II

(Nem jogalkotási aktusok)

HATÁROZATOK

A BIZOTTSÁG (EU) 2021/1772 VÉGREHAJTÁSI RENDELETE

(2021. június 28.)

az (EU) 2016/679 európai parlamenti és tanácsi rendelet szerint a személyes adatok Egyesült Királyság által biztosított megfelelő szintű védelméről

(az értesítés a C(2021) 4800. számú dokumentummal történt)

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az említett adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendeletre (általános adatvédelmi rendelet) ([1]) és különösen annak 45. cikke (3) bekezdésére,

mivel:

1. BEVEZETÉS

(1) Az (EU) 2016/679 rendelet meghatározza a személyes adatoknak az uniós adatkezelők vagy adatfeldolgozók által a harmadik országokba és a nemzetközi szervezeteknek történő továbbítására vonatkozó szabályokat, amennyiben az említett adattovábbítás az alkalmazási körébe tartozik. A nemzetközi adattovábbítás szabályait az említett rendelet V. fejezete, pontosabban a 44–50. cikk határozza meg. Noha a személyes adatok Európai Unión kívüli országokba és az onnan az Unióba történő áramlása elengedhetetlen a nemzetközi együttműködés és a határokon átnyúló kereskedelem bővüléséhez, a személyes adatoknak az Európai Unióban biztosított védelmi szintjét nem szabad a harmadik országokba történő továbbítással veszélyeztetni ([2]).

(2) Az (EU) 2016/679 rendelet 45. cikkének (3) bekezdése értelmében a Bizottság végrehajtási jogi aktusok útján határozhat arról, hogy a harmadik ország, a harmadik ország valamely területe, illetve egy vagy több meghatározott ágazata, illetve valamely nemzetközi szervezet biztosítja a megfelelő védelmi szintet. E feltétel szerint a személyes adatok harmadik országba történő továbbítására további engedély megszerzésének szükségessége nélkül kerülhet sor, az említett rendelet 45. szakaszának (1) bekezdésében és (103) preambulumbekezdésében előírtak szerint.

(3) Ahogy az (EU) 2016/679 rendelet 45. cikkének (2) bekezdése meghatározza, a megfelelőségi határozat elfogadásának a harmadik ország jogrendjére vonatkozó átfogó elemzésen kell alapulnia, lefedve mind az adatátvevőre vonatkozó szabályokat, mind a személyes adatokhoz való, közigazgatási szervek általi hozzáférést illető korlátozásokat és biztosítékokat. Az értékelés során meg kell határozni, hogy az érintett harmadik ország olyan szintű védelmet biztosít-e, amely „lényegében egyenértékű” az Európai Unión belül biztosított védelem szintjével (az (EU) 2016/679 rendelet (104) preambulumbekezdése). A „lényegi egyenértékűség” értékelése az európai uniós jogszabályok, nevezetesen az (EU) 2016/679 rendelet, valamint az Európai Unió Bíróságának ítélkezési gyakorlata alapján történik ([3]). Európai Adatvédelmi Testület megfelelőségi referenciája ebben a tekintetben is jelentős ([4]).

([1]) HL L 119., 2016.5.4., 1. o.
([2]) Lásd az (EU) 2016/679 rendelet (101) preambulumbekezdését.
([3]) Lásd legutóbb a C-311/18. sz., Facebook Írország és Schrems ügyet („Schrems II.”), ECLI:EU:C:2020:559.
([4]) Európai adatvédelmi tábla, Megfelelőségi referencia, WP 254 rev. 01., a következő linken érhető el: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Az Európai Unió Bíróságának pontosítása szerint ez nem feltétlenül jelent azonos szintű védelmet. ([5]) Különösen a harmadik ország által igénybe vett eszközök különbözhetnek az Európai Unióban alkalmazott eszközöktől, amennyiben – a gyakorlatban – ténylegesen megfelelő szintű védelmet biztosítanak ([6]). A megfelelőségre vonatkozó előírás ezért nem követeli meg az uniós szabályok pontról pontra történő leképezését. A vizsgálat ehelyett arra irányul, hogy az adatvédelemhez való jog tartalmát, hatékony végrehajtását, felügyeletét és érvényesítését tekintve az érintett harmadik ország rendszere összességében véve biztosítja-e az elvárt fokú védelmet ([7]).

