA din 2018, în anumite cazuri, IPA din 2016 prevede de asemenea supravegherea ([307]) *ex post* a IPCO.

(194) Atunci când se efectuează interceptarea, sunt aplicabile limitări și garanții suplimentare, având în vedere statutul specific al persoanei (persoanelor) interceptate ([308]). De exemplu, interceptarea articolelor care fac obiectul secretului profesional al avocatului este autorizată numai în prezența unor circumstanțe excepționale și imperative, iar persoana care emite mandatul trebuie să țină seama de interesul public în ceea ce privește confidențialitatea articolelor care fac obiectul secretului profesional al avocatului și de existența unor cerințe specifice pentru gestionarea, păstrarea și divulgarea unor astfel de materiale ([309]).

(195) În plus, IPA din 2016 prevede garanții specifice legate de securitate, păstrare și divulgare pe care secretarul de stat ar trebui să le ia în considerare înainte de emiterea unui mandat țintit ([310]). În special, secțiunea 53 punctul 5 din IPA din 2016 prevede că fiecare copie realizată de pe oricare dintre materialele colectate în temeiul mandatului trebuie să fie stocată în condiții de siguranță și distrusă de îndată ce nu mai există motive relevante pentru a fi păstrată, în timp ce secțiunea 53 punctul 2 din IPA din 2016 impune ca numărul de persoane cărora le sunt divulgate materialele și măsura în care orice material este divulgat, pus la dispoziție sau copiat să fie limitate la minimul necesar în scopuri legale.

(196) În cele din urmă, atunci când materialul care a fost interceptat fie printr-un mandat de interceptare țintită, fie printr-un mandat de asistență reciprocă urmează să fie transmis către o țară terță („divulgări în străinătate"), IPA din 2016 prevede că secretarul de stat trebuie să se asigure că au fost instituite mecanisme adecvate pentru a se asigura că în țara terță respectivă există garanții similare în materie de securitate, păstrare și divulgare ([311]). În plus, articolul 109 alineatul (2) din DPA din 2018 prevede că serviciile de informații pot transfera date cu caracter personal în afara teritoriului Regatului Unit numai dacă transferul este o măsură necesară și proporțională efectuată în scopul îndeplinirii funcțiilor statutare ale operatorului sau în alte scopuri prevăzute în secțiunea 2 punctul 2 litera (a) din Legea privind serviciul de securitate din 1989 sau în secțiunea 2 punctul 2 litera (a) și secțiunea 4 punctul 2 litera (a) din Legea privind serviciile de informații din 1994 ([312]). Este important de remarcat faptul că aceste cerințe se aplică, de asemenea, în cazurile în care se invocă derogarea în materie de securitate națională în temeiul secțiunii 110 din DPA din 2018, întrucât secțiunea 110 din DPA din 2018 nu enumeră secțiunea 109 din DPA din 2018 drept una dintre dispozițiile care pot să nu fie aplicate în cazul în care este necesară o derogare de la anumite dispoziții în scopul protejării securității naționale.

3.3.1.1.2. Achiziția țintită și păstrarea datelor comunicațiilor

(197) IPA din 2016 permite secretarului de stat să solicite operatorilor de telecomunicații să păstreze datele comunicațiilor în scopul accesului țintit al unei serii de autorități publice, inclusiv al agențiilor de aplicare a legii și al serviciilor de informații. Partea 4 din IPA din 2016 prevede păstrarea datelor comunicațiilor, în timp ce partea 3 prevede achiziția țintită a datelor comunicațiilor (TCD). Partea 3 și partea 4 din IPA din 2016 stabilesc, de asemenea, limitări specifice privind utilizarea acestor competențe și prevăd garanții specifice.

([307]) A se vedea *a contrario* secțiunea 229 punctul 4 din IPA.

([308]) Secțiunile 26-29 din IPA din 2016 introduc limitări pentru obținerea unor mandate de interceptare și de examinare țintite în legătură cu interceptarea comunicațiilor trimise de o persoană care este membru al Parlamentului (orice parlament al Regatului Unit) sau destinate acesteia, interceptarea articolelor care fac obiectul secretului profesional al avocatului, interceptarea comunicațiilor pe care autoritatea de interceptare le consideră a fi comunicații care conțin materiale jurnalistice confidențiale și atunci când scopul mandatului este de a identifica sau confirma o sursă de informare jurnalistică.

([309]) Secțiunea 26 din IPA din 2016.

([310]) Secțiunea 19 punctul 1 din IPA din 2016.

([311]) Secțiunea 54 din IPA din 2016. Garanțiile referitoare la divulgarea de materiale către autoritățile străine sunt specificate mai în detaliu în codurile de bune practici: a se vedea în special punctul 9.26 și următoarele și punctul 9.87 din Codul de bune practici privind interceptarea comunicațiilor, precum și punctele 9.33 și următoarele și 9.41 din Codul de bune practici privind intervenția asupra echipamentelor (a se vedea nota de subsol 278).

([312]) Aceste scopuri sunt următoarele: pentru Serviciul de Securitate, prevenirea sau depistarea infracțiunilor grave sau orice proceduri penale [secțiunea 2 punctul 2 litera (a) din Legea privind serviciul de securitate din 1989], pentru Serviciul de Informații, interesele securității naționale, prevenirea sau depistarea infracțiunilor grave sau orice proceduri penale [secțiunea 2 punctul 2 litera (a) din Legea privind serviciile de informații din 1994] și pentru GCHQ, orice proceduri penale [secțiunea 4 punctul 2 litera (a) din Legea privind serviciile de informații din 1994]. A se vedea, de asemenea, notele explicative privind DPA din 2018, disponibile la următoarea adresă: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

(198) Termenul „date ale comunicațiilor” se referă la „cine”, „când”, „unde” și „cum” aferente unei comunicații, dar nu și la conținut, și anume ceea ce s-a spus sau s-a scris. Spre deosebire de interceptare, achiziția și păstrarea datelor comunicațiilor nu au ca scop obținerea conținutului comunicației, ci vizează obținerea de informații precum abonatul la un serviciu telefonic sau o factură detaliată. Aceasta ar putea include ora și durata comunicației, numărul sau adresa de e-mail a emitentului și a destinatarului și, uneori, localizarea dispozitivelor de la care a fost efectuată telecomunicația ([313]).

(199) Ar trebui remarcat faptul că păstrarea și achiziția datelor comunicațiilor nu se referă, în mod normal, la datele cu caracter personal ale persoanelor vizate din UE transferate în temeiul prezentei decizii către Regatul Unit. Obligația de a păstra sau de a divulga date ale comunicațiilor în temeiul părților 3 și 4 din IPA din 2016 se referă la datele care sunt colectate de operatorii de telecomunicații din Regatul Unit direct de la utilizatorii unui serviciu de telecomunicații ([314]). Acest tip de prelucrare „orientată către client” nu implică, de regulă, un transfer în temeiul prezentei decizii, și anume un transfer de la un operator/o persoană împuternicită de operator din UE către un operator/o persoană împuternicită de operator din Regatul Unit.

(200) Cu toate acestea, din motive de exhaustivitate, condițiile și garanțiile care reglementează aceste regimuri de achiziție și păstrare sunt analizate în considerentele următoare.

(201) Ca premisă, trebuie remarcat faptul că păstrarea și achiziția țintită a datelor privind comunicațiile sunt disponibile atât pentru agențiile de securitate națională, cât și pentru anumite autorități de aplicare a legii ([315]). Condițiile de solicitare a păstrării și/sau a achiziției datelor privind comunicațiile pot varia în funcție de motivul solicitării măsurii, și anume securitatea națională sau asigurarea respectării legii.

(202) În special, deși noul regim a introdus cerința generală privind autorizarea *ex ante* de către un organism independent care se va aplica în toate cazurile în care datele comunicațiilor sunt păstrate și/sau obținute (fie în scopul asigurării respectării legii, fie în scopuri de securitate națională), în urma hotărârii pronunțate de Curtea Europeană de Justiție în cauza Tele2/Watson ([316]), au fost introduse garanții specifice atunci când măsura este solicitată în scopul asigurării respectării legii. În special, în cazul în care păstrarea sau achiziția datelor comunicațiilor este solicitată în scopul asigurării respectării legii, autorizarea *ex ante* trebuie să fie întotdeauna acordată de către comisarul pentru competențe de investigare. Acest lucru nu se întâmplă întotdeauna atunci când măsura este solicitată în scopul securității naționale, deoarece, astfel cum se descrie mai jos, în anumite cazuri, un astfel de tip de măsuri poate fi autorizat de diferite „persoane care acordă autorizația”. În plus, noul regim a ridicat la „infracțiuni grave” pragul pentru care pot fi permise păstrarea și achiziția datelor comunicațiilor ([317]).

([313]) Datele privind comunicațiile sunt definite în secțiunea 261 punctul 5 din IPA din 2016. Datele comunicațiilor sunt împărțite în „date referitoare la evenimente” (orice date care identifică sau descriu un eveniment, indiferent dacă se referă sau nu la localizarea acestuia, în sau prin intermediul unei rețele de telecomunicații în care evenimentul constă în angajarea uneia sau mai multor entități într-o anumită activitate la un moment dat) și „date referitoare la entitate” [orice date care: (a) se referă la: (i) o entitate; (ii) o asociere între un serviciu de telecomunicații și o entitate; sau (iii) o asociere între orice parte a unei rețele de telecomunicații și o entitate; (b) constau în sau includ date care identifică sau descriu entitatea (indiferent dacă se referă sau nu la localizarea entității); și (c) nu sunt date referitoare la eveniment].

([314]) Acest lucru rezultă din definiția datelor comunicațiilor, prevăzută la secțiunea 261 punctul 5 din IPA din 2016, potrivit căreia datele comunicațiilor sunt deținute sau obținute de un operator de telecomunicații și fie se referă la utilizatorul unui serviciu de telecomunicații și la furnizarea acestui serviciu, fie sunt cuprinse într-o comunicație, incluse ca parte integrantă în aceasta, atașate la aceasta sau asociate în mod logic acesteia (a se vedea, de asemenea, Codul de bune practici privind datele comunicațiilor, disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, punctele 2.22-2.33). În plus, definiția operatorului de telecomunicații prevăzută în secțiunea 261 punctul 10 din IPA din 2016 impune ca un operator de telecomunicații să fie o persoană care oferă sau furnizează un serviciu de telecomunicații unor persoane din Regatul Unit sau care controlează sau furnizează o rețea de telecomunicații aflată (integral sau parțial) în Regatul Unit sau controlată din Regatul Unit. Aceste definiții clarifică faptul că obligațiile prevăzute de IPA din 2016 nu pot fi impuse operatorilor de telecomunicații ale căror echipamente nu se află în Regatul Unit sau nu sunt controlate din Regatul Unit și care nu oferă sau nu furnizează servicii persoanelor din Regatul Unit (a se vedea, de asemenea, Codul de bune practici privind datele comunicațiilor, punctul 2.1). În cazul în care abonații din UE (indiferent dacă se află în UE sau în Regatul Unit) ar utiliza servicii în Regatul Unit, orice comunicații în legătură cu furnizarea acestui serviciu ar fi colectate direct de către furnizorul de servicii din Regatul Unit, mai degrabă decât să facă obiectul unui transfer din UE.

([315]) Autoritățile relevante sunt enumerate în anexa 4 la IPA din 2016 și includ forțele de poliție, serviciile de informații, unele ministere și departamente guvernamentale, Agenția Națională pentru Combaterea Criminalității, Administrația Fiscală și Vamală din Regatul Unit, Autoritatea pentru Concurență și Piețe, comisarul pentru informații, ambulanța, serviciile de pompieri și de salvare și autoritățile, de exemplu, din domeniul sănătății și siguranței alimentare.

([316]) Cauzele conexate C-203/15 și C-698/15, *Tele2/Watson*, ECLI:EU:C:2016:970.

([317]) A se vedea secțiunea 61.7 litera (b) pentru achiziția datelor de comunicații și secțiunea 87.10A pentru păstrarea datelor comunicațiilor.

(i) *Autorizarea pentru obținerea datelor comunicațiilor*

(203) În conformitate cu partea 3 din IPA din 2016, autoritățile publice relevante sunt autorizate să obțină date ale comunicațiilor de la un operator de telecomunicații sau de la orice persoană care poate obține și divulga astfel de date. Autorizația poate să nu permită interceptarea conținutului comunicațiilor ([318]) și încetează să producă efecte după o perioadă de o lună ([319]), cu posibilitatea de a fi reînnoită sub rezerva unei autorizații suplimentare ([320]). Achiziția de date ale comunicațiilor necesită o autorizație din partea comisarului pentru competențe de investigare (IPC) ([321]) (pentru statutul și competențele IPC, a se vedea considerentele 250-251). Acest lucru este valabil întotdeauna atunci când achiziția de date ale comunicațiilor este solicitată de o autoritate relevantă de aplicare a legii. Cu toate acestea, în conformitate cu secțiunea 61 din IPA din 2016, atunci când datele sunt obținute în interesul securității naționale sau al bunăstării economice a Regatului Unit, atât timp cât acestea sunt relevante pentru securitatea națională, sau în cazul în care o cerere este depusă de un membru al unei agenții de informații în temeiul secțiunii 61 punctul 7 litera (b) ([322]), achiziția poate fi ([323]) autorizată alternativ de către IPC sau de către un funcționar superior desemnat ([324]). Funcționarul desemnat trebuie să fie independent de investigația sau operațiunea în cauză și să dețină cunoștințe practice privind principiile și legislația în domeniul drepturilor omului, în special cele privind necesitatea și proporționalitatea ([325]). Decizia luată de funcționarul desemnat va face obiectul supravegherii *ex post* efectuate de IPC (a se vedea considerentul 254 pentru mai multe detalii privind funcțiile de supraveghere *ex post* ale IPC).

(204) Autorizația de a obține date ale comunicațiilor se bazează pe o evaluare a necesității și proporționalității măsurii. Mai precis, necesitatea măsurii este evaluată în lumina motivelor enumerate în legislație ([326]). Având în vedere caracterul specific al acestei măsuri, aceasta trebuie, de asemenea, să fie necesară pentru o investigație sau o operațiune specifică ([327]). Cerințe suplimentare privind evaluarea necesității măsurilor sunt prevăzute în Codul de bune practici privind datele comunicațiilor ([328]). În special, acest cod prevede că cererea depusă de autoritatea solicitantă ar trebui să identifice trei elemente minime pentru a justifica necesitatea acestei cereri: (i) evenimentul care face obiectul investigației, cum ar fi o infracțiune sau localizarea unei persoane dispărute vulnerabile; (ii) persoana ale cărei date sunt solicitate, cum ar fi un suspect, un martor sau o persoană dispărută, și modul în care acestea sunt legate de eveniment; și (iii) datele comunicațiilor solicitate, cum ar fi un număr de telefon sau o adresă IP, precum și modul în care aceste date sunt legate de persoana în cauză și de eveniment ([329]).

(205) În plus, achiziția de date ale comunicațiilor trebuie să fie proporțională cu ceea ce se urmărește a fi obținut ([330]). Codul de bune practici privind datele comunicațiilor clarifică faptul că, atunci când efectuează o astfel de evaluare, persoana care acordă autorizația ar trebui să efectueze un exercițiu de echilibru între „amploarea ingerinței în drepturile și libertățile unei persoane și un beneficiu concret pentru investigația sau operațiunea efectuată de o

([318]) Secțiunea 60A punctul 6 din IPA din 2016.

([319]) Această perioadă se reduce la trei zile atunci când autorizația este acordată din motive de urgență (secțiunea 65 punctul 3A din IPA din 2016).

([320]) În conformitate cu secțiunea 65 din IPA din 2016, autorizația reînnoită va dura o perioadă de o lună de la data expirării autorizației actuale. Persoana care acordă autorizația o poate anula în orice moment în cazul în care consideră că cerințele nu mai sunt îndeplinite.

([321]) Secțiunea 60A punctul 1 din IPA din 2016. Oficiul pentru autorizații privind datele comunicațiilor (*Office for Communications Data Authorisations* – OCDA) îndeplinește această funcție în numele IPC (a se vedea Codurile de bune practici privind datele comunicațiilor, punctul 5.6).

([322]) Cererea prevăzută în secțiunea 61 punctul 7 litera (b) din IPA din 2016 se depune pentru „un scop aplicabil în materie de criminalitate", însemnând, în conformitate cu secțiunea 61 punctul 7A din IPA din 2016: „în cazul în care datele comunicațiilor sunt, integral sau parțial, date referitoare la evenimente, scopul prevenirii sau al depistării infracțiunilor grave; în orice alt caz, scopul prevenirii sau al depistării infracțiunilor sau al prevenirii tulburărilor ordinii publice".

([323]) Codul de bune practici privind datele comunicațiilor precizează următoarele: „În cazul în care o cerere referitoare la securitatea națională ar putea fi depusă fie în temeiul secțiunii 60A, fie în temeiul secțiunii 61, decizia privind calea de autorizare cea mai adecvată într-un anumit caz ține de competența autorităților publice individuale. Autoritățile publice care doresc să utilizeze calea funcționarilor superiori desemnați ar trebui să dispună de orientări clare cu privire la momentul în care această cale de autorizare este adecvată" (Codul de bune practici privind datele comunicațiilor, punctul 5. 19, disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

([324]) Secțiunea 70 punctul 3 din IPA din 2016 prevede definiția unui „funcționar desemnat", care variază de la o autoritate publică relevantă la alta (astfel cum se prevede în anexa 4 la IPA din 2016).

([325]) Detalii suplimentare privind independența funcționarului superior desemnat sunt furnizate în Codul de bune practici privind datele comunicațiilor (Codul de bune practici privind datele comunicațiilor, punctele 4.12-4.17, a se vedea nota de subsol 323).

([326]) Motivele sunt următoarele: (i) securitatea națională; (ii) prevenirea sau depistarea infracțiunilor sau prevenirea tulburărilor ordinii publice (în cazul „datelor referitoare la evenimente", numai infracțiunile grave); (iii) în interesul bunăstării economice a Regatului Unit, în măsura în care aceste interese sunt relevante și pentru interesele de securitate națională; (iv) în interesul siguranței publice; (v) cu scopul de a preveni decesul, vătămarea sau orice prejudiciu adus sănătății fizice sau mentale a unei persoane sau de a atenua orice vătămare sau prejudiciu adus sănătății fizice sau mentale a unei persoane; (vi) pentru a sprijini investigațiile privind presupusele erori judiciare; sau (vii) pentru a identifica o persoană decedată sau o persoană care nu se poate identifica din cauza unei anumite afecțiuni (secțiunea 61 punctul 7 din IPA din 2016).