(5) A Bizottság gondosan elemezte az Egyesült Királyság jogszabályait és gyakorlatát. A (8)–(270) preambulumbekezdésben kidolgozott megállapítások alapján a Bizottság arra a következtetésre jut, hogy az Egyesült Királyság megfelelő szintű védelmet biztosít az (EU) 2016/679 rendelet hatálya alá tartozó, az Európai Unióból az Egyesült Királyságba továbbított személyes adatok védelme tekintetében.

(6) Ez a következtetés nem vonatkozik a határt átlépő személyforgalom Egyesült Királyság általi ellenőrzése céljaira továbbított személyes adatokra, vagy amelyek egyébként a határt átlépő személyforgalom hatékony ellenőrzése fenntartása céljából az érintettek jogai alóli, az Egyesült Királyság adatvédelmi törvényének 2. melléklete 1. pontjának (4) bekezdése szerinti egyes kivételek (a továbbiakban: „bevándorlási kivétel") hatálya alá tartoznak. Az Egyesült Királyság joga szerint a bevándorlási kivétel érvényességét és értelmezését az angliai és walesi Court of Appeal 2021. május 26-i határozata nem rendezi. Miközben elismeri, hogy az érintettek jogai elvben a határt átlépő személyforgalom ellenőrzésének – mint „fontos közérdek" – céljából korlátozhatók, a Court of Appeal megállapította, hogy a bevándorlási kivétel a jelenlegi formájában összeegyeztethetetlen az Egyesült Királyság jogával, mivel a jogalkotási intézkedésből hiányoznak az Egyesült Királyság általános adatvédelmi rendelete 23. cikkének (2) bekezdésében felsorolt biztosítékokat meghatározó különös rendelkezések ([8]). Ilyen feltételek mellett ki kell zárni e határozat hatálya alól azon személyes adatoknak az Unióból az Egyesült Királyságba történő továbbítását, amelyekre a bevándorlási kivétel alkalmazható ([9]). Az Egyesült Királyság jogszabályaival való összeegyeztethetetlenség orvoslását követően újból értékelni kell a bevándorlási kivételt, valamint azt, hogy szükséges-e e határozat hatályának korlátozását fenntartani.

(7) Ez a határozat nem érinti az (EU) 2016/679 rendeletnek az Egyesült Királyságban letelepedett szervezetekre történő közvetlen alkalmazását, ha teljesülnek az említett rendelet 3. cikkében meghatározott, a rendelet területi hatályára vonatkozó feltételek.

2. A SZEMÉLYES ADATOK KEZELÉSÉRE VONATKOZÓ SZABÁLYOK

2.1. Alkotmányos keret

(8) Az Egyesült Királyság parlamenti demokrácia, amelynek alkotmányos államfője az uralkodó. Minden más kormányzati intézmény felett álló szuverén parlamenttel, a parlamentből választott és a parlament által elszámoltatható végrehajtó hatalommal, valamint független igazságszolgáltatással rendelkezik. A végrehajtó hatalom felhatalmazását abból a képességéből nyeri, hogy képes elnyerni a megválasztott alsóház bizalmát, és elszámoltatható a parlament mindkét háza felé, amelyek feladata a kormány ellenőrzése, valamint a törvények megvitatása és elfogadása.

([5]) C-362/14. sz. Schrems-ügy („Schrems I."), ECLI:EU:C:2015:650, 73. pont.

([6]) Schrems I. ügy, 74. pont.

([7]) Lásd „A személyes adatok cseréje és védelme a globalizált világban" című, az Európai Parlamentnek és a Tanácsnak címzett bizottsági közleményt (COM(2017) 7, 2017.1.10., 3.1. szakasz, 6–7. o., elérhető a következő linken: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017DC0007&from=HU

([8]) Court of Appeal (polgári ügyszak), Open Rights Group kontra belügyminiszter és a digitális, kulturális, média- és sportügyi miniszter, [2021] EWCA Civ 800, 53–56. pont. A Court of Appeal megváltoztatta a High Court of Justice korábban hozott határozatát, amely a kivételt az (EU) 2016/679 rendeletre (különösen annak 23. cikkére) és az Európai Unió Alapjogi Chartájára figyelemmel értékelte, és a kivételt jogszerűnek találta (Open Rights Group & Anor, R (kérelmező) kontra belügyminiszter és Anor [2019] EWHC 2562).