([327]) Secțiunea 60A punctul 1 litera (b) din IPA din 2016.

([328]) Codul de bune practici privind datele comunicațiilor, punctul 3.3 și următoarele, a se vedea nota de subsol 323.

([329]) Codul de bune practici privind datele comunicațiilor, punctul 3.13, a se vedea nota de subsol 323.

([330]) Secțiunea 60 punctul 1 litera (c) din IPA din 2016.

autoritate publică relevantă în interes public" și că, ținând seama de toate considerentele unui anumit caz, „o ingerință în drepturile unei persoane poate să nu fie încă justificată deoarece impactul negativ asupra drepturilor unei alte persoane sau ale unui grup de persoane este prea puternic". Mai mult, pentru a evalua în mod specific proporționalitatea măsurii, codul enumeră o serie de elemente care ar trebui incluse în cererea depusă de autoritatea solicitantă ([331]). În plus, trebuie să se acorde o atenție deosebită tipului de date ale comunicațiilor (date referitoare la „entitate" sau la „evenimente" ([332])) care urmează să fie obținute și trebuie să se acorde prioritate utilizării categoriei de date mai puțin intruzive ([333]). Codul de bune practici privind datele comunicațiilor conține, de asemenea, instrucțiuni specifice pentru autorizațiile care implică date ale comunicațiilor aparținând persoanelor din anumite profesii (cum ar fi medici, avocați, jurnaliști, parlamentari sau preoți) ([334]) care fac obiectul unor garanții suplimentare ([335]).

(ii) *Notificare prin care se solicită păstrarea datelor comunicațiilor*

(206) Partea 4 din IPA din 2016 stabilește normele privind păstrarea datelor comunicațiilor, în special criteriile care permit secretarului de stat să emită o notificare de păstrare ([336]). Garanțiile introduse de IPA sunt identice atunci când datele sunt păstrate fie în scopul asigurării respectării legii, fie în interesul securității naționale.

(207) Emiterea acestor notificări de păstrare are scopul de a garanta că operatorii de telecomunicații păstrează, pentru o perioadă maximă de 12 luni, datele relevante ale comunicațiilor care altfel ar fi șterse atunci când nu mai sunt necesare în scopuri comerciale ([337]). Datele păstrate trebuie să rămână disponibile pe perioada necesară în cazul în care, ulterior, este necesar ca o autoritate publică să le obțină în temeiul unei autorizații pentru achiziția țintită de date ale comunicațiilor prevăzute în partea 3 din IPA din 2016 și descrise în considerentele 203-205.

(208) Exercitarea competenței de a solicita păstrarea anumitor date este supusă unei serii de limitări și garanții. Secretarul de stat poate emite o notificare de păstrare adresată unuia sau mai multor operatori ([338]) numai atunci când consideră că cerința de păstrare a datelor este necesară pentru unul dintre motivele legale ([339]) și este proporțională cu ceea ce se urmărește a fi obținut ([340]). Astfel cum a

([331]) Aceste informații care urmează să fie incluse trebuie să conțină: (i) o descriere a modului în care obținerea datelor va aduce beneficii investigației sau operațiunii; (ii) o explicație a relevanței perioadelor de timp solicitate, inclusiv a modului în care aceste perioade sunt proporționale cu evenimentul care face obiectul investigației; (iii) o explicație a modului în care nivelul de intruziune este justificat atunci când se ia în considerare beneficiul pe care datele îl vor oferi investigației (această justificare ar trebui să includă analizarea posibilității de a efectua investigații mai puțin intruzive pentru a atinge obiectivul); (iv) examinarea drepturilor (în special la viață privată și, în cazurile relevante, la libertatea de exprimare) ale persoanei și realizarea unui echilibru între aceste drepturi și beneficiile aduse investigației; (v) detalii privind intruziunea colaterală care poate surveni și modul în care perioadele de timp solicitate au un impact asupra intruziunii colaterale (Codul de bune practici privind datele comunicațiilor, punctele 3.22-3.26, a se vedea nota de subsol 323).

([332]) A se vedea nota de subsol 313.

([333]) Atunci când se solicită date mai intruzive ale comunicațiilor (și anume, date referitoare la evenimente), codul precizează că este mai adecvat să se obțină mai întâi date referitoare la entitate sau să se obțină direct date referitoare la evenimente în cazuri limitate de urgență specifică (Codul de bune practici privind datele comunicațiilor, punctele 6.10-6.14, a se vedea nota de subsol 323).

([334]) Codul de bune practici privind datele comunicațiilor, punctele 8.8-8.44, a se vedea nota de subsol 323.

([335]) Codul de bune practici prevede că „o persoană care acordă autorizația trebuie să acorde o atenție deosebită analizării acestor cereri, inclusiv analizării suplimentare a posibilității de a exista consecințe nedorite ale acestor cereri și de a stabili dacă cererea servește cel mai bine interesului public" (Codul de bune practici privind datele comunicațiilor, punctul 8.8). În plus, trebuie păstrate evidențe pentru acest tip de cereri și, la următoarea inspecție, aceste cereri ar trebui să fie marcate în atenția IPC (Codul de bune practici privind datele comunicațiilor, punctul 8.10, a se vedea nota de subsol 323).

([336]) Secțiunile 87-89 din IPA din 2016.

([337]) În temeiul secțiunii 90 din IPA din 2016, un operator de telecomunicații căruia i se transmite o notificare de păstrare a datelor poate solicita o revizuire din partea secretarului de stat care a emis-o.

([338]) În temeiul articolului 87 alineatul (2) litera (a) din IPA din 2016, o notificare de păstrare se poate referi la „un anumit operator sau la orice categorie de operatori".

([339]) Scopurile sunt următoarele: (i) interesul securității naționale; (ii) scopul aplicabil în materie de criminalitate (astfel cum este definit în secțiunea 87.10A din IPA din 2016); (iii) interesele bunăstării economice a Regatului Unit, în măsura în care aceste interese sunt relevante și pentru interesele de securitate națională; (iv) interesul siguranței publice; (v) scopul de a preveni decesul, vătămarea sau orice prejudiciu adus sănătății fizice sau mentale a unei persoane sau de a atenua orice vătămare sau prejudiciu adus sănătății fizice sau mentale a unei persoane; sau (vi) pentru a sprijini investigațiile privind presupusele erori judiciare (secțiunea 87 din IPA).

([340]) Secțiunea 87 din IPA din 2016. În plus, în conformitate cu codul de bune practici relevant, pentru a evalua proporționalitatea notificării de păstrare, se aplică criteriile prevăzute în secțiunea 2 punctul 2 din IPA din 2016, în special cerința de a evalua dacă ceea ce se urmărește a fi obținut prin notificare ar putea fi obținut în mod rezonabil prin mijloace mai puțin intruzive. În mod similar evaluării proporționalității în ceea ce privește achiziția de date ale comunicațiilor, Codul de bune practici privind datele comunicațiilor clarifică faptul că o astfel de evaluare implică „asigurarea unui echilibru între amploarea ingerinței în dreptul unei persoane la respectarea vieții private și un beneficiu concret pentru investigație" (Codul de bune practici privind datele comunicațiilor, punctul 16.3, a se vedea nota de subsol 323).

fost clarificat chiar de IPA din 2016 ([341]), înainte de a emite o notificare de păstrare, secretarul de stat trebuie să țină seama de: beneficiile probabile ale notificării ([342]); o descriere a serviciilor de telecomunicații; oportunitatea limitării datelor care urmează să fie păstrate în funcție de locație sau descrieri ale persoanelor cărora le sunt furnizate servicii de telecomunicații ([343]); numărul probabil de utilizatori (dacă se cunoaște) ai oricărui serviciu de telecomunicații la care se referă notificarea ([344]); fezabilitatea tehnică a respectării notificării; costul probabil al respectării notificării și orice alt efect al notificării asupra operatorului de telecomunicații (sau a descrierii operatorilor) la care se referă ([345]). După cum se precizează mai departe în capitolul 17 din Codul de bune practici privind datele comunicațiilor, toate notificările de păstrare trebuie să specifice fiecare tip de date care trebuie păstrate și modul în care respectivul tip de date îndeplinește testele necesare pentru păstrare.

(209) În toate cazurile (atât în scopuri de securitate națională, cât și de asigurare a respectării legii), decizia secretarului de stat de a emite notificarea de păstrare trebuie să fie aprobată de un comisar judiciar independent în cadrul așa-numitei „proceduri de protecție dublă", care trebuie să verifice în special dacă notificarea de păstrare a datelor relevante ale comunicațiilor este necesară și proporțională pentru unul sau mai multe dintre scopurile statutare ([346]).

3.3.1.1.3. Intervenția asupra echipamentelor

(210) Intervenția asupra echipamentelor reprezintă un set de tehnici utilizate pentru a obține o varietate de date de la echipamente ([347]), care includ calculatoare, tablete și telefoane inteligente, precum și cabluri, fire și dispozitive de stocare ([348]). Intervenția asupra echipamentelor permite obținerea atât a conținutului comunicațiilor, cât și a datelor referitoare la echipamente ([349]).

(211) În conformitate cu secțiunea 13 punctul 1 din IPA din 2016, pentru intervenția asupra echipamentelor de către un serviciu de informații, este necesară o autorizație prin intermediul unui mandat în cadrul procedurii de „protecție dublă" instituite de IPA din 2016, cu condiția să existe o „legătură cu Insulele Britanice" ([350]). Conform explicațiilor furnizate de autoritățile Regatului Unit, în situațiile în care datele sunt transferate din Uniunea Europeană către

([341]) A se vedea secțiunea 88 din IPA din 2016.

([342]) Beneficiile pot fi existente sau preconizate și trebuie să respecte scopurile legale pentru care datele pot fi păstrate (Codul de bune practici privind datele comunicațiilor, punctul 17.17, a se vedea nota de subsol 323).

([343]) Aceste considerații vor stabili inclusiv dacă sfera geografică completă a notificării de păstrare este necesară și proporțională și dacă este necesar și proporțional să se includă sau să se excludă anumite descrieri de persoane (Codul de bune practici privind datele comunicațiilor, punctul 17.17, a se vedea nota de subsol 323).

([344]) Acest lucru va ajuta secretarul de stat să analizeze atât nivelul de intruziune asupra clienților, cât și beneficiile probabile ale datelor care urmează să fie păstrate (Codul de bune practici privind datele comunicațiilor, punctul 17.17, a se vedea nota de subsol 323).

([345]) Secțiunea 88 din IPA din 2016.

([346]) Secțiunea 89 din IPA din 2016.

([347]) În temeiul secțiunii 135 punctul 1 și al secțiunii 198 punctul 1 din IPA din 2016, „echipamente" înseamnă echipamente care produc emisii electromagnetice, acustice sau de altă natură, precum și orice dispozitiv care poate fi utilizat în legătură cu asemenea echipamente.

([348]) Codul de bune practici privind intervenția asupra echipamentelor (*Code of Practice on Equipment Interference*), disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, punctul 2.2.

([349]) Datele referitoare la echipamente sunt definite în secțiunea 100 din IPA din 2016 ca date de sistem și date care sunt: (a) cuprinse într-o comunicație, incluse ca parte integrantă în aceasta, atașate la aceasta sau asociate în mod logic acesteia (indiferent dacă aceste operațiuni sunt efectuate sau nu de către expeditor) sau oricărei alte informații; (b) pot fi separate în mod logic de restul comunicației sau al informației; și (c) dacă ar fi astfel separate, nu ar dezvălui nimic din ceea ce ar putea fi considerat în mod rezonabil a fi sensul (dacă este cazul) al comunicației sau al informației.

([350]) Pentru ca cerința referitoare la mandat să fie obligatorie, secțiunea 13 punctul 1 din IPA din 2016 prevede, de asemenea, ca comportamentul serviciului de informații să constituie una sau mai multe infracțiuni în temeiul secțiunilor 1-3A din *Computer Misuse Act 1990* (Legea privind protejarea materialelor informatice împotriva utilizării abuzive), ceea ce ar fi adevărat în marea majoritate a circumstanțelor (a se vedea Codul de bune practici privind intervenția asupra echipamentelor, punctele 3.32 și 3.6-3.9). În conformitate cu secțiunea 13 punctul 2 din IPA din 2016, există o „legătură cu Insulele Britanice" în cazul în care: (a) orice comportament ar avea loc în Insulele Britanice (indiferent de localizarea echipamentelor asupra cărora s-ar interveni sau asupra cărora se poate interveni); (b) serviciul de informații consideră că oricare dintre echipamentele asupra cărora s-ar interveni sau asupra cărora se poate interveni s-ar afla sau ar putea să se afle în Insulele Britanice la un moment dat, în timpul efectuării intervenției; sau (c) un scop al intervenției este de a obține: (i) comunicații trimise de către sau către o persoană care se află sau despre care serviciul de informații consideră că se află, în prezent, în Insulele Britanice; (ii) informații private referitoare la o persoană care se află sau despre care serviciul de informații consideră că se află, în prezent, în Insulele Britanice; sau (iii) date referitoare la echipamente care fac parte din comunicațiile sau informațiile private care intră sub incidența punctului (i) sau (ii) sau care au legătură cu acestea.

Regatul Unit în cadrul domeniului de aplicare al prezentei decizii, ar exista întotdeauna o „legătură cu Insulele Britanice" și orice intervenție asupra echipamentelor care acoperă astfel de date ar face, prin urmare, obiectul cerinței obligatorii referitoare la mandat din secțiunea 13 punctul 1 din IPA din 2016 ([351]).

(212) Normele privind mandatele de intervenție țintită asupra echipamentelor sunt prevăzute în partea 5 din IPA din 2016. La fel ca interceptarea țintită, intervenția țintită asupra echipamentelor trebuie să se refere la o anumită „țintă" care trebuie să fie specificată în mandat ([352]). Detaliile privind modul în care trebuie identificată o „țintă" depind de problematică și de tipul de echipament asupra căruia urmează să se intervină. În special secțiunea 115 punctul 3 din IPA precizează elementele care ar trebui incluse în mandat (de exemplu, numele persoanei sau denumirea organizației, descrierea locului), în funcție, de exemplu, de faptul dacă intervenția se referă la un echipament care aparține, este utilizat sau se află în posesia unei anumite persoane, a unei organizații sau a unui grup de persoane, se află într-un anumit loc etc. ([353]) Scopurile pentru care pot fi emise mandate de intervenție țintită asupra echipamentelor depind de autoritatea publică solicitantă ([354]).

(213) La fel ca interceptarea țintită, autoritatea emitentă trebuie să analizeze dacă măsura este necesară pentru atingerea unui anumit scop și dacă este proporțională cu ceea ce se urmărește a fi obținut ([355]). În plus, aceasta ar trebui să analizeze, de asemenea, dacă există garanții în ceea ce privește securitatea, păstrarea și divulgarea, precum și în ceea ce privește „divulgarea în străinătate" ([356]) (a se vedea considerentul 196).

(214) Mandatul trebuie să fie aprobat de un comisar judiciar, cu excepția cazurilor de urgență ([357]). În acest din urmă caz, un comisar judiciar trebuie să fie informat că a fost emis un mandat, iar acesta trebuie să îl aprobe în termen de trei zile lucrătoare. În cazul în care comisarul judiciar refuză să îl aprobe, mandatul încetează să mai producă efecte și nu poate fi reînnoit ([358]). În plus, comisarul judiciar are competența de a solicita ștergerea ([359]) oricăror date care au fost obținute în temeiul mandatului. Faptul că un mandat a fost emis de urgență nu afectează supravegherea *ex post* (a se vedea considerentele 244-255) sau posibilitățile persoanelor fizice de a obține reparații (a se vedea considerentele 260-270). Persoanele fizice pot depune o plângere la ICO sau pot depune o plângere cu privire la orice presupus comportament la Tribunalul cu competențe de investigare în modul obișnuit. În toate cazurile, testul aplicat de comisarul judiciar atunci când decide dacă să aprobe sau nu un mandat este testul de necesitate și proporționalitate aplicabil cererilor de interceptare țintită ([360]) (a se vedea considerentul 192).

([351]) Din motive de exhaustivitate, trebuie remarcat faptul că, chiar și în situațiile în care nu există o „legătură cu Insulele Britanice" și utilizarea intervenției asupra echipamentelor nu este, prin urmare, supusă cerinței obligatorii referitoare la mandat prevăzute în secțiunea 13 punctul 1 din IPA din 2016, un serviciu de informații care intenționează să desfășoare o activitate pentru care este în măsură să obțină un mandat pentru intervenția în masă asupra echipamentelor ar trebui să obțină un astfel de mandat ca principiu de politică (a se vedea Codul de bune practici privind intervenția asupra echipamentelor, punctul 3.24). Chiar și în cazul în care un mandat pentru intervenția asupra echipamentelor în temeiul IPA din 2016 nu este nici impus prin lege, nici obținut ca principiu de politică, acțiunile serviciilor de informații fac obiectul unei serii de condiții și limitări în temeiul secțiunii 7 din Legea privind serviciile de informații din 1994. Aceasta include în special cerința unei autorizații din partea secretarului de stat, care trebuie să se asigure că nicio acțiune nu depășește ceea ce este necesar pentru îndeplinirea corespunzătoare a funcțiilor Serviciului de informații.

([352]) Secțiunea 115 din IPA din 2016 reglementează conținutul mandatului, specificând că acesta trebuie să includă numele sau descrierea persoanelor, organizațiilor, locului sau grupului de persoane care constituie „ținta", o descriere a naturii investigației și o descriere a activităților pentru care se utilizează echipamentele. El trebuie, de asemenea, să descrie tipul de echipament și comportamentul pe care persoana căreia îi este adresat mandatul este autorizată să îl adopte.

([353]) A se vedea, de asemenea, Codul de bune practici privind intervenția asupra echipamentelor, punctul 5.7, a se vedea nota de subsol 348.