([9]) Az irányadó feltételek teljesülésének feltételével a határt átlépő személyforgalom Egyesült Királyság általi ellenőrzése céljaira történő adattovábbítás az (EU) 2016/679 rendelet 46–49. cikkében előírt adattovábbítási mechanizmus alapján végezhető.

(9) Az Egyesült Királyság parlamentje átruházta mindazon skóciai, walesi és észak-írországi belső ügyekben történő törvényhozás terén a felelősséget rendre a skót parlamentre, a walesi parlamentre (Senedd Cymru) és az észak-írországi parlamentre, amelyeket az Egyesült Királyság parlamentje nem tartott fenn magának. Noha az adatvédelem fenntartott tárgykör, azaz ugyanazon jogszabályok érvényesek az ország egész területén, az e határozat szempontjából releváns egyéb szakpolitikai területek átruházott tárgykörök. Például Skócia és Észak-Írország büntető igazságszolgáltatási rendszereit – beleértve a rendészetet – a skót parlamentre és az észak-írországi parlamentre ruházták át. Az Egyesült Királyság nem rendelkezik rögzített alkotmányos okmány értelmében vett kodifikált alkotmánnyal. Az idő múlásával kialakultak az alkotmányos elvek, amelyek különösen az ítélkezési gyakorlatból és a szokásjogból származnak. A bíróságok elismerik bizonyos törvények, például a Magna Carta, az 1689-es Bill of Rights és az 1998-as emberi jogi törvény alkotmányos értékét. Az egyének alapvető jogait az alkotmány részeként fejlesztették ki a „common law", e törvények és nemzetközi szerződések, különösen az Egyesült Királyság által 1951-ben ratifikált emberi jogok európai egyezménye révén. Az Egyesült Királyság 1987-ben ratifikálta az Európa Tanács az egyéneknek a személyes adatok gépi feldolgozása során való védelméről szóló egyezményét (108. egyezmény) ([10]).

(10) Az 1998. évi emberi jogi törvény beépíti az emberi jogok európai egyezményében foglalt jogokat az Egyesült Királyság jogába. Az emberi jogi törvény minden egyén számára biztosítja az emberi jogok európai egyezményének 2–12. és 14. cikkében, valamint az első jegyzőkönyve 1., 2. és 3. cikkében és a tizenharmadik jegyzőkönyv 1. cikkében – az EJEE 16, 17. és 18. cikkével együttesen – biztosított alapvető jogokat és szabadságokat. Ez magában foglalja a magán- és a családi élet tiszteletben tartásához való jogot (és e jog részeként az adatvédelemhez való jogot) és a tisztességes eljáráshoz való jogot ([11]). Az Egyezmény 8. cikke értelmében e jog gyakorlásába hatóság csak a törvényben meghatározott, olyan esetekben avatkozhat be, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges.

(11) Az 1998. évi emberi jogi törvénynek megfelelően a hatóságok minden intézkedésének összeegyeztethetőnek kell lennie az egyezmény szerinti jogokkal ([12]). Ezenkívül az elsődleges és az alárendelt jogszabályokat az egyezmény szerinti jogokkal összeegyeztethető módon kell értelmezni és érvényre juttatni ([13]).

2.2. **Az Egyesült Királyság adatvédelmi kerete**

(12) Az Egyesült Királyság 2020. január 31-én kilépett az Európai Unióból. A Nagy-Britannia és Észak-Írország Egyesült Királyságának az Európai Unióból és az Európai Atomenergia-közösségből történő kilépéséről szóló megállapodás ([14]) alapján az uniós jogszabályok a 2020. december 31-ig tartó átmeneti időszakban alkalmazandók voltak az Egyesült Királyságban. A kilépés előtt és az átmeneti időszak alatt a személyes adatok Egyesült Királyságban történő védelmére vonatkozó jogszabályi keretet a vonatkozó uniós jogszabályok (különösen az (EU) 2016/679 rendelet és az (EU) 2016/680 európai parlamenti és tanácsi irányelv ([15])) és a nemzeti jogszabályok, különösen a Data Protection Act 2018 elnevezésű törvény (2018. évi adatvédelmi törvény) ([16]) alkották, amely előírta a nemzeti szabályokat, amennyiben az (EU) 2016/679 rendelet lehetővé tette, meghatározva és korlátozva az (EU) 2016/679 rendelet szabályainak alkalmazását és átültette az (EU) 2016/680 irányelvet.

([10]) A 108. egyezmény elveit az Egyesült Királyság jogába eredetileg az 1984-es adatvédelmi törvény révén ültették át, amelyet felváltott az 1998-as adatvédelmi törvény, majd pedig a 2018-as adatvédelmi törvény (az Egyesült Királyság általános adatvédelmi rendeletével együttesen értelmezve). Az Egyesült Királyság 2018-ban aláírta az egyéneknek a személyes adatok gépi feldolgozása során való védelméről szóló egyezményt módosító jegyzőkönyvet (az úgynevezett 108+ egyezményt), és jelenleg az egyezmény ratifikálásán dolgozik.

([11]) Az EJEE 6. és 8. cikke (lásd még az 1998. évi emberi jogi törvény 1. mellékletét).

([12]) Az 1998. évi emberi jogi törvény 6. szakasza.

([13]) Az 1998. évi emberi jogi törvény 3. szakasza.

([14]) Megállapodás Nagy-Britannia és Észak-Írország Egyesült Királyságának az Európai Unióból és az Európai Atomenergia-közösségből történő kilépéséről, 2019/C 384 I/01, XT/21054/2019/INIT (HL C 384I., 2019.11.12., 1. o., elérhető a következő linken: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=HU

([15]) Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az említett adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (HL L 119., 2016.5.4., 89. o.), elérhető a következő linken: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L0680&from=HU

([16]) A 2018. évi adatvédelmi törvény a következő linken érhető el: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

(13) Az Európai Unióból való kilépés előkészítése érdekében az Egyesült Királyság kormánya elfogadta az European Union (Withdrawal) Act 2018 ([17]) elnevezésű (kilépési) törvényt (kilépési törvény), amely beépítette a közvetlenül alkalmazandó uniós jogszabályokat az Egyesült Királyság jogába ([18]). Ezek az úgynevezett „megtartott uniós jogszabályok" teljes egészében magukban foglalják az (EU) 2016/679 rendeletet (annak preambulumbekezdéseivel együtt) ([19]). Az említett törvénnyel összhangban a módosítás nélkül megtartott uniós jogszabályokat az Egyesült Királyság bíróságainak az Európai Unió Bírósága (Bíróság) vonatkozó ítélkezési gyakorlatának és az uniós jog általános elveinek megfelelően kell értelmezniük, mivel azok közvetlenül az átmeneti időszak vége előtt hatályban voltak (a továbbiakban: „megtartott uniós ítélkezési gyakorlat", illetve „az uniós jog megtartott általános elvei") ([20]).

(14) A 2018. évi kilépési törvény értelmében az Egyesült Királyság miniszterei hatáskörrel rendelkeznek arra, hogy jogszabályi eszközök útján másodlagos jogszabályokat vezessenek be, hogy a megtartott uniós jogszabályokban elvégezzék az Egyesült Királyság Unióból való kilépéséből következő módosításokat. A hatáskör gyakorlását a Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 elnevezésű jogszabály (a kilépéssel kapcsolatos adatvédelmi szabályozás) ([21]) elfogadása jelentette. A kilépéssel kapcsolatos adatvédelmi szabályozás úgy módosítja az Egyesült Királyság jogába beépített (EU) 2016/679 rendeletet a 2018. évi kilépési törvény, a 2018. évi adatvédelmi törvény és más adatvédelmi jogszabályok révén, hogy az illeszkedjen a hazai környezetbe ([22]).

(15) Ennek következtében az Egyesült Királyságban az átmeneti időszak vége után a személyes adatok védelmére vonatkozó jogi keret a következőkből áll:

– az Egyesült Királyság általános adatvédelmi rendelete, az Egyesült Királyság jogszabályaiba a 2018. évi kilépési törvénye alapján beépített, és a kilépéssel kapcsolatos adatvédelmi szabályozással módosított ([23]) formában, és

– a kilépéssel kapcsolatos adatvédelmi szabályozással módosított 2018. évi adatvédelmi törvény ([24]).

(16) Ahogy az Egyesült Királyság általános adatvédelmi rendeletének alapját az uniós jogszabályok képezik, az Egyesült Királyság adatvédelmi szabályai sok szempontból szorosan tükrözik az Európai Unióban alkalmazandó, megfelelő szabályokat.