([354]) Agențiile de securitate națională pot solicita un mandat de intervenție asupra echipamentelor atunci când acest lucru este necesar în scopuri de securitate națională, în scopul depistării infracțiunilor grave și/sau în interesul bunăstării economice a Regatului Unit, în măsura în care aceste interese sunt relevante și pentru interesele de securitate națională (secțiunile 102-103 din IPA din 2016). În funcție de agenție, un mandat de intervenție asupra echipamentelor poate fi solicitat în scopul asigurării respectării legii atunci când acest lucru este necesar pentru depistarea sau prevenirea unei infracțiuni grave sau în scopul prevenirii decesului sau a oricărei vătămări sau a oricărui prejudiciu adus sănătății fizice sau mentale a unei persoane sau pentru a atenua orice vătămare sau prejudiciu adus sănătății fizice sau mentale a unei persoane (a se vedea secțiunea 106 punctele 1 și 3 din IPA din 2016).

([355]) Secțiunea 102 punctul 1 din IPA din 2016.

([356]) Secțiunile 129-131 din IPA din 2016.

([357]) Secțiunea 109 din IPA din 2016.

([358]) Secțiunea 109 punctul 4 din IPA din 2016.

([359]) Secțiunea 110 punctul 3 litera (b) din IPA din 2016. În conformitate cu punctul 5.67 din Codul de bune practici privind intervenția asupra echipamentelor, urgența se stabilește prin faptul dacă ar fi rezonabil din punct de vedere practic să se solicite aprobarea comisarului judiciar pentru emiterea mandatului în termenul disponibil pentru a răspunde unei necesități operaționale sau de investigare. Mandatele urgente ar trebui să se încadreze într-una sau în ambele categorii de mai jos: (i) amenințarea iminentă la adresa vieții sau vătămarea gravă – de exemplu, dacă o persoană a fost răpită și se apreciază că viața sa este în pericol iminent; sau (ii) o posibilitate de colectare de informații sau de investigare cu timp limitat pentru a acționa – de exemplu, un transport de droguri din clasa A este pe cale să intre în Regatul Unit, iar agențiile de aplicare a legii doresc să aibă o acoperire a autorilor infracțiunilor grave pentru a efectua arestări. A se vedea nota de subsol 348.

([360]) Secțiunea 108 din IPA din 2016.

(215) În cele din urmă, garanțiile specifice aplicabile interceptării țintite se aplică, de asemenea, intervenției asupra echipamentelor în ceea ce privește durata, reînnoirea și modificarea mandatului, precum și interceptării membrilor Parlamentului, a articolelor care fac obiectul secretului profesional al avocatului și a materialelor jurnalistice (a se vedea mai multe detalii în considerentul 193).

3.3.1.1.4. Exercitarea competențelor în masă

(216) Competențele în masă sunt reglementate în partea 6 din IPA din 2016. În plus, codurile de bune practici prevăd mai multe detalii cu privire la utilizarea competențelor în masă. Deși în legislația Regatului Unit nu există nicio definiție a „competenței în masă", în contextul IPA din 2016, aceasta a fost descrisă ca fiind colectarea și păstrarea unor volume mari de date obținute de guvern prin diverse mijloace (și anume, competențele de interceptare în masă, achiziție în masă, intervenție în masă asupra echipamentelor și seturi de date cu caracter personal colectate în masă) și care pot fi accesate ulterior de către autorități. Această descriere este clarificată prin comparare cu ceea ce nu reprezintă „competența în masă": aceasta nu echivalează cu așa-numita „supraveghere în masă" fără limitări sau garanții. Dimpotrivă, astfel cum se explică mai jos, aceasta include limitări și garanții menite să asigure că accesul la date nu este acordat în mod nediscriminatoriu sau nejustificat ([361]). În special, competențele în masă pot fi utilizate numai dacă se stabilește o legătură între măsura tehnică pe care o agenție națională de informații intenționează să o utilizeze și obiectivul operațional pentru care se solicită o astfel de măsură.

(217) În plus, competențele în masă sunt disponibile numai agențiilor de informații și fac întotdeauna obiectul unui mandat emis de secretarul de stat și aprobat de un comisar judiciar. La alegerea mijloacelor de colectare a informațiilor, trebuie să se ia în considerare dacă obiectivul în cauză poate fi urmărit prin „mijloace mai puțin intruzive" ([362]). Această abordare decurge din cadrul legislației care se bazează pe principiul proporționalității și, prin urmare, acordă prioritate colectării țintite față de colectarea în masă.

3.3.1.1.4.1. Interceptarea în masă și intervenția în masă asupra echipamentelor

(218) Regimul de interceptare în masă este prevăzut în partea 6 capitolul 1 din IPA din 2016, în timp ce capitolul 3 din aceeași parte reglementează intervenția în masă asupra echipamentelor. Aceste regimuri sunt în esență aceleași, astfel încât condițiile și garanțiile suplimentare aplicabile mandatelor respective sunt analizate împreună.

(i) *Condiții și criterii pentru emiterea mandatului*

(219) Un mandat de interceptare în masă se limitează la interceptarea comunicațiilor în cursul transmisiei lor trimise sau primite de către persoane fizice care se află în afara Insulelor Britanice ([363]), așa-numitele „comunicații în străinătate" ([364]), precum și a altor date relevante și la selectarea ulterioară pentru examinarea materialului

([361]) Potrivit Raportului privind competențele în masă prezentat de Lord David Anderson, evaluator independent al legislației în materie de combatere a terorismului înainte de aprobarea IPA din 2016, „ar trebui să fie clar faptul că colectarea și păstrarea datelor în masă nu echivalează cu așa-numita «supraveghere în masă». Orice sistem juridic care își merită denumirea va include limitări și garanții concepute tocmai pentru a se asigura că accesul la baza de date sensibile […] nu este acordat în mod nediscriminatoriu sau nejustificat. Aceste limitări și garanții există cu siguranță în proiectul de lege." Lord David Anderson, *Report of the bulk power review (Raport privind evaluarea competențelor în masă),* august 2016, punctul 1.9 (sublinierea noastră), disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF

([362]) Secțiunea 2.2 din IPA din 2016. A se vedea, de exemplu, Codul de bune practici privind achiziția în masă a datelor comunicațiilor, punctul 4.11, disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf

([363]) „Insulele Britanice" constituie Regatul Unit, Insulele Anglo-Normande și Insula Man și sunt definite în anexa 1 la *Interpretation Act 1978* (Legea din 1978 privind interpretarea legii), disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/1978/30/schedule/1

([364]) În conformitate cu secțiunea 136 din IPA din 2016, „comunicații în străinătate" înseamnă: (i) comunicații transmise de persoane care se află în afara Insulelor Britanice; sau (ii) comunicații primite de persoane care se află în afara Insulelor Britanice. Acest regim, astfel cum a fost confirmat de autoritățile Regatului Unit, acoperă, de asemenea, comunicațiile dintre două persoane care se află în afara Insulelor Britanice. În cauza Big Brother Watch și alții/Regatul Unit (a se vedea nota de subsol 279 de mai sus), Marea Cameră a Curții Europene a Drepturilor Omului a constatat la punctul 376, în ceea ce privește o limitare similară (referitoare la „comunicațiile externe") a comunicațiilor care pot fi capturate prin interceptări în masă în temeiul RIPA din 2000, că aceasta era suficient de delimitată și previzibilă.

interceptat ([365]). Un mandat de intervenție în masă asupra echipamentelor ([366]) autorizează destinatarul să asigure intervenția asupra oricărui echipament în scopul obținerii de comunicații în străinătate (inclusiv orice elemente care includ vorbire, muzică, sunete, imagini vizuale sau date de orice tip), date referitoare la echipamente (date care permit sau facilitează funcționarea unui serviciu poștal; a unei rețele de telecomunicații; a unui serviciu de telecomunicații) sau orice alte informații ([367]).

(220) Secretarul de stat poate emite un mandat în masă numai la cererea unui șef al unui serviciu de informații ([368]). Mandatul de autorizare a unei interceptări în masă sau a unei intervenții în masă asupra echipamentelor trebuie emis numai dacă acest lucru este necesar în interesul securității naționale și în scopul prevenirii sau al depistării infracțiunilor grave sau în interesul bunăstării economice a Regatului Unit, atunci când acest lucru este relevant pentru securitatea națională ([369]). În plus, secțiunea 142 punctul 7 din IPA din 2016 prevede că un mandat de interceptare în masă trebuie să fie specificat într-un mod mai detaliat decât simpla referire la „interesele securității naționale", la „bunăstarea economică a Regatului Unit" și la „prevenirea și combaterea infracțiunilor grave", dar trebuie stabilită o legătură între măsura care urmează să fie solicitată și unul sau mai multe scopuri operaționale care trebuie incluse în mandat.

(221) Alegerea scopului operațional este rezultatul unui proces pe mai multe niveluri. Secțiunea 142 punctul 4 prevede că scopurile operaționale specificate în mandat trebuie să fie specificate într-o listă gestionată de șefii serviciilor de informații, ca scopuri pe care aceștia le consideră a fi scopuri operaționale pentru care conținutul interceptat sau datele secundare obținute în baza unor mandate de interceptare în masă pot fi selectate în vederea examinării. Lista scopurilor operaționale trebuie aprobată de secretarul de stat. Secretarul de stat poate acorda o astfel de aprobare numai în cazul în care se asigură că scopul operațional este specificat la un nivel mai ridicat de detaliere decât motivele generale de autorizare a mandatului (securitate națională sau securitate națională și bunăstare economică sau prevenirea infracțiunilor grave) ([370]). La sfârșitul fiecărei perioade relevante de trei luni, secretarul de stat trebuie să transmită Comisiei de informații și securitate a Parlamentului o copie a listei de scopuri operaționale. În cele din urmă, prim-ministrul trebuie să revizuiască lista scopurilor operaționale cel puțin o dată pe an ([371]). Astfel cum a constatat Înalta Curte, „[a]cestea nu trebuie să fie minimalizate ca garanții nesemnificative, deoarece construiesc împreună un set complex de moduri de răspundere, care implică atât parlamentul, cât și membrii guvernului la cel mai înalt nivel" ([372]).

(222) Astfel de scopuri operaționale limitează, de asemenea, domeniul de aplicare al selecției materialelor de interceptare pentru etapa de examinare. Selecția pentru examinarea oricăror materiale colectate în temeiul mandatului în masă trebuie să fie justificată având în vedere scopul (scopurile) operațional(e). Astfel cum au explicat autoritățile Regatului Unit, acest lucru înseamnă că modalitățile practice de examinare trebuie să fie evaluate de către secretarul de stat încă din etapa mandatului, oferind suficiente detalii pentru îndeplinirea obligațiilor statutare prevăzute în secțiunile 152 și 193 din IPA din 2016 ([373]). Detaliile furnizate secretarului de stat în legătură cu aceste modalități ar trebui să includă, de exemplu, informații (dacă este cazul) cu privire la modul în care modalitățile de filtrare pot varia în perioada în care un mandat va produce efecte ([374]). Pentru mai multe detalii privind procesul și garanțiile aplicate etapelor de filtrare și de examinare, a se vedea considerentul 229.

([365]) Secțiunea 136 punctul 4 din IPA din 2016. Potrivit explicațiilor primite de la guvernul Regatului Unit, interceptarea în masă poate fi utilizată, de exemplu, pentru a identifica amenințările până atunci necunoscute la adresa securității naționale a Regatului Unit, prin filtrarea și analizarea materialelor interceptate în vederea identificării comunicațiilor care prezintă interes pentru serviciile de informații (Cadrul explicativ al Regatului Unit, secțiunea H: Securitatea națională, pp. 27-28, a se vedea nota de subsol 29). Astfel cum au explicat autoritățile Regatului Unit, astfel de instrumente pot fi utilizate pentru a stabili legături între subiectele de interes cunoscute, precum și pentru a căuta urme de activități ale unor persoane care este posibil să nu fie cunoscute încă, dar care sunt dezvăluite în cursul unei investigații, precum și pentru a identifica tipare de activitate care ar putea indica o amenințare pentru Regatul Unit.

([366]) În conformitate cu secțiunea 13 punctul 1 din IPA din 2016, pentru intervenția asupra echipamentelor de către un serviciu de informații, este necesară o autorizație prin intermediul unui mandat prevăzut în cadrul IPA din 2016, cu condiția să existe o „legătură cu Insulele Britanice"; a se vedea considerentul 211.

([367]) Secțiunea 176 din IPA din 2016. Un mandat de intervenție în masă asupra echipamentelor nu poate autoriza un comportament care (cu excepția cazului în care este adoptat cu o autorizație legală) ar constitui o interceptare ilegală (cu excepția cazului în care are legătură cu o comunicație stocată). Conform Cadrului explicativ al Regatului Unit, informațiile obținute ar putea fi necesare pentru identificarea subiectelor de interes și ar constitui operațiuni de regulă adecvate, la scară largă (Cadrul explicativ al Regatului Unit, secțiunea H: Securitatea națională, p. 28, a se vedea nota de subsol 29).

([368]) Secțiunea 138 punctul 1 și secțiunea 178 punctul 1 din IPA din 2016.

([369]) Secțiunea 138 punctul 2 și secțiunea 178 punctul 2 din IPA din 2016.

([370]) Conform explicațiilor furnizate de autoritățile Regatului Unit, de exemplu, un scop operațional poate limita domeniul de aplicare al măsurii la existența unei amenințări într-o anumită zonă geografică.

([371]) Secțiunea 142 punctele 4-10 din IPA din 2016.

([372]) Înalta Curte de Justiție, *Liberty*, [2019] EWHC 2057 (Admin), punctul 167.

([373]) Secțiunile 152 și 193 din IPA din 2016 prevăd următoarele: (a) selecția pentru examinare se efectuează numai în scopurile operaționale specificate în mandat; (b) selecția pentru examinare este necesară și proporțională în toate circumstanțele; și (c) selecția pentru examinare nu încalcă interdicția de a selecta materiale și de a identifica acele comunicații care au fost transmise de către persoane cunoscute ca aflându-se în Insulele Britanice la momentul respectiv sau care sunt destinate acestora.

([374]) A se vedea Codul de bune practici privind interceptarea comunicațiilor, punctul 6.6, a se vedea nota de subsol 278.

(223) O competență în masă poate fi autorizată numai dacă este proporțională cu ceea ce se urmărește a fi obținut ([375]). Astfel cum se specifică în Codul de bune practici privind interceptarea comunicațiilor, orice evaluare a proporționalității implică „asigurarea unui echilibru între gravitatea intruziunii în viața privată (și alte considerente prevăzute în secțiunea 2 punctul 2) și necesitatea activității din punct de vedere operațional, al investigării și al capacității. Comportamentul autorizat ar trebui să ofere o perspectivă realistă de a aduce beneficiul scontat și nu ar trebui să fie disproporționat sau arbitrar" ([376]). După cum s-a menționat deja, în practică, aceasta înseamnă că testul de proporționalitate se bazează pe un test de echilibru între ceea ce se urmărește a fi obținut [„scopul/scopurile operațional(e)"] și opțiunile tehnice disponibile (de exemplu, interceptarea țintită sau în masă, intervenția asupra echipamentelor, achiziția de date ale comunicațiilor), acordând prioritate mijloacelor cel mai puțin intruzive (a se vedea considerentele 181 și 182). În cazul în care mai multe măsuri sunt adecvate obiectivului, trebuie să se acorde prioritate mijloacelor mai puțin intruzive.

(224) O garanție suplimentară privind evaluarea proporționalității măsurii solicitate este asigurată de faptul că secretarul de stat trebuie să primească informațiile relevante necesare pentru a-și efectua evaluarea în mod corespunzător. În special, Codul de bune practici privind interceptarea comunicațiilor și Codul de bune practici privind intervenția asupra echipamentelor impun ca cererea depusă de autoritatea relevantă să menționeze contextul cererii, descrierea comunicațiilor care urmează să fie interceptate și operatorii de telecomunicații care trebuie să acorde asistență, descrierea comportamentului care urmează să fie autorizat, scopurile operaționale și o explicație a motivului pentru care comportamentul este necesar și proporțional ([377]).

(225) În cele din urmă și cel mai important, decizia secretarului de stat de a emite mandatul trebuie să fie aprobată de un comisar judiciar independent care evaluează necesitatea și proporționalitatea măsurii propuse, utilizând aceleași principii care ar fi utilizate de o instanță judecătorească în cadrul unei cereri de control jurisdicțional ([378]). Mai precis, comisarul judiciar va examina concluziile secretarului de stat cu privire la necesitatea mandatului și la proporționalitatea comportamentului în raport cu principiile stabilite în secțiunea 2 punctul 2 din IPA din 2016 (obligații generale în ceea ce privește dreptul la viață privată). Comisarul judiciar va examina, de asemenea, concluziile secretarului de stat cu privire la faptul dacă fiecare dintre scopurile operaționale specificate în mandat este un scop pentru care selecția este sau poate fi necesară. În cazul în care comisarul judiciar refuză să aprobe decizia de emitere a unui mandat, secretarul de stat poate: (i) să accepte decizia și, prin urmare, să nu emită mandatul; sau (ii) să sesizeze comisarul pentru competențe de investigare în vederea pronunțării unei decizii (cu excepția cazului în care comisarul pentru competențe de investigare a luat decizia inițială) ([379]).

(ii) *Garanții suplimentare*

(226) IPA din 2016 a introdus limite suplimentare privind durata, reînnoirea și modificarea unui mandat în masă. Mandatul trebuie să aibă o durată maximă de șase luni, iar orice decizie de reînnoire sau modificare (cu excepția unor modificări minore) a mandatului trebuie, de asemenea, să fie aprobată de un comisar judiciar ([380]). Codul de bune practici privind interceptarea comunicațiilor și Codul de bune practici privind intervenția asupra echipamentelor specifică faptul că o modificare a scopurilor operaționale ale mandatului este considerată o modificare majoră a mandatului ([381]).

([375]) Secțiunea 138 punctul 1 literele (b) și (c) și secțiunile 178 literele (b) și (c) din IPA din 2016.

([376]) Codul de bune practici privind interceptarea comunicațiilor, punctul 4.10, a se vedea nota de subsol 278.

([377]) Codul de bune practici privind interceptarea comunicațiilor, punctul 6.20, a se vedea nota de subsol 278, și Codul de bune practici privind intervenția asupra echipamentelor, punctul 6.13, a se vedea nota de subsol 348.

([378]) Secțiunea 138 punctul 1 litera (g) și secțiunea 178 punctul 1 litera (f) din IPA din 2016. Autorizarea prealabilă de către un organism independent a fost identificată în special de Curtea Europeană a Drepturilor Omului ca o garanție importantă împotriva abuzurilor în contextul interceptării în masă. Curtea Europeană a Drepturilor Omului (Marea Cameră), Big Brother Watch și alții/Regatul Unit (a se vedea nota de subsol 269 de mai sus), punctele 351 și 352. Este important de reținut că această hotărâre se referea la cadrul juridic anterior (RIPA din 2000) care nu conținea unele dintre garanțiile (inclusiv autorizarea prealabilă din partea unui comisar judiciar independent) introduse de IPA din 2016.

([379]) Secțiunea 159 punctele 3 și 4 din IPA din 2016.

([380]) Secțiunile 143-146 și 184-188 din IPA din 2016. În cazul unei modificări urgente, secretarul de stat poate efectua modificarea fără aprobare, dar trebuie să notifice comisarul, iar apoi comisarul trebuie să decidă dacă să aprobe sau să refuze modificarea (secțiunea 147 din IPA din 2016). Mandatele trebuie anulate în cazul în care nu mai sunt necesare sau proporționale sau în cazul în care examinarea conținutului interceptat, a metadatelor sau a altor date obținute în temeiul mandatului nu mai este necesară pentru niciunul dintre scopurile operaționale specificate în mandat (secțiunile 148 și 189 din IPA din 2016).

([381]) Codul de bune practici privind interceptarea comunicațiilor, punctele 6.44-6.47, a se vedea nota de subsol 278, și Codul de bune practici privind intervenția asupra echipamentelor, punctul 6.48, a se vedea nota de subsol 348.

(227) În mod similar cu ceea ce se prevede pentru interceptarea țintită, partea 6 din IPA din 2016 prevede că secretarul de stat trebuie să se asigure că sunt în vigoare modalități pentru a oferi garanții privind păstrarea și divulgarea materialelor obținute în temeiul mandatului ([382]), precum și pentru divulgarea în străinătate ([383]). În special, secțiunea 150 punctul 5 și secțiunea 191 punctul 5 din IPA din 2016 prevăd că fiecare copie realizată de pe oricare dintre materialele colectate în temeiul mandatului trebuie să fie stocată în condiții de siguranță și distrusă de îndată ce nu mai există motive relevante pentru a fi păstrată, în timp ce secțiunea 150 punctul 2 și secțiunea 191 punctul 2 impun ca numărul de persoane cărora le sunt divulgate materialele și măsura în care orice material este divulgat, pus la dispoziție sau copiat să fie limitate la minimul necesar în scopuri legale ([384]).

(228) În cele din urmă, atunci când materialul care a fost interceptat fie printr-o interceptare în masă, fie printr-o intervenție în masă asupra echipamentelor urmează să fie transmis către o țară terță („divulgări în străinătate"), IPA din 2016 prevede că secretarul de stat trebuie să se asigure că au fost instituite mecanisme adecvate pentru a se asigura că în țara terță respectivă există garanții similare în materie de securitate, păstrare și divulgare ([385]). În plus, secțiunea 109 din DPA din 2018 stabilește cerințe specifice pentru transferurile internaționale de date cu caracter personal de către serviciile de informații către țări terțe sau organizații internaționale și interzic transferul datelor cu caracter personal către o țară sau un teritoriu din afara Regatului Unit sau către o organizație internațională cu excepția cazului în care transferul este necesar și proporțional în scopul îndeplinirii funcțiilor statutare ale operatorului sau în alte scopuri prevăzute în secțiunea 2 punctul 2 litera (a) din Legea privind serviciile de securitate din 1989 sau în secțiunea 2 punctul 2 litera (a) și secțiunea 4 punctul 2 litera (a) din Legea privind serviciile de informații din 1994 ([386]). Este important de remarcat faptul că aceste cerințe se aplică, de asemenea, în cazurile în care se invocă derogarea în materie de securitate națională în temeiul secțiunii 110 din DPA din 2018, întrucât secțiunea 110 din DPA din 2018 nu enumeră secțiunea 109 din DPA din 2018 drept una dintre dispozițiile care pot să nu fie aplicate în cazul în care este necesară o derogare de la anumite dispoziții în scopul protejării securității naționale.

(229) Odată ce mandatul a fost aprobat și datele au fost colectate în masă, datele vor face obiectul unei selecții înainte de a fi examinate. Etapa de selecție și examinare face obiectul unui nou test de proporționalitate efectuat de analist, care definește criteriile de selecție pe baza scopurilor operaționale incluse în mandat (și a modalităților de filtrare potențial existente). Astfel cum se prevede în secțiunile 152 și 193 din IPA, atunci când emite mandatul, secretarul de stat trebuie să se asigure că sunt instituite mecanisme pentru a garanta că selecția materialelor se efectuează numai în scopurile operaționale specificate și că aceasta este necesară și proporțională în toate circumstanțele. În acest sens, autoritățile Regatului Unit au clarificat faptul că materialele interceptate în masă sunt selectate, în primul rând, prin filtrare automată cu scopul de a elimina date care este puțin probabil să fie de interes pentru securitatea națională. Filtrele vor varia în timp (pe măsură ce se modifică tiparele, tipurile și protocoalele de trafic de internet) și vor depinde de tehnologie și de contextul operațional. După această etapă, datele pot fi selectate pentru examinare numai dacă sunt relevante pentru scopurile operaționale specificate în mandat ([387]). Garanțiile prevăzute de IPA din 2016 pentru examinarea materialelor colectate se aplică oricărui tip de date (atât conținutul interceptat, cât și datele secundare) ([388]). Secțiunile 152 și 193 din IPA din 2016 prevăd, de asemenea, o interdicție generală de a selecta pentru examinare materiale referitoare la conversații trimise de persoane care se află în Insulele Britanice sau destinate acestora. În cazul în care autoritățile doresc să examineze asemenea materiale, acestea ar depune o cerere pentru un mandat de examinare țintită în temeiul părților 2 și 4 din IPA din 2016, emis de secretarul de stat și aprobat de un comisar judiciar ([389]). În cazul în care o persoană selectează în mod deliberat conținut interceptat în vederea examinării, cu încălcarea cerințelor stabilite în legislație ([390]), aceasta comite o infracțiune ([391]).

([382]) Secțiunea 156 din IPA din 2016.

([383]) Secțiunile 150 și 191 din IPA din 2016.

([384]) În cauza Big Brother Watch și alții/Regatul Unit (a se vedea nota de subsol 268de mai sus), Marea Cameră a Curții Europene a Drepturilor Omului a confirmat sistemul de garanții suplimentare pentru păstrarea, accesul și divulgarea datelor care era prevăzut în RIPA din 2000, a se vedea punctele 392-394 și 402-405. Același sistem de garanții este prevăzut de IPA din 2016.

([385]) Secțiunile 151 și 192 din IPA din 2016.

([386]) Pentru mai multe informații privind aceste scopuri, a se vedea nota de subsol 312.

([387]) Codurile privind interceptarea comunicațiilor precizează, în acest sens, următoarele: „Aceste sisteme de prelucrare prelucrează datele din legăturile sau semnalele de comunicații pe care autoritatea de interceptare a ales să le intercepteze. În continuare se aplică un anumit grad de filtrare traficului de pe aceste legături și semnale, destinat să selecteze tipuri de comunicații care ar putea prezenta interes pentru serviciile de informații, eliminându-le în același timp pe cele mai puțin susceptibile de a prezenta un astfel de interes. Ca urmare a acestei filtrări, care va varia de la un sistem de prelucrare la altul, o parte semnificativă a comunicațiilor de pe aceste legături și semnale va fi eliminată în mod automat. Ulterior, pot avea loc căutări complexe suplimentare pentru a extrage în continuare comunicațiile cele mai susceptibile să prezinte cel mai mare interes pentru serviciile de informații, care se referă la funcțiile statutare ale agenției. Aceste comunicații pot fi apoi selectate în vederea examinării pentru unul sau mai multe dintre scopurile operaționale specificate în mandat, în cazul în care sunt îndeplinite condițiile de necesitate și proporționalitate. Numai articolele care nu au fost excluse prin filtrare pot fi selectate pentru examinare de către persoane autorizate" (Codul de bune practici privind interceptarea comunicațiilor, punctul 6.6, a se vedea nota de subsol 278).

([388]) A se vedea secțiunea 152 punctul 1 literele (a) și (b) din IPA din 2016, conform căreia examinarea ambelor tipuri de date (conținutul interceptat și datele secundare) trebuie efectuată numai în scopul specificat și trebuie să fie necesară și proporțională în toate circumstanțele.

([389]) Acest tip de mandat nu este necesar atunci când datele referitoare la persoanele care se află în Insulele Britanice sunt „date secundare" [a se vedea secțiunea 152 punctul 1 litera (c) din IPA din 2016].

([390]) Secțiunile 152 și 193 din IPA din 2016.

([391]) Secțiunile 155 și 196 din IPA din 2016.

(230) Evaluarea efectuată de către analist cu privire la selecția materialelor face obiectul unei supravegheri *ex post* de către IPC care evaluează respectarea garanțiilor specifice prevăzute în IPA din 2016 pentru etapa de examinare ([392]) (a se vedea, de asemenea, considerentul 229). IPC trebuie să monitorizeze (inclusiv prin audit, inspecție și investigație) exercitarea de către autoritățile publice a competențelor de investigare menționate în IPA din 2016 ([393]). În acest sens, Codul de bune practici privind interceptarea și Codul de bune practici privind intervenția asupra echipamentelor clarifică faptul că agenția trebuie să țină evidențe în scopul examinării și al auditurilor ulterioare, iar aceste evidențe trebuie să prezinte motivele pentru care accesul la materiale al persoanelor autorizate este necesar și proporțional, precum și scopurile operaționale aplicabile ([394]). De exemplu, în raportul său anual pe 2018, Biroul comisarului pentru competențe de investigare (IPCO) ([395]) a concluzionat că justificările înregistrate de analiști pentru examinarea anumitor materiale colectate în masă au respectat standardul de proporționalitate necesar, oferind detalii suficiente cu privire la motivele „interogărilor" lor în raport cu scopul care trebuie atins ([396]). În raportul său din 2019, în ceea ce privește competențele în masă, IPCO și-a exprimat în mod clar intenția de a continua inspecțiile interceptărilor în masă, inclusiv o examinare detaliată a selectoarelor și a criteriilor de căutare ([397]). De asemenea, IPCO va continua să examineze cu atenție, de la caz la caz, alegerea măsurilor de supraveghere (țintite sau în masă) atât în timpul examinării cererilor de mandat în temeiul procedurii de protecție dublă, cât și în timpul inspecțiilor ([398]). Această monitorizare suplimentară va fi luată în considerare în mod corespunzător în contextul monitorizării de către Comisie a prezentei decizii menționate în considerentele 281-284.

3.3.1.1.4.2. Achiziția în masă de date ale comunicațiilor

(231) Partea 6 capitolul 2 din IPA din 2016 reglementează mandatele de achiziție în masă care autorizează destinatarul să solicite unui operator de telecomunicații să divulge sau să obțină orice date ale comunicațiilor aflate în posesia operatorului. Aceste mandate autorizează, de asemenea, autoritatea solicitantă să selecteze datele pentru etapa următoare a examinării. La fel ca în cazul păstrării și al achiziției țintite a datelor comunicațiilor (a se vedea considerentul 199), nici achiziția în masă a datelor comunicațiilor nu se referă, în mod normal, la datele cu caracter personal ale persoanelor vizate din UE transferate în temeiul prezentei decizii către Regatul Unit. Obligația de a divulga date ale comunicațiilor în temeiul părții 6 capitolul 2 din IPA din 2016 se referă la datele care sunt colectate de operatorii de telecomunicații din Regatul Unit direct de la utilizatorii unui serviciu de telecomunicații ([399]). Acest tip de prelucrare „orientată către client" nu implică, de regulă, un transfer în temeiul prezentei decizii, și anume un transfer de la un operator/o persoană împuternicită de operator din UE către un operator/o persoană împuternicită de operator din Regatul Unit.

(232) Cu toate acestea, din motive de exhaustivitate, condițiile și garanțiile care reglementează achiziția de date ale comunicațiilor în masă sunt descrise mai jos.

([392]) Secțiunile 152 și 193 din IPA din 2016.

([393]) Secțiunea 229 din IPA din 2016.

([394]) Codul de bune practici privind interceptarea comunicațiilor, punctul 6.74, a se vedea nota de subsol 278, și Codul de bune practici privind intervenția asupra echipamentelor, punctul 6.78, a se vedea nota de subsol 348.

([395]) IPCO este constituit în temeiul secțiunii 238 din IPA din 2016 pentru a furniza IPC personalul, localurile, echipamentele și alte instalații și servicii necesare pentru îndeplinirea funcțiilor sale (a se vedea considerentul 251).

([396]) În raportul anual al IPCO pe 2018 s-a precizat că justificările înregistrate de analiștii GCHQ „au respectat standardul cerut, iar analiștii au contabilizat suficient de detaliat proporționalitatea interogărilor lor de date colectate în masă". Raportul anual pe 2018 al comisarului pentru competențe de investigare, punctul 6.22, a se vedea nota de subsol 464.

([397]) Raportul anual pe 2019 al comisarului pentru competențe de investigare, punctul 7.6, a se vedea nota de subsol 463.

([398]) Raportul anual pe 2019 al comisarului pentru competențe de investigare, punctul 10.22, a se vedea nota de subsol 463.

([399]) Acest lucru rezultă din definiția datelor comunicațiilor, prevăzută la secțiunea 261 punctul 5 din IPA din 2016, potrivit căreia datele comunicațiilor sunt deținute sau obținute de un operator de telecomunicații și fie se referă la utilizatorul unui serviciu de telecomunicații și la furnizarea acestui serviciu, fie sunt cuprinse într-o comunicație, incluse ca parte integrantă în aceasta, atașate la aceasta sau asociate în mod logic acesteia (a se vedea, de asemenea, Codul de bune practici privind achiziția în masă a datelor comunicațiilor, disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, punctele 2.15-2.22). În plus, definiția operatorului de telecomunicații prevăzută în secțiunea 261 punctul 10 din IPA din 2016 impune ca un operator de telecomunicații să fie o persoană care oferă sau furnizează un serviciu de telecomunicații unor persoane din Regatul Unit sau care controlează sau furnizează o rețea de telecomunicații aflată (integral sau parțial) în Regatul Unit sau controlată din Regatul Unit. Aceste definiții clarifică faptul că obligațiile prevăzute de IPA din 2016 nu pot fi impuse operatorilor de telecomunicații ale căror echipamente nu se află în Regatul Unit sau nu sunt controlate din Regatul Unit și care nu oferă sau nu furnizează servicii persoanelor din Regatul Unit (a se vedea, de asemenea, Codul de bune practici privind achiziția în masă a datelor comunicațiilor, punctul 2.2). În cazul în care abonații din UE (indiferent dacă se află în UE sau în Regatul Unit) ar utiliza servicii în Regatul Unit, orice comunicații în legătură cu furnizarea acestui serviciu ar fi colectate direct de către furnizorul de servicii din Regatul Unit, mai degrabă decât să facă obiectul unui transfer din UE.

(233) IPA din 2016 înlocuiește legislația privind achiziția de date ale comunicațiilor în masă, care a făcut obiectul hotărârii CJUE în cauza *Privacy International*. Legislația în discuție în această cauză a fost abrogată, iar noul regim prevede condiții și garanții specifice în temeiul cărora poate fi autorizată o astfel de măsură.

(234) În special, spre deosebire de regimul anterior în care secretarul de stat dispunea de o putere de apreciere deplină în ceea ce privește autorizarea măsurii ([400]), IPA din 2016 impune secretarului de stat să emită un mandat numai dacă măsura este necesară și proporțională. În practică, aceasta înseamnă că ar trebui să existe o legătură între accesul la date și scopul urmărit ([401]). Mai precis, secretarul de stat va trebui să evalueze existența unei legături între măsura solicitată și unul sau mai multe „scopuri operaționale" indicate în mandat (a se vedea considerentul 219) în ceea ce privește evaluarea proporționalității, codul de bune practici relevant precizând că „secretarul de stat trebuie să analizeze dacă ceea ce se urmărește a fi obținut prin mandat ar putea fi obținut în mod rezonabil prin alte mijloace mai puțin invazive [secțiunea 2 punctul 2 litera (a) din lege]. De exemplu, obținerea informațiilor necesare prin intermediul unei competențe mai puțin intruzive, cum ar fi achiziția țintită de date ale comunicațiilor" ([402]).

(235) Pentru a efectua o astfel de evaluare, secretarul de stat se va baza pe informații pe care șefii serviciilor de informații ([403]) sunt obligați să le prezinte în cererea lor, cum ar fi motivele pentru care măsura este considerată necesară pentru unul dintre temeiurile legale și motivele pentru care ceea ce se urmărește a fi obținut nu ar putea fi obținut în mod rezonabil prin alte mijloace mai puțin intruzive ([404]). În plus, scopurile operaționale limitează domeniul de aplicare pentru care datele obținute în temeiul mandatului pot fi selectate pentru examinare ([405]). Astfel cum se specifică în codul de bune practici relevant, scopurile operaționale trebuie să descrie o cerință clară și să conțină suficiente detalii pentru a convinge secretarul de stat că datele obținute pot fi selectate pentru examinare numai din motive specifice ([406]). Astfel, secretarul de stat va trebui să se asigure, înainte de a autoriza mandatul, că sunt în vigoare mecanisme specifice pentru a se asigura că numai materialele care au fost considerate necesare pentru examinare în scopuri operaționale și statutare sunt selectate pentru examinare și că acestea trebuie să fie proporționale și necesare în orice circumstanță. Această cerință specifică, reflectată în secțiunile 158 și 172 ([407]) din IPA din 2016, referitoare la evaluarea prealabilă a necesității și proporționalității criteriilor utilizate în scopul selecției, reprezintă o altă noutate importantă a regimului introdus prin IPA din 2016 în comparație cu regimul existent anterior.

(236) IPA din 2016 a introdus, de asemenea, obligația secretarului de stat de a se asigura că, înainte de emiterea mandatului pentru achiziția în masă a datelor comunicațiilor, sunt instituite limitări specifice privind securitatea, păstrarea și divulgarea datelor cu caracter personal colectate ([408]). În cazul divulgării în străinătate, garanțiile, descrise în considerentul 227, pentru interceptarea în masă și intervenția în masă asupra echipamentelor, se aplică și în acest context ([409]). Legislația prevede și alte limitări privind durata ([410]), reînnoirea ([411]) și modificarea mandatelor în masă ([412]).