(17) A miniszter számára a 2018. évi kilépési törvény által biztosított hatáskörök mellett a 2018. évi adatvédelmi törvény számos rendelkezése felhatalmazást ad a miniszternek arra, hogy másodlagos jogszabályokat fogadjon el a törvény egyes rendelkezéseinek módosítására, illetve kiegészítő és további rendelkezések előírására ([25]). A miniszter eddig a 2018. évi adatvédelmi törvény 137. szakasza szerinti hatáskört csak a Data Protection (Charges and Information)

([17]) A 2018. évi kilépési törvény a következő linken érhető el: https://www.legislation.gov.uk/ukpga/2018/16/contents

([18]) A 2018. évi kilépési törvény célja és hatása az, hogy minden olyan közvetlen hatályú uniós jogszabályt, amely az átmeneti időszak végén része volt az Egyesült Királyság jogának, beépített az Egyesült Királyság jogába, ahogyan azok közvetlenül az átmeneti időszak vége előtt az uniós jogban hatályosak voltak, lásd a 2018. évi kilépési törvény 3. szakaszát.

([19]) A 2018. évi kilépési törvény indokolása a következőket írja elő: „Ha a jogszabályokat e szakasz alapján átalakítják, ott maga a jogszabály szövege fogja a hazai jogszabályok részét képezni. Ez magában fogja foglalni minden uniós jogi aktus teljes szövegét (beleértve annak preambulumbekezdéseit is)". (A 2018. évi kilépési törvény indokolása, 83. pont, elérhető a következő linken: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Az Egyesült Királyság hatóságai által szolgáltatott információk szerint, mivel a preambulumbekezdések nem rendelkeznek a kötelező érvényű jogszabályok jogállásával, nem volt szükség azoknak az (EU) 2016/679 rendelet cikkeinek a kilépéssel kapcsolatos adatvédelmi szabályozásban történttel megegyező módosítására.

([20]) A 2018. évi kilépési törvény 6. szakasza.

([21]) A Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 elnevezésű jogszabály a következő linken érhető el: https://www.legislation.gov.uk/uksi/2019/419/contents/made, a kilépéssel kapcsolatos 2020. évi adatvédelmi szabályozással módosított formában a következő linken érhető el: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([22]) Az Egyesült Királyság általános adatvédelmi rendeletének és a 2018. évi adatvédelmi törvénynek ezek a módosításai többnyire technikai jellegűek, például a „tagállamokra" történő hivatkozások törlése vagy a terminológia kiigazítása, például az (EU) 2016/679 rendeletre történő hivatkozások felváltása az Egyesült Királyság általános adatvédelmi rendeletére való hivatkozásokkal. Bizonyos esetekben változtatásokra volt szükség a rendelkezések tisztán belföldi összefüggéseinek megjelenítése érdekében, például azzal kapcsolatban, hogy az Egyesült Királyság adatvédelmi jogszabályi keretrendszere alkalmazásában „ki" fogad el „megfelelőségi rendeleteket" (lásd a 2018. évi adatvédelmi törvény 17A. szakaszát), azaz az Európai Bizottság helyett a miniszter.

([23]) Általános adatvédelmi rendelet, Keeling melléklet, elérhető a következő linken: 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]) A 2018. évi adatvédelmi törvény Keeling melléklete a következő linken érhető el: 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]) Ezeket a hatásköröket például a 2018. évi adatvédelmi törvény 16. (hatáskör arra, hogy meghatározott, szűken körülírt helyzetekben további kivételeket engedjen az Egyesült Királyság általános adatvédelmi rendeletének egyes rendelkezései alól), 17A. (hatáskör megfelelőségi rendeletek elfogadására), 212. és 213. (hatáskör jogszabály kezdeményezésére és átmeneti intézkedések elfogadására), valamint 211. szakasza (hatáskör kisebb és következményi módosítások elvégzésére) tartalmazza.

(Amendment) Regulations elnevezésű (az adatvédelem (díjak és információk) (módosítás) 2019. évi) szabályozás elfogadására vette igénybe, amely meghatározza azokat a körülményeket, amelyek mellett az adatkezelőknek éves díjat kell fizetniük az Egyesült Királyság független adatvédelmi hatóságának, az információügyi biztosnak.