(237) Este important de remarcat faptul că, la fel ca în cazul celorlalte competențe în masă, înainte de emiterea mandatului, secretarul de stat trebuie să obțină aprobarea unui comisar judiciar ([413]). Aceasta este o caracteristică esențială a regimului instituit prin IPA din 2016.

([400]) Secțiunea 94 punctul 1 din *Telecommunications Act 1984* (Legea privind telecomunicațiile din 1984) prevedea că secretarul de stat poate emite „instrucțiuni cu caracter general, pe care secretarul de stat le consideră necesare sau oportune în interesul securității naționale […]" (a se vedea nota de subsol 451).

([401]) A se vedea *Privacy International*, punctul 78.

([402]) A se vedea Codul de bune practici privind achiziția în masă a datelor comunicațiilor, punctul 4.11 (a se vedea nota de subsol 399414).

([403]) Un mandat de achiziție în masă poate fi solicitat numai de către șefii serviciilor de informații care sunt: (i) directorul general al Serviciului de Securitate; (ii) șeful Serviciului Secret de Informații; sau (iii) directorul GCHQ (a se vedea secțiunile 158 și 263 din IPA din 2016).

([404]) Codul de bune practici privind achiziția în masă a datelor comunicațiilor, punctul 4.5 (a se vedea nota de subsol 399).

([405]) În conformitate cu secțiunea 161 din IPA din 2016, scopurile operaționale specificate în mandat trebuie să fie cele specificate, într-o listă gestionată de șefii serviciilor de informații (denumită în continuare „lista scopurilor operaționale"), drept scopuri pe care aceștia le consideră scopuri operaționale în care datele comunicațiilor obținute în temeiul mandatelor de achiziție în masă pot fi selectate în vederea examinării.

([406]) Codul de bune practici privind achiziția în masă a datelor comunicațiilor, punctul 6.6 (a se vedea nota de subsol 399).

([407]) Secțiunea 172 din IPA din 2016 prevede obligativitatea instituirii de garanții specifice pentru etapa de filtrare și selecție pentru examinarea datelor comunicațiilor dobândite în masă. În plus, o examinare deliberată care încalcă aceste garanții constituie, de asemenea, o infracțiune (a se vedea secțiunea 173 din IPA din 2016).

([408]) Secțiunea 171 din IPA din 2016.

([409]) Secțiunea 171 punctul 9 din IPA din 2016.

([410]) Secțiunea 162 din IPA din 2016.

([411]) Secțiunea 163 din IPA din 2016.

([412]) Secțiunile 164-166 din IPA din 2016.

([413]) Secțiunea 159 din IPA din 2016.

(238) IPC efectuează o supraveghere *ex post* a procedurii de examinare a materialelor (date ale comunicațiilor) dobândite în masă (a se vedea considerentul 254). În această privință, IPA din 2016 a introdus cerința potrivit căreia analistul de informații care efectuează examinarea trebuie să înregistreze, înainte de selectarea datelor pentru examinare, motivul pentru care examinarea propusă este necesară și proporțională într-un anumit scop operațional ([414]). În raportul anual al IPCO pe 2019 s-a constatat, în ceea ce privește practica GCHQ și a MI5, că „rolul esențial al datelor comunicațiilor colectate în masă pentru gama de activități desfășurate la GCHQ a fost bine articulat în cazurile pe care le-am inspectat. Am analizat natura datelor solicitate și cerințele declarate în materie de informații și am fost mulțumiți de faptul că documentația a demonstrat că abordarea acestora este necesară și proporțională" ([415]). Justificările înregistrate de MI5 au fost la un standard adecvat și au respectat principiile necesității și proporționalității" ([416]).

3.3.1.1.4.3. Păstrarea și examinarea seturilor de date cu caracter personal colectate în masă

(239) Mandatele pentru seturile de date cu caracter personal colectate în masă (BPD – *Bulk Personal Dataset*) ([417]) autorizează agențiile de informații să păstreze și să examineze seturi de date care conțin date cu caracter personal referitoare la o serie de persoane. Potrivit explicațiilor furnizate de autoritățile Regatului Unit, analiza acestor seturi de date poate fi „singura modalitate pentru ca UKIC să înregistreze progrese în cadrul investigațiilor și să identifice teroriștii dintr-un număr foarte limitat de informații de bază sau atunci când comunicațiile acestora au fost ascunse în mod deliberat" ([418]). Există două tipuri de mandate: „mandate din clasa BPD" ([419]) care se referă la o anumită categorie de seturi de date, și anume seturi de date care sunt similare din punctul de vedere al conținutului și al utilizării propuse și care prezintă considerații similare cu privire, de exemplu, la gradul de intruziune și sensibilitate și la proporționalitatea utilizării datelor, permițând astfel secretarului de stat să analizeze necesitatea și proporționalitatea obținerii simultane a tuturor datelor în cadrul clasei relevante. De exemplu, un mandat din clasa BPD poate acoperi seturile de date de călătorie care se referă la rute similare ([420]). „Mandate BPD specifice" ([421]) se referă în schimb la un set de date specific, cum ar fi un set de date aferent unui tip nou sau neobișnuit de informații care nu se încadrează într-un mandat existent din clasa BPD sau un set de date care se referă la anumite tipuri de date cu caracter personal ([422]) și care, prin urmare, necesită garanții suplimentare ([423]). Dispozițiile IPA din 2016 referitoare la BPD permit examinarea și păstrarea acestor seturi de date numai în cazul în care acest lucru este necesar și proporțional ([424]) și în conformitate cu obligațiile generale privind viața privată ([425]).

(240) Competența de a emite un mandat BPD face obiectul procedurii de „protecție dublă": evaluarea necesității și a proporționalității măsurii este efectuată mai întâi de secretarul de stat și apoi de comisarul judiciar ([426]). Secretarul de stat trebuie să analizeze natura și domeniul de aplicare al tipului de mandat solicitat, categoria de date în cauză și numărul de seturi individuale de date cu caracter personal colectate în masă care ar putea intra sub incidența tipului specific de mandat ([427]). De asemenea, astfel cum se specifică în Codul de bune practici privind păstrarea și utilizarea de către serviciile de informații a seturilor de date cu caracter personal colectate în masă, trebuie păstrate evidențe detaliate care fac obiectul auditului IPC ([428]). Păstrarea și examinarea BPD în afara limitelor instituite de IPA din 2016 constituie o infracțiune ([429]).

([414]) Raportul anual al IPCO pe 2019, punctul 8.6, a se vedea nota de subsol 463.
([415]) Raportul anual al IPCO pe 2019, punctul 10.4, a se vedea nota de subsol 463.
([416]) Raportul anual al IPCO pe 2019, punctul 8.37, a se vedea nota de subsol 463.
([417]) Secțiunea 200 din IPA din 2016.
([418]) Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat, secțiunea H: Securitatea națională, pagina 34, a se vedea nota de subsol 29.
([419]) Secțiunea 204 din IPA din 2016.
([420]) Codul de bune practici privind păstrarea și utilizarea de către serviciile de informații a seturilor de date cu caracter personal colectate în masă, punctul 4.7, disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf
([421]) Secțiunea 205 din IPA din 2016.
([422]) Cum ar fi, de exemplu, datele sensibile cu caracter personal, a se vedea secțiunea 202 din IPA din 2016 și Codul de bune practici privind păstrarea și utilizarea de către serviciile de informații a seturilor de date cu caracter personal colectate în masă, punctele 4.21 și 4.12, a se vedea nota de subsol 469.
([423]) O cerere pentru un mandat BPD specific trebuie să fie analizată individual de către secretarul de stat, și anume în ceea ce privește un set de date specific. Conform secțiunii 205 din IPA, serviciul de informații trebuie să includă în cererea sa de solicitare a unui mandat BPD specific o explicație detaliată a naturii și a amplorii materialelor în cauză, precum și o listă a „scopurilor operaționale" pentru care serviciul de informații relevant dorește să examineze BPD (în cazul în care serviciul de informații solicită un mandat de păstrare și examinare, mai degrabă decât doar de păstrare). Atunci când emite un mandat din clasa BPD, secretarul analizează, în schimb, întreaga categorie de seturi de date simultan.
([424]) Secțiunile 204 și 205 din IPA din 2016.
([425]) Secțiunea 2 din IPA din 2016.
([426]) Secțiunile 204 și 205 din IPA din 2016.
([427]) Codul de bune practici privind păstrarea și utilizarea de către serviciile de informații a seturilor de date cu caracter personal colectate în masă, punctul 5.2, a se vedea nota de subsol 420.
([428]) Codul de bune practici privind păstrarea și utilizarea de către serviciile de informații a seturilor de date cu caracter personal colectate în masă, punctele 8.1-8.15, a se vedea nota de subsol 420.
([429]) Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat, secțiunea H: Securitatea națională, pagina 34, a se vedea nota de subsol 29.

3.3.2. *Utilizarea ulterioară a informațiilor colectate*

(241) Datele cu caracter personal prelucrate în temeiul părții 4 din DPA din 2018 nu trebuie prelucrate într-un mod incompatibil cu scopul pentru care au fost colectate ([430]). DPA din 2018 prevede că operatorul poate prelucra datele în alt scop, diferit de cel pentru care au fost colectate, atunci când acesta este compatibil cu cel inițial și cu condiția ca operatorul să fie autorizat prin lege să prelucreze datele și ca prelucrarea să fie necesară și proporțională ([431]). În plus, Legea privind serviciul de securitate din 1989 și Legea privind serviciile de informații din 1994 precizează că șefii serviciilor de informații au datoria de a se asigura că nicio informație nu este obținută sau divulgată decât în măsura în care acest lucru este necesar pentru îndeplinirea corespunzătoare a funcțiilor agenției sau în alte scopuri limitate și specifice enumerate în dispozițiile relevante ([432]).

(242) În plus, secțiunea 109 din DPA din 2018 stabilește cerințe specifice pentru transferurile internaționale de date cu caracter personal de către serviciile de informații către țări terțe sau organizații internaționale. Conform acestei dispoziții, datele cu caracter personal nu pot fi transferate către o țară sau un teritoriu din afara Regatului Unit sau către o organizație internațională decât în cazul în care transferul este necesar și proporțional în scopul îndeplinirii funcțiilor statutare ale operatorului sau în alte scopuri prevăzute în secțiunea 2 punctul 2 litera (a) din Legea privind serviciul de securitate din 1989 sau în secțiunea 2 punctul 2 litera (a) și secțiunea 4 punctul 2 litera (a) din Legea privind serviciile de informații din 1994 ([433]). Este important de remarcat faptul că aceste cerințe se aplică, de asemenea, în cazurile în care se invocă derogarea în materie de securitate națională în temeiul secțiunii 110 din DPA din 2018, întrucât secțiunea 110 din DPA din 2018 nu enumeră secțiunea 109 din DPA din 2018 drept una dintre dispozițiile care pot să nu fie aplicate în cazul în care este necesară o derogare de la anumite dispoziții în scopul protejării securității naționale.

(243) În plus, astfel cum a subliniat ICO în orientările sale privind prelucrarea de către serviciile de informații, pe lângă garanțiile prevăzute în partea 4 din DPA din 2018, o agenție de informații, atunci când face schimb de date cu un organism de informații dintr-o țară terță, face, de asemenea, obiectul garanțiilor oferite de alte măsuri legislative care li se aplică pentru a se asigura că datele cu caracter personal sunt obținute, partajate și gestionate în mod legal și responsabil ([434]). De exemplu, IPA din 2016 stabilește garanții suplimentare în ceea ce privește transferurile către o țară terță de materiale colectate prin interceptare țintită ([435]), intervenție țintită asupra echipamentelor ([436]), interceptare în masă ([437]), achiziția în masă de date ale comunicațiilor ([438]) și intervenție în masă asupra echipamentelor ([439]) (așa-numitele „divulgări în străinătate"). În special, autoritatea care emite mandatul trebuie să se asigure că sunt instituite mecanisme pentru a se asigura că țara terță care primește datele limitează la minimul necesar, în scopurile autorizate prevăzute în IPA din 2016, numărul de persoane care văd materialele, amploarea divulgării și numărul de copii realizate de pe orice materiale ([440]).

3.3.3. *Supravegherea*

(244) Accesul administrației publice în scopuri de securitate națională este supravegheat de o serie de organisme diferite. Comisarul pentru informații supraveghează prelucrarea datelor cu caracter personal în lumina DPA din 2018 (pentru mai multe informații privind independența, rolul de numire și competențele comisarului, a se vedea considerentele 85-98), în timp ce IPC asigură supravegherea independentă și judiciară a utilizării competențelor de

([430]) Secțiunea 87 punctul 1 din DPA din 2018.

([431]) Secțiunea 87 punctul 3 din DPA din 2018. Deși operatorii pot fi scutiți de la respectarea acestui principiu în temeiul secțiunii 110 din DPA din 2018, în măsura în care o astfel de derogare este necesară pentru a proteja securitatea națională, derogarea în cauză trebuie să fie evaluată de la caz la caz și poate fi invocată numai în măsura în care aplicarea unei anumite dispoziții ar avea consecințe negative asupra securității naționale (a se vedea considerentul 132). Certificatele de securitate națională pentru serviciile de informații din Regatul Unit (disponibile la următoarea adresă: https://ico.org.uk/about-the-ico/our-information/national-security-certificates) nu acoperă secțiunea 87 punctul 3 din DPA din 2018. În plus, întrucât orice prelucrare în alt scop trebuie să fie autorizată prin lege, serviciile de informații trebuie să aibă un temei juridic clar pentru prelucrarea ulterioară.

([432]) Pentru mai multe informații privind aceste scopuri, a se vedea nota de subsol 312.

([433]) A se vedea nota de subsol 312.

([434]) Orientările ICO privind prelucrarea de către serviciile de informații (a se vedea nota de subsol 161).

([435]) Secțiunea 54 din IPA din 2016.

([436]) Secțiunea 130 din IPA din 2016.

([437]) Secțiunea 151 din IPA din 2016.

([438]) Secțiunea 171 punctul 9 din IPA din 2016.

([439]) Secțiunea 192 din IPA din 2016.

([440]) Mecanismele trebuie să includă măsuri de asigurare a faptului că fiecare copie realizată de pe oricare dintre aceste materiale este stocată, pe perioada păstrării, în condiții de siguranță. Materialele obținute în temeiul unui mandat și fiecare copie a oricăruia dintre aceste materiale trebuie distruse de îndată ce nu mai există motive relevante pentru a fi păstrate (a se vedea secțiunea 150 punctul 2, secțiunea 150 punctul 5 și secțiunea 151 punctul 2 din IPA din 2016). Trebuie remarcat faptul că garanții similare, prevăzute în cadrul juridic anterior (RIPA din 2000), au fost considerate conforme cu cerințele stabilite de Curtea Europeană a Drepturilor Omului pentru schimbul de materiale obținute prin interceptarea în masă cu state străine sau cu organizații internaționale [Curtea Europeană a Drepturilor Omului (Marea Cameră), Big Brother Watch și alții/Regatul Unit (a se vedea nota de subsol 279 de mai sus), punctele 362 și 399].

investigare în temeiul IPA din 2016. IPC supraveghează utilizarea competențelor de investigare prevăzute în IPA din 2016 atât de către autoritățile de aplicare a legii, cât și de către autoritățile de securitate națională. Supravegherea politică este garantată de Comisia pentru serviciile de informații din cadrul Parlamentului.

3.3.3.1. Supravegherea în temeiul părții 4 din DPA

(245) Prelucrarea datelor cu caracter personal efectuată de serviciile de informații în temeiul părții 4 din DPA din 2018 este supravegheată de comisarul pentru informații ([441]).

(246) Funcțiile generale ale comisarului pentru informații în ceea ce privește prelucrarea datelor cu caracter personal de către serviciile de informații în temeiul părții 4 din DPA din 2018 sunt prevăzute în anexa 13 la DPA din 2018. Sarcinile includ, însă nu se limitează la monitorizarea și punerea în aplicare a părții 4 din DPA din 2018, promovarea sensibilizării publicului, consilierea Parlamentului, a guvernului și a altor instituții cu privire la măsurile legislative și administrative, promovarea sensibilizării operatorilor și a persoanelor împuternicite de operatori cu privire la obligațiile ce le revin, furnizarea de informații unei persoane vizate cu privire la exercitarea drepturilor persoanei vizate, desfășurarea de anchete etc.

(247) În ceea ce privește partea 3 din DPA din 2018, comisarul are competența de a informa operatorii cu privire la o presupusă încălcare și de a emite avertismente cu privire la probabilitatea ca o prelucrare să încalce normele și de a emite mustrări atunci când încălcarea este confirmată. De asemenea, acesta poate emite notificări de executare și de sancționare pentru încălcarea anumitor dispoziții ale legii ([442]). Cu toate acestea, spre deosebire de alte părți din DPA din 2018, comisarul nu poate emite o notificare de evaluare adresată unui organism de securitate națională ([443]).

(248) În plus, secțiunea 110 din DPA din 2018 prevede o excepție de la utilizarea anumitor competențe ale comisarului atunci când acest lucru este necesar în scopul protejării securității naționale. Aceasta include competența comisarului de a emite (orice tip de) notificări în temeiul DPA (notificări de informare, de evaluare, de executare și de sancționare), competența de a efectua inspecții în conformitate cu obligațiile internaționale, competențe de intrare și de inspecție, precum și norme privind infracțiunile ([444]). Astfel cum se explică în considerentul 126, aceste excepții se vor aplica numai dacă sunt necesare și proporționale și de la caz la caz.

(249) ICO și serviciile de informații din Regatul Unit au semnat un memorandum de înțelegere ([445]) care stabilește un cadru de cooperare cu privire la o serie de aspecte, inclusiv notificări privind încălcarea securității datelor și tratarea plângerilor persoanelor vizate. În special, acesta prevede că, la primirea unei plângeri, ICO va evalua dacă a fost utilizată în mod corespunzător aplicarea vreunei derogări în materie de securitate națională. Răspunsurile la întrebările adresate de ICO în contextul examinării plângerilor individuale trebuie să fie furnizate de către agenția de informații în cauză în termen de 20 de zile lucrătoare, utilizând canale securizate adecvate, în cazul în care acestea implică informații clasificate. Din aprilie 2018 până în prezent, ICO a primit 21 de plângeri de la persoane fizice cu privire la serviciile de informații. Fiecare plângere a fost evaluată, iar rezultatul a fost comunicat persoanei vizate ([446]).

([441]) Secțiunea 116 din DPA din 2018.

([442]) În conformitate cu punctul 2 din anexa 13 la DPA din 2018, notificările de punere în aplicare și de sancționare pot fi transmise unui operator sau unei persoane împuternicite de operator în legătură cu încălcări ale părții 4 capitolul 2 din DPA din 2018 (principiile prelucrării), ale unei dispoziții a părții 4 din DPA din 2018 ce conferă drepturi unei persoane vizate, ale cerinței de a comunica o încălcare a securității datelor cu caracter personal comisarului în temeiul secțiunii 108 din DPA din 2018 și ale principiilor privind transferurile de date cu caracter personal către țări terțe, țări care nu participă la convenție și organizații internaționale din secțiunea 109 din DPA din 2018 (pentru detalii suplimentare privind notificările de executare și de sancționare, a se vedea considerentul 92).

([443]) În temeiul secțiunii 147 punctul 6 din DPA din 2018, comisarul pentru informații nu poate transmite o notificare de evaluare organismelor menționate la secțiunea 23 punctul 3 din Legea din 2000 privind liberul acces la informațiile de interes public. Printre acestea se numără Serviciul de Securitate (MI5), Serviciul Secret de Informații (MI6) și Cartierul General pentru Comunicații.

([444]) Dispozițiile care pot fi exceptate sunt: secțiunea 108 (informarea comisarului cu privire la încălcarea securității datelor cu caracter personal), secțiunea 119 (inspecție în conformitate cu obligațiile internaționale); secțiunile 142-154 și anexa 15 (Notificările comisarului și competențele de intrare și de inspecție); și secțiunile 170-173 (infracțiuni legate de datele cu caracter personal). În plus, în ceea ce privește prelucrarea de către serviciile de informații din anexa 13 (alte funcții generale ale comisarului), punctul 1 literele (a) și (g) și punctul 2.

([445]) Memorandumul de înțelegere dintre Biroul comisarului pentru informații și serviciile de informații din Regatul Unit, a se vedea nota de subsol 165.

([446]) În șapte dintre aceste cazuri, ICO a recomandat reclamantului să prezinte problema în fața operatorului de date (acest lucru este valabil atunci când o persoană fizică a prezentat o problemă în fața ICO, dar ar fi trebuit să o prezinte mai întâi în fața operatorului de date), în unul dintre aceste cazuri, ICO a oferit consiliere generală operatorului de date (această procedură este utilizată atunci când acțiunile operatorului nu par să fi încălcat legislația, dar este posibil ca o îmbunătățire a practicilor să fi evitat prezentarea problemei în fața ICO), iar în celelalte 13 cazuri, operatorul nu a avut obligația de a întreprinde nicio acțiune (această procedură este utilizată atunci când problemele prezentate de persoana fizică intră sub incidența Legii privind protecția datelor din 2018 deoarece se referă la prelucrarea informațiilor cu caracter personal, dar, pe baza informațiilor furnizate de operator, nu par să fi încălcat legislația).

3.3.3.2. Supravegherea utilizării competențelor de investigare în temeiul IPA din 2016

(250) În conformitate cu partea 8 din IPA din 2016, supravegherea utilizării competențelor de investigare este exercitată de comisarul pentru competențe de investigare (IPC). IPC este asistat de alți comisari judiciari, care sunt denumiți în mod colectiv comisari judiciari ([447]). IPA din 2016 stabilește garanțiile care protejează independența comisarilor judiciari. Comisarii judiciari trebuie să dețină sau să fi deținut o înaltă funcție judiciară ([448]) (adică să fie sau să fi fost membri ai instanțelor de cel mai înalt grad) și, ca orice membru al sistemului judiciar, aceștia beneficiază de un statut independent față de guvern ([449]). În temeiul secțiunii 227 din IPA din 2016, prim-ministrul este cel care numește IPC și numărul de comisari judiciari pe care îl consideră necesar. Toți comisarii, indiferent dacă sunt actuali sau foști membri ai sistemului judiciar, pot fi numiți numai pe baza unei recomandări comune din partea celor trei judecători șefi (Chief Justices) pentru Anglia & Țara Galilor, Scoția și Irlanda de Nord și Lord Cancelar ([450]). Secretarul de stat trebuie să furnizeze IPC personal, localuri, echipamente și alte instalații și servicii ([451]). Mandatul comisarilor este de trei ani, aceștia putând fi numiți din nou ([452]). Ca o garanție suplimentară a independenței lor, comisarii judiciari pot fi revocați din funcție numai în condiții stricte care impun un prag ridicat: fie de către prim-ministru în circumstanțele specifice enumerate în mod exhaustiv în secțiunea 228 punctul 5 din IPA din 2016 (cum ar fi falimentul sau încarcerarea), fie în cazul în care fiecare cameră a Parlamentului a adoptat o hotărâre de aprobare a revocării ([453]).

(251) IPC și comisarii judiciari sunt sprijiniți în ceea ce privește rolurile lor de către Biroul comisarului pentru competențe de investigare (IPCO). Personalul IPCO include o echipă de inspectori, expertiză juridică și tehnică internă și un grup consultativ tehnologic care oferă consultanță de specialitate. La fel ca în cazul comisarilor judiciari individuali, independența IPCO este protejată. IPCO este un „organism independent" (*arm's-length body*) în cadrul Ministerului de Interne, și anume primește finanțare din partea Ministerului de Interne, dar își îndeplinește funcțiile în mod independent ([454]).

(252) Principalele funcții ale comisarilor judiciari sunt stabilite în secțiunea 229 din IPA din 2016 ([455]). În special, comisarii judiciari dispun de o competență extinsă de aprobare prealabilă, care face parte din garanțiile introduse în cadrul juridic al Regatului Unit prin IPA din 2016. Mandatele în legătură cu interceptarea țintită, intervenția asupra echipamentelor, seturile de date cu caracter personal colectate în masă, achiziția în masă a datelor comunicațiilor, precum și notificările de păstrare a datelor comunicațiilor trebuie să fie aprobate de comisarii judiciari ([456]). De asemenea, IPC trebuie să pre-autorizeze întotdeauna achiziția datelor comunicațiilor în scopul asigurării respectării legii ([457]). În cazul în care un comisar refuză să aprobe un mandat, secretarul de stat poate depune o contestație la comisarul pentru competențe de investigare, a cărui decizie este definitivă.

([447]) În conformitate cu secțiunea 227 punctele 7 și 8 din IPA din 2016, comisarul pentru competențe de investigare este un comisar judiciar, iar comisarul pentru competențe de investigare și ceilalți comisari judiciari sunt cunoscuți, în mod colectiv, sub denumirea de comisari judiciari. În prezent, există 15 comisari judiciari.

([448]) În conformitate cu secțiunea 60 punctul 2 din partea 3 din *Constitutional Reform Act 2005* (Legea din 2005 privind reforma constituțională), o „înaltă funcție judiciară" înseamnă funcția de judecător în cadrul oricăreia dintre următoarele instanțe: (i) Curtea Supremă; (ii) Curtea de Apel din Anglia și Țara Galilor; (iii) Înalta Curte din Anglia și Țara Galilor; (iv) *Court of Session;* (v) Curtea de Apel din Irlanda de Nord; (vi) Înalta Curte din Irlanda de Nord; sau în calitate de *Lord of Appeal in Ordinary*.

([449]) Independența sistemului judiciar se bazează pe convenție și a fost recunoscută pe scară largă începând cu *1701 Act of Settlement*.

([450]) Secțiunea 227 punctul 3 din IPA din 2016. Comisarii judiciari trebuie să fie recomandați și de către comisarul pentru competențe de investigare, astfel cum se prevede în secțiunea 227 punctul 4 litera (e) din IPA din 2016.

([451]) Secțiunea 238 din IPA din 2016.

([452]) Secțiunea 227 punctul 2 din IPA din 2016.

([453]) Procesul de revocare este identic cu procesul de revocare pentru alți judecători din Regatul Unit [a se vedea, de exemplu, secțiunea 11 punctul 3 din *Senior Courts Act 1981* (Legea din 1981 privind instanțele superioare) și secțiunea 33 din Legea din 2005 privind reforma constituțională, care impun, de asemenea, o hotărâre în urma aprobării de către ambele camere ale Parlamentului]. Până în prezent, niciun comisar judiciar nu a fost revocat din funcție.

([454]) Un „organism independent" (*arm's-length body*) este o organizație sau o agenție care primește finanțare de la un guvern, dar care este în măsură să acționeze independent (pentru o definiție și mai multe informații cu privire la un organism care funcționează în condiții de concurență deplină, a se vedea Manualul Cabinetului privind clasificarea organismelor publice, disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf și primul raport al sesiunii 2014-2015 al Comisiei speciale pentru administrație publică a Camerei Comunelor, disponibil la următoarea adresă: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf).

([455]) În conformitate cu secțiunea 229 din IPA din 2016, comisarul judiciar are competențe extinse de supraveghere, care acoperă, de asemenea, supravegherea păstrării și a divulgării datelor colectate de agențiile de informații.

([456]) Deciziile privind aprobarea unei decizii a secretarului de stat de emitere a unui mandat țin de competența comisarilor judiciari înșiși. În cazul în care un comisar refuză să aprobe un mandat, secretarul de stat poate depune o contestație la comisarul pentru competențe de investigare, a cărui decizie este definitivă.

([457]) Autorizația IPC este întotdeauna solicitată în cazul în care datele comunicațiilor sunt obținute în scopul asigurării respectării legii (secțiunea 60A din IPA din 2016). În cazul în care datele comunicațiilor sunt obținute în scopul securității naționale, autorizația poate fi acordată de IPC sau, în mod alternativ, de un înalt funcționar desemnat al autorității publice relevante (a se vedea secțiunile 61 și 61A din IPA din 2016 și considerentul 203).

(253) Raportorul special al ONU privind dreptul la viață privată a salutat înființarea comisarilor judiciari în temeiul IPA din 2016, deoarece „toate cererile mai sensibile sau mai intruzive de a efectua supravegherea trebuie să fie autorizate atât de un ministru al Cabinetului, cât și de Biroul comisarului pentru competențe de investigare". În special, acesta a subliniat că „acest element al controlului jurisdicțional [prin rolul IPC], alături de o echipă cu resurse mai bune de inspectori și experți cu experiență în domeniul tehnologiei, reprezintă una dintre cele mai importante garanții noi introduse de IPA", care a înlocuit un sistem anterior fragmentat de autorități de supraveghere și completează rolul Comisiei pentru Informații și Securitate a Parlamentului și al Tribunalului cu competențe de investigare" ([458]).

(254) În plus, IPC are competența de a efectua o supraveghere *ex post*, inclusiv prin audit, inspecție și investigație, a utilizării competențelor de investigare în temeiul IPA din 2016 ([459]) și a altor competențe și funcții prevăzute în legislația relevantă ([460]). Rezultatele acestei supravegheri *ex post* sunt incluse în raportul pe care IPC trebuie să îl întocmească anual și să îl prezinte prim-ministrului ([461]) și care trebuie publicat și prezentat Parlamentului ([462]). Raportul conține statistici și informații relevante cu privire la utilizarea competențelor de investigare de către serviciile de informații și autoritățile de aplicare a legii, precum și cu privire la utilizarea garanțiilor în ceea ce privește articolele care fac obiectul secretului profesional al avocatului, materialele jurnalistice confidențiale și sursele de informare jurnalistice, informații privind măsurile luate și scopurile operaționale utilizate în contextul mandatelor în masă. În cele din urmă, în raportul anual al IPCO se specifică în ce domeniu au fost adresate recomandări autorităților publice și modul în care acestea au fost abordate ([463]).

(255) În conformitate cu secțiunea 231 din IPA din 2016, în cazul în care IPC ia cunoștință de o eroare relevantă comisă de autoritățile publice în exercitarea competențelor lor de investigare, acesta trebuie să informeze persoana în cauză atunci când consideră că eroarea este gravă și că este în interesul public ca persoana în cauză să fie informată ([464]). În special, secțiunea 231 din IPA din 2016 precizează că, atunci când informează o persoană cu privire la o eroare, IPC trebuie să furnizeze informații cu privire la orice drept al acesteia de a se adresa Tribunalului cu competențe de investigare și să furnizeze detaliile pe care comisarul le consideră necesare pentru exercitarea acestor drepturi și dacă există un interes public pentru divulgare ([465]).

([458]) Declarația de sfârșit de mandat a Raportorului special privind dreptul la viață privată la încheierea misiunii sale în Regatul Unit al Marii Britanii și Irlandei de Nord (a se vedea nota de subsol 281).

([459]) Secțiunea 229 din IPA din 2016. Competențelor de investigare și în materie de informații ale comisarilor judiciari sunt stabilite în secțiunea 235 din IPA din 2016.

([460]) Aceasta include măsuri de supraveghere în temeiul RIPA din 2000, exercitarea funcțiilor în temeiul părții 3 din *Police Act 1997* – Legea privind poliția din 1997 (autorizarea acțiunii în ceea ce privește bunurile) și exercitarea de către secretarul de stat a funcțiilor în temeiul secțiunilor 5-7 din Legea privind serviciile de informații din 1994 (mandate pentru intervenția asupra radiotelegrafiei, intrarea și intervenția asupra bunurilor (secțiunea 229 din IPA din 2016).

([461]) Secțiunea 230 din IPA din 2016. IPC poate, de asemenea, să raporteze prim-ministrului din proprie inițiativă cu privire la orice aspect legat de funcțiile sale. IPC trebuie, de asemenea, să raporteze prim-ministrului la cererea acestuia, iar prim-ministrul poate solicita IPC să revizuiască orice funcție a serviciilor de informații.

([462]) Unele părți pot fi excluse dacă publicarea lor ar contraveni securității naționale.

([463]) De exemplu, în raportul anual al IPCO pe 2019 (punctul 6.38) se menționează că MI5 i s-a recomandat să își modifice politica de păstrare pentru seturile de date cu caracter personal colectate în masă (BPD), deoarece ar fi trebuit să adopte o abordare în care să se ia în considerare proporționalitatea păstrării pentru toate câmpurile din bazele BPD deținute și pentru fiecare BPD deținut. La sfârșitul anului 2018, IPCO nu a considerat că această recomandare a fost respectată, iar raportul din 2019 a explicat că MI5 introduce în prezent un nou proces de îndeplinire a acestei cerințe. Raportul anual pe 2019 (punctul 8.22) menționează, de asemenea, că GHCQ a primit o serie de recomandări cu privire la evidența proporționalității interogărilor sale privind datele colectate în masă. Raportul confirmă faptul că s-au realizat îmbunătățiri în acest domeniu la sfârșitul anului 2018. Raportul anual pe 2019 al Biroului comisarului pentru competențe de investigare, disponibil la următoarea adresă: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. În plus, fiecare inspecție a unei autorități publice efectuată de IPCO se încheie cu un raport care este furnizat autorității și include toate recomandările care rezultă în urma acestei inspecții. IPCO începe apoi fiecare inspecție ulterioară cu o examinare a oricăror recomandări anterioare de la ultima inspecție și se precizează în noul raport de inspecție dacă recomandările anterioare au fost luate în considerare sau dacă sunt reportate.

([464]) O eroare este considerată „gravă" atunci când comisarul consideră că a cauzat prejudicii sau daune semnificative persoanei în cauză (secțiunea 231 punctul 2 din IPA din 2016). În 2018, au fost raportate 22 de erori, dintre care opt au fost considerate grave și au condus la informarea persoanei în cauză. A se vedea Raportul anual pe 2018 al Biroului comisarului pentru competențe de investigare, anexa C (a se vedea https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). În 2019, 14 erori au fost considerate grave. A se vedea Raportul anual pe 2019 al Biroului comisarului pentru competențe de investigare, anexa C, a se vedea nota de subsol 463.

([465]) Secțiunea 231 din IPA din 2016 precizează că, atunci când informează o persoană cu privire la o eroare, IPC trebuie să furnizeze detaliile pe care comisarul le consideră necesare pentru exercitarea acestor drepturi, având în vedere în special măsura în care divulgarea detaliilor ar contraveni interesului public sau ar aduce atingere prevenirii sau depistării infracțiunilor grave, bunăstării economice a Regatului Unit sau exercitării continue a funcțiilor oricărui serviciu de informații.

3.3.3.3. Supravegherea parlamentară a serviciilor de informații

(256) Supravegherea parlamentară de către Comisia pentru Informații și Securitate (ISC) își are temeiul juridic în *Justice and Security Act 2013* – Legea din 2013 privind justiția și securitatea (JSA 2013) ([466]). Legea instituie ISC ca o comisie a Parlamentului Regatului Unit. Începând din 2013, ISC a beneficiat de competențe sporite, inclusiv supravegherea activităților operaționale ale serviciilor de securitate. În temeiul secțiunii 2 din JSA din 2013, ISC are sarcina de a supraveghea cheltuielile, administrarea, politicile și operațiunile agențiilor de securitate națională. JSA din 2013 specifică faptul că ISC este în măsură să desfășoare investigații cu privire la aspecte operaționale atunci când acestea nu se referă la operațiuni în curs ([467]). Memorandumul de înțelegere convenit între prim-ministru și ISC ([468]) precizează în detaliu elementele care trebuie luate în considerare atunci când se analizează dacă o activitate nu face parte din nicio operațiune în curs ([469]). De asemenea, ISC poate fi invitată să investigheze operațiunile în curs de desfășurare de către prim-ministru și poate revizui informațiile furnizate în mod voluntar de agenții.

(257) În conformitate cu anexa 1 la JSA din 2013, ISC poate solicita șefilor oricăruia dintre cele trei servicii de informații să divulge informații. Agenția trebuie să pună la dispoziție aceste informații, cu excepția cazului în care secretarul de stat își exercită un drept de veto în acest sens ([470]). Potrivit explicațiilor furnizate de autoritățile Regatului Unit, în practică, foarte puține informații nu sunt comunicate ISC ([471]).