(18) Végül további útmutatás található az Egyesült Királyság adatvédelmi jogszabályairól az információügyi biztos által elfogadott gyakorlati kódexekben és egyéb útmutatókban. Bár formálisan nem jogilag kötelező érvényű, az útmutatónak értelmezési súlya van, és bemutatja, hogy az adatvédelmi jogszabályokat miként alkalmazza és a biztos hogyan juttatja érvényre a gyakorlatban. Különösen a 2018. évi adatvédelmi törvény 121–125. szakasza írja elő a biztos számára az adatmegosztásra, a direkt marketingre, az életkornak megfelelő tervezésre, az adatvédelem és az újságírás kérdéskörére vonatkozó gyakorlati kódex elkészítését.

(19) Az Egyesült Királyság e határozat alapján továbbított adatokra alkalmazandó jogi kerete felépítésében és fő alkotóelemeiben tehát nagyon hasonló az Európai Unióban alkalmazotthoz. Ennek része az a tény, hogy az említett keretrendszer nem csak a nemzeti jogban meghatározott, az uniós jog által kialakított kötelezettségekre támaszkodik, hanem a nemzetközi jogban rögzített kötelezettségekre is, különösen az EJEE és a 108. egyezmény Egyesült Királyság általi betartása, valamint az Emberi Jogok Európai Bírósága joghatóságának való alávetése révén. Ezek a jogilag kötelező érvényű nemzetközi okmányokból eredő, nevezetesen a személyes adatok védelme tekintetében fennálló kötelezettségek ezért az e határozatban értékelt jogi keret kiemelt jelentőségű elemét képezik.

2.3. **Tárgyi és területi hatály**

(20) Az (EU) 2016/679 rendelethez hasonlóan az Egyesült Királyság általános adatvédelmi rendelete vonatkozik a személyes adatok részben vagy egészben automatizált módon történő kezelésére, vagy egyéb adatkezelésre, ha a személyes adatok egy nyilvántartási rendszer részét képezik ([26]). Az Egyesült Királyság általános adatvédelmi rendeletében a „személyes adatok", az „érintett" és a „feldolgozás" fogalommeghatározása megegyezik az (EU) 2016/679 rendeletben adott meghatározással ([27]). Ezenkívül az Egyesült Királyság általános adatvédelmi rendelete az egyes egyesült királyságbeli hatóságok birtokában levő ([28]) személyes adatok kézi strukturálatlan kezelésre is vonatkozik ([29]), bár az Egyesült Királyság általános adatvédelmi rendelete szerinti, az említett személyes adatok vonatkozásában nem releváns alapelvek és jogok alkalmazását a 2018. évi adatvédelmi törvény 24. és 25. szakasza beszüntette. Az (EU) 2016/679 rendeletben előírtakhoz hasonlóan az Egyesült Királyság általános adatvédelmi rendelete nem vonatkozik a személyes adatok természetes személy által kizárólag személyes vagy otthoni tevékenység keretében végzett kezelésére ([30]).

(21) Az Egyesült Királyság általános adatvédelmi rendelete kiterjeszti hatályát azon tevékenység során történt adatkezelésre is, amely közvetlenül az átmeneti időszak vége előtt az uniós jog hatályán kívül esett (pl. nemzetbiztonság) ([31]), vagy az Európai Unióról szóló szerződés 5. címének 2. fejezete (közös kül- és biztonságpolitikai tevékenységek) hatálya alá tartozott ([32]). Az Európai Unió rendszeréhez hasonlóan az Egyesült Királyság általános adatvédelmi rendelete nem vonatkozik a személyes adatok illetékes hatóságok általi, bűncselekmények megelőzése, kivizsgálása, felderítése vagy büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából történő kezelésére, ideértve a közbiztonságot fenyegető veszélyek elleni védelmet és azok megelőzését (ún.

([26]) Az Egyesült Királyság általános adatvédelmi rendelete 2. szakaszának (1) és (5) bekezdése.

([27]) Az Egyesült Királyság általános adatvédelmi rendelete 4. szakaszának (1) és (2) bekezdése.

([28]) Az Egyesült Királyság általános adatvédelmi rendelete 2. szakaszának (1A) bekezdése előírja, hogy a rendelet az információszabadsággal foglalkozó hatóságok birtokában lévő strukturálatlan személyes adatok kézi kezelésére is vonatkozik. Az információszabadsággal foglalkozó hatóságokra való hivatkozás a 2000. évi információszabadságról szóló törvényben meghatározott összes hatóság, illetve a Freedom of Information (Scotland) Act 2002 elnevezésű (2002. évi információszabadságról (Skócia) szóló) törvényben (13. asp.) meghatározott skót hatóságok. A 2018. évi adatvédelmi törvény 21. szakaszának (5) bekezdése.