(258) ISC este alcătuită din membri care aparțin uneia dintre camerele Parlamentului și sunt numiți de prim-ministru după consultarea liderului opoziției ([472]). ISC trebuie să prezinte Parlamentului un raport anual privind îndeplinirea funcțiilor sale, precum și alte rapoarte pe care le consideră adecvate ([473]). În plus, ISC are dreptul de a primi, o dată la trei luni, lista scopurilor operaționale utilizate pentru examinarea materialelor obținute în masă ([474]). Prim-ministrul transmite ISC copii ale investigațiilor, inspecțiilor sau auditurilor comisarului pentru competențe de investigare atunci când chestiunea rapoartelor este relevantă pentru competențele statutare ale comisiei ([475]). În cele din urmă, comisia poate solicita IPC să efectueze o investigație, iar comisarul trebuie să informeze ISC cu privire la decizia de a efectua o astfel de investigație ([476]).

(259) ISC a contribuit, de asemenea, la proiectul IPA din 2016, conducând la o serie de amendamente care se reflectă în prezent în IPA din 2016 ([477]). În special, ISC a recomandat consolidarea măsurilor de protecție a vieții private prin introducerea unui set de măsuri de protecție a vieții private care să se aplice întregii game de competențe de

([466]) Astfel cum au explicat autoritățile Regatului Unit, JSA a extins domeniul de competență al ISC pentru a include un rol în supravegherea comunității serviciilor de informații dincolo de cele trei agenții și pentru a permite supravegherea retrospectivă a activităților operaționale ale agențiilor în chestiuni de interes național major.

([467]) Secțiunea 2 din JSA din 2013.

([468]) Memorandumul de înțelegere dintre prim-ministru și ISC, disponibil la următoarea adresă: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf

([469]) Memorandumul de înțelegere dintre prim-ministru și ISC, punctul 14, a se vedea nota de subsol 468.

([470]) Secretarul de stat se poate opune divulgării informațiilor numai în două cazuri: informațiile sunt sensibile și nu ar trebui divulgate ISC în interesul securității naționale; sau este vorba de informații de o asemenea natură încât, în cazul în care secretarul de stat ar fi solicitat să le prezinte în fața unei comisii departamentale restrânse a Camerei Comunelor, secretarul de stat ar considera (pentru motive care nu se limitează la securitatea națională) că nu ar trebui să facă acest lucru (punctul 4 subpunctul 2 din anexa 1 la JSA din 2013).

([471]) Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat, secțiunea H: Securitatea națională, pagina 43, a se vedea nota de subsol 31.

([472]) Secțiunea 1 din JSA din 2013. Miniștrii nu sunt eligibili pentru statutul de membri. Membrii își exercită funcția în cadrul ISC pe durata mandatului Parlamentului în cursul căruia au fost numiți. Aceștia pot fi revocați printr-o rezoluție a Camerei prin care au fost numiți, în cazul în care nu mai au calitatea de membri sau devin miniștri. De asemenea, un membru poate demisiona.

([473]) Rapoartele și declarațiile comisiei sunt disponibile online la următoarea adresă: https://isc.independent.gov.uk/publications. În 2015, ISC a publicat un raport privind „Dreptul la viață privată și securitatea: un cadru juridic modern și transparent" (*Privacy and Security: A modern and transparent legal framework*) (a se vedea: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf) în care a analizat cadrul juridic pentru tehnicile de supraveghere utilizate de agențiile de informații și a emis o serie de recomandări care au fost apoi luate în considerare și integrate în proiectul de lege privind competențele de investigare, care a fost transformat în lege, IPA din 2016. Răspunsul guvernului la raportul privind dreptul la viață privată și securitatea este disponibil la următoarea adresă: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf

([474]) Secțiunile 142, 161 și 183 din IPA din 2016.

([475]) Secțiunea 234 din IPA din 2016.

([476]) Secțiunea 236 din IPA din 2016.

([477]) Comisia pentru Informații și Securitate a Parlamentului, Raport privind proiectul de lege privind competențele de investigare, disponibil la următoarea adresă: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

investigare ([478]). De asemenea, aceasta a sugerat modificări ale capacităților propuse în ceea ce privește intervenția asupra echipamentelor, BPD și datele comunicațiilor și a solicitat alte modificări specifice în vederea consolidării limitărilor și garanțiilor pentru utilizarea competențelor de investigare ([479]).

3.3.4. *Căi de atac*

(260) În domeniul accesului administrației publice în scopuri de securitate națională, persoanele vizate trebuie să dispună de posibilitatea de a exercita căi legale în fața unei instanțe judecătorești independente și imparțiale pentru a avea acces la date cu caracter personal care le privesc sau de a obține rectificarea sau ștergerea acestor date ([480]). Un astfel de organism judiciar trebuie să dispună, în special, de competența de a adopta decizii obligatorii cu privire la serviciul de informații ([481]). În Regatul Unit, astfel cum se explică în considerentele 261-271, o serie de căi de atac judiciare oferă persoanelor vizate posibilitatea de a introduce și de a obține astfel de căi de atac legale.

3.3.4.1. Mecanisme de exercitare a unei căi de atac disponibile în temeiul părții 4 din DPA

(261) În temeiul secțiunii 165 din DPA din 2018, o persoană vizată are dreptul de a depune o plângere la comisarul pentru informații în cazul în care persoana vizată consideră că, în ceea ce privește datele cu caracter personal care o privesc, există o încălcare a părții 4 din DPA din 2018. Comisarul pentru informații are competența de a evalua conformitatea operatorului și a persoanei împuternicite de operator cu DPA din 2018 și de a le impune să ia măsurile necesare. În plus, în temeiul părții 4 din DPA din 2018, persoanele fizice au dreptul să solicite Înaltei Curți (sau *Court of Session* din Scoția) un ordin prin care să îi impună operatorului să respecte drepturile de acces la date ([482]), să se opună prelucrării ([483]) și să rectifice sau să șteargă datele ([484]).

(262) De asemenea, persoanele fizice au dreptul să solicite operatorului sau unei persoane împuternicite de operator ([485]) despăgubiri pentru prejudiciile suferite ca urmare a încălcării unei cerințe prevăzute în partea 4 din DPA din 2018. Prejudiciul include atât pierderi financiare, cât și prejudicii care nu implică pierderi financiare, cum ar fi suferințele clinice ([486]).

3.3.4.2. Mecanisme de exercitare a unei căi de atac disponibile în cadrul IPA din 2016

(263) Persoanele fizice pot obține reparații pentru încălcări ale IPA din 2016 în fața Tribunalului cu competențe de investigare.

(264) Tribunalul cu competențe de investigare este instituit prin RIPA din 2000 și este independent de puterea executivă ([487]). În conformitate cu secțiunea 65 din RIPA din 2000, membrii Tribunalului sunt numiți de Majestatea Sa pentru o perioadă de cinci ani. Un membru al Tribunalului poate fi revocat din funcție de Majestatea Sa în urma unei propuneri („*address*") ([488]) formulate de ambele camere ale Parlamentului ([489]).

([478]) Aceste obligații generale în ceea ce privește dreptul la viață privată sunt prevăzute în prezent în secțiunea 2 punctul 2 din IPA din 2016, care prevede că o autoritate publică acționând în temeiul IPA din 2016 trebuie să aibă în vedere dacă scopul urmărit prin mandat, autorizație sau notificare ar putea fi realizat în mod rezonabil prin alte mijloace mai puțin intruzive, dacă nivelul de protecție care urmează să fie aplicat în legătură cu orice obținere de informații în temeiul mandatului, al autorizației sau al notificării este mai ridicat ca urmare a sensibilității deosebite a informațiilor respective, a interesului public în ceea ce privește integritatea și securitatea rețelelor de telecomunicații și a serviciilor poștale, precum și a oricăror alte aspecte ale interesului public în ceea ce privește protecția vieții private.

([479]) De exemplu, ca urmare a solicitării ISC, numărul de zile în care un mandat „urgent" poate fi în vigoare înainte de a trebui să fie aprobat de către comisarul judiciar a fost redus de la cinci la trei zile lucrătoare, iar ISC a fost împuternicită să sesizeze comisarul pentru competențe de investigare în vederea desfășurării unei investigații.

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

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

([482]) Secțiunea 94 punctul 11 din DPA din 2018.

([483]) Secțiunea 99 punctul 4 din DPA din 2018.

([484]) Secțiunea 100 punctul 1 din DPA din 2018.

([485]) Secțiunea 169 din DPA din 2018 admite cererile depuse de „O persoană care suferă prejudicii ca urmare a încălcării unei cerințe a legislației privind protecția datelor". Potrivit informațiilor furnizate de autoritățile Regatului Unit, în practică, o cerere sau o plângere împotriva serviciilor de informații poate fi înaintată Tribunalului cu competențe de investigare care are o competență extinsă și poate acorda despăgubiri/daune-interese, iar introducerea unei acțiuni în fața acestui tribunal nu implică niciun cost.

([486]) Secțiunea 169 punctul 5 din DPA din 2018.

([487]) În conformitate cu anexa 3 la RIPA din 2000, membrii trebuie să aibă o experiență judiciară specifică și să fie eligibili pentru o nouă numire.

([488]) „Address" este o propunere prezentată Parlamentului prin care se urmărește informarea monarhului cu privire la opiniile Parlamentului referitoare la o anumită chestiune.

([489]) Punctul 1 subpunctul 5 din anexa 3 la RIPA din 2000.

(265) În temeiul secțiunii 65 din RIPA din 2000, Tribunalul este organismul judiciar adecvat pentru orice plângere depusă de o persoană lezată de un comportament prevăzut în IPA din 2016, RIPA din 2000 sau de orice comportament al serviciilor de informații ([490]).

(266) Pentru a introduce o acțiune în fața Tribunalului cu competențe de investigare („cerință privind calitatea procesuală"), în conformitate cu secțiunea 65 din RIPA din 2000, o persoană fizică trebuie să aibă convingerea ([491]) că a avut loc un serviciu de informații în legătură cu ea, cu privire la oricare dintre bunurile sale, cu privire la orice comunicare trimisă de sau către ea ori care îi este destinată sau utilizarea oricărui serviciu poștal, serviciu de telecomunicații sau sistem de telecomunicații ([492]). În plus, reclamantul trebuie să aibă convingerea că acest comportament a avut loc în „circumstanțe atacabile" ([493]) sau „a fost efectuat de către sau în numele serviciilor de informații" ([494]). Întrucât, în special, acest standard în materie de „convingere" a fost interpretat în sens destul de larg ([495]), introducerea unei cauze în fața tribunalului în cauză face obiectul unui nivel scăzut de cerințe privind calitatea procesuală.

(267) În cazul în care Tribunalul cu competențe de investigare examinează o plângere care îi este adresată, este de datoria Tribunalului să investigheze dacă persoanele împotriva cărora se face vreo acuzație în plângere au fost implicate în relații cu reclamantul, precum și să investigheze autoritatea care se presupune că a fost implicată în încălcări și dacă presupusul comportament a avut loc ([496]). În cazul în care tribunalul menționat judecă o procedură, acesta trebuie să aplice, în cadrul procedurii respective, aceleași principii care ar fi aplicate de o instanță cu privire la o cerere de control jurisdicțional ([497]). În plus, destinatarii mandatelor sau ai notificărilor în temeiul IPA din 2016, precum și orice altă persoană care deține o funcție în cadrul Coroanei, angajată de forțele de poliție sau de comisarul pentru investigații și evaluare a poliției (*Police Investigations and Review Commissioner*), au obligația de a divulga sau de a furniza Tribunalului respectiv toate documentele și informațiile de care Tribunalul ar putea avea nevoie pentru a le permite să își exercite competența ([498]).

(268) Tribunalul cu competențe de investigare trebuie să informeze reclamantul dacă a fost luată o hotărâre în favoarea acestuia sau nu ([499]). În temeiul secțiunii 67 punctele 6 și 7 din RIPA din 2000, Tribunalul are competența de a emite ordine provizorii și de a pronunța orice hotărâre de despăgubire sau orice altă ordonanță pe care o consideră adecvată. Aceasta poate include un ordin de casare sau de anulare a oricărui mandat sau a oricărei autorizații și un

([490]) Secțiunea 65 punctul 5 din RIPA din 2000.

([491]) În ceea ce privește standardul testului în materie de „convingere", a se vedea cauza *Human Rights Watch/Secretary of State* [2016] UKIPTrib15_165-CH, punctul 41. În acest caz, Tribunalul cu competențe de investigare, făcând trimitere la jurisprudența Curții Europene a Drepturilor Omului, a statuat că, în ceea ce privește convingerea declarată că orice comportament care intră sub incidența subsecțiunii 68 punctul 5 din RIPA din 2000 a fost efectuat de către sau în numele unui serviciu de informații, testul adecvat este de a stabili dacă există un temei pentru o astfel de convingere, de așa natură încât o persoană poate pretinde că este victima unei încălcări determinate de simpla existență a unor măsuri secrete sau a unei legislații care permite măsuri secrete, numai în cazul în care poate demonstra că, din cauza situației sale personale, aceasta poate fi expusă riscului de a face obiectul unor astfel de măsuri.

([492]) Secțiunea 65 punctul 4 litera (a) din RIPA din 2000.

([493]) Astfel de circumstanțe se referă la comportamentul autorităților publice cu autoritate (de exemplu, un mandat, o autorizație/notificare pentru achiziția de comunicații etc.) sau dacă circumstanțele sunt de așa natură încât (indiferent dacă există sau nu o astfel de autoritate), nu ar fi fost adecvat ca respectivul comportament să aibă loc în lipsa acestuia sau, cel puțin, fără să se fi analizat în mod corespunzător dacă o astfel de autoritate ar trebui solicitată. Se consideră că un comportament autorizat de un comisar judiciar a avut loc în circumstanțe atacabile (secțiunea 65 punctul 7ZA din RIPA din 2000), în timp ce alte comportamente care au loc cu permisiunea unei persoane care deține funcții judiciare sunt considerate a nu fi avut loc în circumstanțe atacabile (secțiunea 65 punctele 7 și 8 din RIPA din 2000).

([494]) Potrivit informațiilor furnizate de autoritățile Regatului Unit, pragul redus pentru depunerea unei plângeri determină că nu este neobișnuit ca ancheta Tribunalului să stabilească faptul că reclamantul nu a făcut niciodată obiectul unei anchete desfășurate de către o autoritate publică. Cel mai recent raport statistic al Tribunalului cu competențe de investigare precizează că, în 2016, Tribunalul a înregistrat 209 plângeri, 52 % dintre acestea au fost considerate neserioase sau vexatorii, iar 25 % au rămas nesoluționate. Autoritățile Regatului Unit au explicat că acest lucru înseamnă fie că nu au fost utilizate activități/competențe disimulate în legătură cu reclamantul, fie că au fost utilizate tehnici ascunse, iar tribunalul a stabilit că activitatea este legală. În plus, 11 % au fost excluse din jurisdicție, retrase sau nevalabile, 5 % au fost prescrise, 7 % au fost stabilite în favoarea reclamantului. Raportul statistic al Tribunalului cu competențe de investigare din 2016, disponibil la următoarea adresă: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([495]) A se vedea cauza *Human Rights Watch/Secretary of State* [2016] UKIPTrib15_165-CH. În acest caz, Tribunalul cu competențe de investigare, făcând trimitere la jurisprudența Curții Europene a Drepturilor Omului, a statuat că, în ceea ce privește convingerea că orice comportament care intră sub incidența subsecțiunii 68 punctul 5 din RIPA din 2000 a fost efectuat de către sau în numele unui serviciu de informații, testul adecvat este de a stabili dacă există un temei pentru o astfel de convingere, inclusiv faptul că o persoană poate pretinde că este victima unei încălcări determinate de simpla existență a unor măsuri secrete sau a unei legislații care permite măsuri secrete, numai în cazul în care poate demonstra că, din cauza situației sale personale, aceasta poate fi expusă riscului de a face obiectul unor astfel de măsuri (a se vedea *Human Rights Watch/Secretary of State*, punctul 41).

([496]) Secțiunea 67 punctul 3 din RIPA din 2000.

([497]) Secțiunea 67 punctul 2 din RIPA din 2000.

([498]) Secțiunea 68 punctele 6-7 din RIPA din 2000.

([499]) Secțiunea 68 punctul 4 din RIPA din 2000.

ordin prin care se solicită distrugerea oricăror înregistrări de informații obținute în exercitarea oricărei competențe conferite de un mandat, o autorizație sau o notificare, sau altfel deținute de orice autoritate publică în legătură cu orice persoană ([500]). În conformitate cu secțiunea 67A din RIPA din 2000, o decizie a Tribunalului poate fi atacată, sub rezerva autorizării de către Tribunal sau de către instanța de apel competentă.

(269) În cele din urmă, trebuie remarcat faptul că rolul Tribunalului cu competențe de investigare a fost discutat în contextul acțiunilor în justiție introduse în fața Curții Europene a Drepturilor Omului în mai multe rânduri, în special în cauza *Kennedy/Regatul Unit* ([501]) și, mai recent, în cauza *Big Brother Watch și alții/Regatul Unit* ([502]), în care Curtea a declarat că „IPT a oferit o cale de atac judiciară solidă oricărei persoane care a suspectat faptul că comunicațiile sale au fost interceptate de serviciile de informații" ([503]).

3.3.4.3. Alte mecanisme de exercitare a unei căi de atac disponibile

(270) Astfel cum se explică în considerentele 109-111, căile de atac prevăzute de Legea privind drepturile omului din 1998 și în fața Curții Europene Drepturilor Omului ([504]) sunt, de asemenea, disponibile în domeniul securității naționale. Secțiunea 65 punctul 2 din RIPA din 2000 acordă Tribunalului cu competențe de investigare competență judiciară exclusivă pentru toate cererile în baza Legii privind drepturile omului în legătură cu agențiile de informații ([505]). Astfel cum a remarcat High Court (Înalta Curte), aceasta înseamnă că „dacă a existat o încălcare a HRA cu privire la situația de fapt dintr-o anumită cauză, acest fapt poate fi invocat și soluționat, în principiu, de către un tribunal independent care poate avea acces la toate elementele relevante, inclusiv la materiale secrete. […] De asemenea, în acest context, avem în vedere faptul că Tribunalul este în prezent supus posibilității de a introduce o cale de atac la o instanță de apel adecvată (în Anglia și Țara Galilor, aceasta este Curtea de Apel); iar Curtea Supremă a decis recent că Tribunalul poate, în principiu, să facă obiectul unui control jurisdicțional: a se vedea R (Privacy International)/ Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219" ([506]).