([29]) A személyes adatok kézi, strukturálatlan kezelését a 2. cikk (5) bekezdésének b) pontja a személyes adatok olyan kezeléseként határozza meg, amely nem minősül a személyes adatok automatizált vagy strukturált kezelésének.

([30]) Az Egyesült Királyság általános adatvédelmi rendelete 2. szakaszának (2) bekezdése.

([31]) A nemzetbiztonsági tevékenységek csak annyiban tartoznak az Egyesült Királyság általános adatvédelmi rendeletének hatálya alá, amennyiben azokat nembűnüldözési célokra illetékes hatóság (ebben az esetben a 2018. évi adatvédelmi törvény 3. részét kell alkalmazni) vagy hírszerző ügynökség végzi (amelynek tevékenységét kivették az Egyesült Királyság általános adatvédelmi rendeletének hatálya alól, és az Egyesült Királyság általános adatvédelmi rendelete 2. cikke (2) bekezdésének c) pontja alapján a 2018. évi adatvédelmi törvény 4. részének hatálya alá tartozik). Például a rendőrség biztonsági ellenőrzéseket végezhet egy munkavállaló ellen annak biztosítása érdekében, hogy meg lehessen benne bízni nemzetbiztonsági anyagokhoz való hozzáférés tekintetében. Annak ellenére, hogy a rendőrség bűnüldözési szempontból illetékes hatóság, a kérdéses adatkezelés nem bűnüldözési célú, és az Egyesült Királyság általános adatvédelmi rendeletét kell alkalmazni. Lásd az Egyesült Királyság magyarázatát a megfelelőségi megbeszélésekre, H. szakasz: Nemzetbiztonsági adatvédelmi és nyomozati hatásköri keret, 8. oldal, elérhető a következő linken https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf

([32]) Az Egyesült Királyság általános adatvédelmi rendelete 2. szakasza (1) bekezdésének a) és b) pontja.

„bűnüldözési célok") – az említett adatkezelést ehelyett a 2018. évi adatvédelmi törvény 3. része szabályozza, ahogyan ez az európai uniós jogban az (EU) 2016/680 irányelv szerint történik, vagy a személyes adatok hírszerző ügynökségek (a biztonsági szolgálat, a titkosszolgálat és a kormányzati kommunikációs központ) általi kezelésére, amelyet a 2018. évi adatvédelmi törvény 4. része szabályoz ([33]).

(22) Az Egyesült Királyság általános adatvédelmi rendeleténekterületi hatályát a 3. szakasz ([34]) ismerteti és az alá tartozik az Egyesült Királyságban az adatkezelő vagy az adatfeldolgozó telephelyének tevékenységeivel összefüggő személyes adatok kezelése (függetlenül attól, hogy hol történik), az Egyesült Királyságban tartózkodó érintettek személyes adatainak kezelése, amennyiben az adatkezelési tevékenységek az érintetteknek áruk vagy szolgáltatások felkínálásával vagy viselkedésük figyelemmel kísérésével kapcsolatosak ([35]). Ez az (EU) 2016/679 rendelet 3. cikkének megközelítését tükrözi.

2.4. **A személyes adat, valamint az adatkezelő és az adatfeldolgozó fogalmának meghatározása**

(23) Az Egyesült Királyság általános adatvédelmi rendelete a személyes adatok, az adatkezelés, az adatkezelő, az adatfeldolgozó, valamint az álnevesítés (EU) 2016/679 rendeletben adott fogalommeghatározását lényeges módosítások nélkül megtartotta ([36]). Ezenkívül az Egyesült Királyság általános adatvédelmi rendelete 9. szakaszának (1) bekezdése ugyanúgy határozza meg a különleges adatok kategóriáit, mint az (EU) 2016/679 rendelet („faji vagy etnikai származás, politikai vélemények, vallási vagy filozófiai meggyőződések felfedése, vagy szakszervezeti tagság, valamint genetikai adatok, biometrikus adatok kezelése természetes személy egyedi azonosítása céljából, egészségügyi adatok, illetve természetes személy szexuális életére vagy szexuális irányultságára vonatkozó adatok"). A 2018. évi adatvédelmi törvény 205. szakasza adja a „biometrikus adatok" ([37]), „az egészségügyi adatok" ([38]) és „a genetikai adatok" ([39]) fogalmának meghatározását.