(271) Din cele de mai sus rezultă că, atunci când autoritățile de aplicare a legii sau autoritățile de securitate națională din Regatul Unit accesează date cu caracter personal care intră în domeniul de aplicare al prezentei decizii, un astfel de acces este reglementat de legi care stabilesc condițiile în care poate avea loc accesul și asigură faptul că accesul și utilizarea ulterioară a datelor sunt limitate la ceea ce este necesar și proporțional cu obiectivul de asigurare a respectării legii sau de securitate națională urmărit. În plus, un astfel de acces face, în majoritatea cazurilor, obiectul unei autorizări prealabile de către un organism judiciar, prin aprobarea unui mandat sau a unui ordin de divulgare și, în orice caz, al unei supravegheri independente. Odată ce datele au fost accesate de autoritățile publice, prelucrarea acestora, inclusiv partajarea și transferurile ulterioare, face obiectul unor garanții specifice privind protecția datelor prevăzute în partea 3 din DPA din 2018, care le reflectă pe cele prevăzute în Directiva (UE) 2016/680, pentru prelucrarea de către autoritățile de aplicare a legii și în partea 4 din DPA din 2018 pentru prelucrarea de către serviciile de informații. În cele din urmă, persoanele vizate beneficiază în acest domeniu de căi de atac administrative și judiciare eficace, inclusiv dreptul de a obține accesul la datele lor sau dreptul la rectificarea sau ștergerea datelor respective.

(272) Având în vedere importanța acestor condiții, limitări și garanții în sensul prezentei decizii, Comisia va monitoriza îndeaproape aplicarea și interpretarea normelor Regatului Unit care reglementează accesul guvernului la date. Aceasta va include evoluțiile legislative, de reglementare și ale jurisprudenței relevante, precum și activitățile ICO și ale altor autorități de supraveghere în acest domeniu. De asemenea, se va acorda o atenție deosebită executării de

([500]) Un exemplu de aplicare a acestor competențe este cauza *Liberty și alții/Security Service, SIS, GCHQ*, [2015] UKIP Trib 13_77-H_2. Tribunalul s-a pronunțat în favoarea a doi reclamanți, întrucât comunicațiile acestora, într-un caz, au fost păstrate dincolo de limitele stabilite și, în celălalt caz, întrucât procedura de examinare nu a fost urmată, astfel cum se prevede în normele interne ale GCHQ. În prima cauză, Curtea a dispus ca serviciile de informații să distrugă comunicațiile care au fost păstrate pentru o perioadă mai lungă decât termenul relevant. În al doilea caz, nu a fost emis un ordin de distrugere deoarece comunicațiile nu au fost păstrate.

([501]) *Kennedy*, a se vedea nota de subsol 129.

([502]) Curtea Europeană a Drepturilor Omului, *Big Brother Watch și alții/Regatul Unit* (a se vedea nota de subsol 268de mai sus), punctele 413-415.

([503]) Curtea Europeană a Drepturilor Omului, *Big Brother Watch*, punctul 425.

([504]) După cum o ilustrează, de exemplu, recenta hotărâre a Marii Camere a Curții Europene a Drepturilor Omului în cauza *Big Brother Watch și alții/Regatul Unit* (a se vedea nota de subsol 279 de mai sus), acest lucru permite exercitarea de către o instanță internațională a unui control jurisdicțional efectiv – similar celui la care sunt supuse statele membre ale UE – asupra respectării de către autoritățile publice a drepturilor fundamentale atunci când accesează date cu caracter personal. În plus, executarea hotărârilor Curții Europene a Drepturilor Omului face obiectul unei supravegheri specifice din partea Consiliului Europei.

([505]) În cauza *Belhaj și alții* [2017] UKSC 3, constatarea caracterului ilegal al interceptării materialului cu caracter juridic privilegiat s-a bazat direct pe articolul 8 din Convenția europeană a drepturilor omului (a se vedea constatarea 11).

([506]) Înalta Curte de Justiție, *Liberty*, [2019] EWHC 2057 (Admin), punctul 170.

către Regatul Unit a hotărârilor relevante ale Curții Europene a Drepturilor Omului, inclusiv a măsurilor identificate în „planurile de acțiune” și în „rapoartele de acțiune” prezentate Comitetului de Miniștri în contextul supravegherii respectării hotărârilor Curții.

4. **CONCLUZIE**

(273) Comisia consideră că RGPD al Regatului Unit și DPA din 2018 asigură un nivel de protecție a datelor cu caracter personal transferate din Uniunea Europeană, care este în esență echivalent cu cel garantat de Regulamentul (UE) 2016/679.

(274) În plus, Comisia consideră că, în ansamblu, mecanismele de supraveghere și căile de atac prevăzute în legislația Regatului Unit permit detectarea și pedepsirea în practică a încălcărilor comise și pun la dispoziția persoanelor vizate căile de atac juridice necesare pentru a obține accesul la datele cu caracter personal care le privesc și, în cele din urmă, rectificarea sau ștergerea datelor respective.

(275) În cele din urmă, pe baza informațiilor disponibile cu privire la ordinea juridică a Regatului Unit, Comisia consideră că orice atingere adusă, în scopuri de interes public, în special în scopul asigurării respectării legii și al securității naționale, de autoritățile publice ale Regatului Unit drepturilor fundamentale ale persoanelor fizice ale căror date cu caracter personal sunt transferate din Uniunea Europeană în Regatul Unit, se va limita la ceea ce este strict necesar pentru îndeplinirea obiectivului legitim în cauză, cât și că există o protecție juridică eficace împotriva unor astfel de atingeri.

(276) Prin urmare, în lumina constatărilor prezentei decizii, ar trebui să se decidă că Regatul Unit asigură un nivel adecvat de protecție în sensul articolului 45 din Regulamentul (UE) 2016/679, interpretat în lumina Cartei drepturilor fundamentale a Uniunii Europene.

(277) Această concluzie se bazează atât pe regimul intern relevant al Regatului Unit, cât și pe angajamentele sale internaționale, în special aderarea la Convenția europeană a drepturilor omului și recunoașterea competenței Curții Europene a Drepturilor Omului. Respectarea în continuare a acestor obligații internaționale este, prin urmare, un element deosebit de important al evaluării pe care se bazează prezenta decizie.

5. **EFECTELE PREZENTEI DECIZII ȘI ACȚIUNILE AUTORITĂȚILOR PENTRU PROTECȚIA DATELOR**

(278) Statele membre și organele acestora au obligația de a lua măsurile necesare pentru a se conforma actelor instituțiilor Uniunii, întrucât se presupune că aceste acte sunt legale și, prin urmare, produc efecte juridice atât timp cât nu expiră, sunt retrase, anulate în cadrul unei acțiuni în anulare sau declarate nule ca urmare a unei trimiteri preliminare sau a unei excepții de nelegalitate.

(279) În consecință, o decizie a Comisiei privind caracterul adecvat al nivelului de protecție, adoptată în temeiul articolului 45 alineatul (3) din Regulamentul (UE) 2016/679, este obligatorie pentru toate organele statelor membre cărora li se adresează, inclusiv pentru autoritățile de supraveghere independente ale acestora. În special, în cursul perioadei de aplicare a prezentei decizii, transferurile de la un operator sau de la o persoană împuternicită de operator din Uniunea Europeană către operatori sau persoane împuternicite de operatori din Regatul Unit pot avea loc fără a fi necesară obținerea unei autorizații suplimentare.

(280) Ar trebui reamintit faptul că, în temeiul articolului 58 alineatul (5) din Regulamentul (UE) 2016/679 și astfel cum este explicat de Curtea de Justiție în hotărârea pronunțată în cauza *Schrems* ([507]), în cazul în care o autoritate națională de protecție a datelor pune sub semnul întrebării, inclusiv în urma primirii unei plângeri, compatibilitatea unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție cu dreptul fundamental al unei persoane la viață privată și la protecția datelor, legislația națională trebuie să prevadă o cale de atac pentru a prezenta obiecțiile respective în fața unei instanțe naționale, care poate fi obligată să efectueze o trimitere preliminară către Curtea de Justiție ([508]).

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

([508]) *Schrems*, punctul 65: „În această privință, revine legiuitorului național sarcina de a prevedea căi de atac care să permită autorității naționale de supraveghere în cauză să invoce motivele pe care le consideră întemeiate în fața instanțelor naționale, astfel încât acestea din urmă să efectueze, dacă împărtășesc îndoielile acestei autorități în ceea ce privește validitatea deciziei Comisiei, o trimitere preliminară în vederea examinării validității acestei decizii.”

6. MONITORIZAREA, SUSPENDAREA, ABROGAREA SAU MODIFICAREA PREZENTEI DECIZII

(281) În temeiul articolului 45 alineatul (4) din Regulamentul (UE) 2016/679, Comisia trebuie să monitorizeze în permanență evoluțiile relevante din Regatul Unit după adoptarea prezentei decizii pentru a evalua dacă aceasta garantează în continuare un nivel de protecție echivalent în esență. O astfel de monitorizare este deosebit de importantă în acest caz, întrucât Regatul Unit va administra, va aplica și va asigura respectarea unui nou regim de protecție a datelor care nu mai intră sub incidența dreptului Uniunii Europene și care ar putea evolua. În acest sens, se va acorda o atenție deosebită aplicării în practică a normelor Regatului Unit privind transferurile de date cu caracter personal către țări terțe, impactului pe care aceasta l-ar putea avea asupra nivelului de protecție acordat datelor transferate în temeiul prezentei decizii; eficacității exercitării drepturilor individuale, inclusiv orice evoluție relevantă a legislației și a practicii în ceea ce privește excepțiile sau restricțiile privind aceste drepturi (în special cel referitor la menținerea unui control efectiv al imigrației); precum și respectării limitărilor și a garanțiilor în ceea ce privește accesul guvernului. Printre alte elemente, evoluțiile jurisprudenței și supravegherea de către ICO și alte organisme independente vor contribui la monitorizarea efectuată de Comisie.

(282) Pentru a facilita această monitorizare, autoritățile Regatului Unit ar trebui să informeze cu promptitudine Comisia cu privire la orice modificare substanțială a ordinii juridice a Regatului Unit care are un impact asupra cadrului juridic care face obiectul prezentei decizii, precum și cu privire la orice evoluție a practicilor legate de prelucrarea datelor cu caracter personal evaluate în prezenta decizie, atât în ceea ce privește prelucrarea datelor cu caracter personal de către operatori și persoane împuternicite de operatori în temeiul RGPD al Regatului Unit, cât și limitările și garanțiile aplicabile accesului autorităților publice la datele cu caracter personal. Aceasta ar trebui să includă evoluțiile privind elementele menționate în considerentul 281.

(283) În plus, pentru a permite Comisiei să își exercite în mod eficace funcția de monitorizare, statele membre ar trebui să informeze Comisia cu privire la orice acțiune relevantă întreprinsă de autoritățile naționale de protecție a datelor, în special în ceea ce privește solicitările sau plângerile formulate de persoanele vizate din UE cu privire la transferul de date cu caracter personal din Uniunea Europeană către operatori sau persoane împuternicite de operatori din Regatul Unit. De asemenea, Comisia ar trebui să fie informată cu privire la orice indiciu potrivit căruia acțiunile autorităților publice din Regatul Unit responsabile cu prevenirea, investigarea, detectarea sau aducerea în fața instanței a infracțiunilor sau cu securitatea națională, inclusiv acțiunile oricărui organism de supraveghere, nu asigură nivelul de protecție necesar.

(284) În cazul în care informațiile disponibile, în special informațiile care rezultă din monitorizarea prezentei decizii sau cele furnizate de autoritățile Regatului Unit sau ale statelor membre, arată că nivelul de protecție oferit de Regatul Unit ar putea să nu mai fie adecvat, Comisia ar trebui să informeze autoritățile Regatului Unit competente în acest sens și să solicite luarea unor măsuri adecvate într-un termen rezonabil specificat, care nu poate depăși trei luni. Dacă este necesar, acest termen poate fi prelungit cu o anumită perioadă de timp, ținând seama de natura problemei în cauză și/sau de măsurile care trebuie luate. De exemplu, o astfel de procedură ar fi declanșată în cazurile în care transferurile ulterioare, inclusiv pe baza noilor regulamente privind caracterul adecvat al nivelului de protecție adoptate de secretarul de stat sau a acordurilor internaționale încheiate de Regatul Unit, nu ar mai fi efectuate cu respectarea unor garanții care să asigure continuitatea protecției în sensul articolului 44 din Regulamentul (UE) 2016/679.

(285) În cazul în care, la expirarea termenului specificat, autoritățile competente ale Regatului Unit nu iau măsurile respective sau nu demonstrează în mod satisfăcător că prezenta decizie continuă să se bazeze pe un nivel adecvat de protecție, Comisia va iniția procedura menționată la articolul 93 alineatul (2) din Regulamentul (UE) 2016/679 în vederea suspendării sau abrogării parțiale sau integrale a prezentei decizii.

(286) Ca alternativă, Comisia va iniția această procedură în vederea modificării prezentei decizii, în special prin aplicarea unor condiții suplimentare transferurilor de date sau prin limitarea domeniului de aplicare al constatării referitoare la caracterul adecvat numai la transferurile de date pentru care se asigură în continuare un nivel adecvat de protecție.

(287) Din motive imperioase de urgență justificate corespunzător, Comisia va face uz de posibilitatea de a adopta, în conformitate cu procedura menționată la articolul 93 alineatul (3) din Regulamentul (UE) 2016/679, acte de punere în aplicare imediat aplicabile de suspendare, abrogare sau modificare a deciziei.

7. DURATA ȘI REÎNNOIREA PREZENTEI DECIZII

(288) Comisia trebuie să țină seama de faptul că, odată cu încheierea perioadei de tranziție prevăzute în Acordul de retragere și de îndată ce dispoziția provizorie prevăzută la articolul 782 din Acordul comercial și de cooperare UE-Regatul Unit va înceta să se aplice, Regatul Unit va administra, va aplica și va asigura respectarea unui nou regim de protecție a datelor în raport cu cel în vigoare în perioada în care avea obligații în temeiul dreptului Uniunii. Acest lucru poate implica, în special, amendamente sau modificări ale cadrului de protecție a datelor evaluat în prezenta decizie, precum și alte evoluții relevante.

(289) Prin urmare, este oportun să se prevadă că prezenta decizie se va aplica pentru o perioadă de patru ani de la intrarea sa în vigoare.

(290) În cazul în care, în special, informațiile obținute în urma monitorizării prezentei decizii arată că respectivele constatări referitoare la caracterul adecvat al nivelului de protecție asigurat în Regatul Unit sunt încă justificate de fapt și de drept, Comisia ar trebui, cel târziu cu șase luni înainte de încetarea aplicării prezentei decizii, să inițieze procedura de modificare a prezentei decizii prin extinderea domeniului său de aplicare temporal, în principiu, pentru o perioadă suplimentară de patru ani. Orice act de punere în aplicare de modificare a prezentei decizii urmează să fie adoptat în conformitate cu procedura menționată la articolul 93 alineatul (2) din Regulamentul (UE) 2016/679.

8. **CONSIDERAȚII FINALE**

(291) Comitetul european pentru protecția datelor și-a publicat avizul ([509]), care a fost luat în considerare la pregătirea prezentei decizii.

(292) Măsurile prevăzute în prezenta decizie sunt conforme cu avizul comitetului instituit în temeiul articolului 93 din Regulamentul (UE) 2016/679,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

(1) În sensul articolului 45 din Regulamentul (UE) 2016/679, Regatul Unit asigură un nivel adecvat de protecție a datelor cu caracter personal care intră în domeniul de aplicare al Regulamentului (UE) 2016/679, transferate din Uniunea Europeană către Regatul Unit.

(2) Prezenta decizie nu vizează datele cu caracter personal transferate în scopul controlului imigrației în Regatul Unit sau care, altfel, ar intra în domeniul de aplicare al derogării de la anumite drepturi ale persoanelor vizate în scopul menținerii unui control eficace al imigrației în temeiul punctului 4 alineatul (1) din anexa 2 la DPA din 2018.

Articolul 2

Ori de câte ori autoritățile de supraveghere competente din statele membre, pentru a proteja persoanele fizice în ceea ce privește prelucrarea datelor cu caracter personal, își exercită competențele în temeiul articolului 58 din Regulamentul (UE) 2016/679 în ceea ce privește transferurile de date care intră în domeniul de aplicare prevăzut la articolul 1, statul membru în cauză informează fără întârziere Comisia.

Articolul 3

(1) Comisia monitorizează în permanență aplicarea cadrului juridic pe care se bazează prezenta decizie, inclusiv condițiile în care se efectuează transferurile ulterioare, în care se exercită drepturile individuale și în care autoritățile publice din Regatul Unit au acces la datele transferate în temeiul prezentei decizii, pentru a evalua dacă Regatul Unit continuă să asigure un nivel adecvat de protecție în sensul articolului 1.

(2) Statele membre și Comisia se informează reciproc cu privire la cazurile în care comisarul pentru informații, sau orice altă autoritate competentă a Regatului Unit nu asigură respectarea cadrului juridic pe care se bazează prezenta decizie.

(3) Statele membre și Comisia se informează reciproc atât cu privire la orice indiciu potrivit căruia atingerile aduse de autoritățile publice din Regatul Unit dreptului persoanelor fizice la protecția datelor cu caracter personal depășesc ceea ce este strict necesar, cât și cu privire la faptul că nu există o protecție juridică eficace împotriva unor astfel de atingeri.

(4) În cazul în care Comisia are indicii că nu mai este asigurat un nivel adecvat de protecție, Comisia informează autoritățile competente din Regatul Unit și poate suspenda, abroga sau modifica prezenta decizie.

([509]) Avizul 14/2021 privind Proiectul de decizie de punere în aplicare a Comisiei Europene în temeiul Regulamentului (UE) 2016/679 privind protecția adecvată a datelor cu caracter personal în Regatul Unit, disponibil la următoarea adresă: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en

(5) Comisia poate suspenda, abroga sau modifica prezenta decizie în cazul în care lipsa de cooperare a guvernului Regatului Unit împiedică Comisia să stabilească dacă este afectată constatarea de la articolul 1 alineatul (1).

Articolul 4

Prezenta decizie expiră la 27 iunie 2025, cu excepția cazului în care este prelungită în conformitate cu procedura menționată la articolul 93 alineatul (2) din Regulamentul (UE) 2016/679.

Articolul 5

Prezenta decizie se adresează statelor membre.

Adoptată la Bruxelles, 28 iunie 2021.

Pentru Comisie
Didier REYNDERS
Membru al Comisiei