2.5. **Biztosítékok, jogok és kötelezettségek**

2.5.1. *Az adatkezelés jogszerűsége és tisztességessége*

(24) A személyes adatokat jogszerűen és tisztességesen kell kezelni.

(25) A jogszerűség, a tisztesség és az átláthatóság elveit, valamint a jogszerű adatkezelési okokat az Egyesült Királyság törvényei garantálják az Egyesült Királyság általános adatvédelmi rendeletének 5. cikke (1) bekezdésének a) pontján és 6. szakaszának (1) bekezdésén keresztül, amelyek megegyeznek a (EU) 2016/679 rendelet vonatkozó rendelkezéseivel ([40]). A 2018. évi adatvédelmi törvény 8. szakasza kiegészíti a 6. cikk (1) bekezdésének e) pontját azzal, hogy a személyes adatok Egyesült Királyság általános adatvédelmi rendelete 6. cikke (1) bekezdésének e) pontja alapján történő kezelése (a közérdekből végzett feladatok ellátásához, vagy az adatkezelő hatósági

([33]) Az Egyesült Királyság általános adatvédelmi rendelete 2. szakasza (2) bekezdésének b) és c) pontja.

([34]) Ugyanez a területi hatály érvényes a személyes adatok az Egyesült Királyság általános adatvédelmi rendeletét kiegészítő 2018. évi adatvédelmi törvény 2. része szerinti kezelésére (207. szakasz (1A) bekezdés).

([35]) Ez annyit jelent, hogy a 2018. évi adatvédelmi törvény és ezért ez a határozat sem vonatkozik az Egyesült Királyság koronagyarmataira (Jersey, Guernsey és Man-sziget) és az Egyesült Királyság tengerentúli területeire, például a Falkland-szigetekre és Gibraltár területére.

([36]) Az Egyesült Királyság általános adatvédelmi rendelete 4. szakaszának (1), (2), (5), (7) és (8) bekezdése.

([37]) „Biometrikus adat": egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a magánszemély egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat.

([38]) „Egészségügyi adat": egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a magánszemély számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információkat hordoz a magánszemély egészségi állapotáról.

([39]) „Genetikai adat": egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered.

([40]) Az Egyesült Királyság általános adatvédelmi rendelete 6. szakaszának (1) bekezdése szerint az adatkezelés csak akkor és annyiban engedélyezett, ha: a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez; b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges; c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges; d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges; e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges; vagy f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

hatáskörének gyakorlása során szükséges adatkezelés) magában foglalja az igazságszolgáltatás igazgatásához, a Parlament bármelyik házának feladatainak ellátásához, valamely személy törvény vagy a jogállamiság által ráruházott funkciójának gyakorlásához, az állam, valamely miniszter vagy egy kormányzati szerv funkciójának gyakorlásához, vagy a demokratikus elkötelezettséget támogató vagy elősegítő tevékenységhez.

(26) A hozzájárulás (a jogszerű feldolgozás egyik alapja) tekintetében az Egyesült Királyság általános adatvédelmi rendelete változatlanul megtartja az (EU) 2016/679 rendelet 7. cikkében előírt feltételeket, vagyis az adatkezelőnek képesnek kell lennie annak bizonyítására, hogy az érintett hozzájárulását adta, az írásbeli hozzájárulás iránti kérelmet világos és érthető nyelven kell bemutatni, az érintettnek bármikor jogában áll visszavonni a hozzájárulását, és annak értékelésekor, hogy a hozzájárulás szabadon megadott-e, figyelembe kell venni, hogy a szerződés teljesítésének feltétele olyan személyes adatok kezeléséhez való hozzájárulás, amelyek nem szükségesek az adott szerződés teljesítéséhez. Ezenkívül az Egyesült Királyság általános adatvédelmi rendeletének 8. cikke értelmében az információs társadalommal összefüggő szolgáltatások nyújtásával összefüggésben gyermek hozzájárulása csak akkor jogszerű, ha a gyermek legalább 13 éves. Ez az (EU) 2016/679 rendelet 8. cikkében megállapított életkori tartományon belül esik.

2.5.2. *A különleges személyes adatok kategóriáinak kezelése*

(27) „Különleges adatok kategóriáinak” kezelése esetén külön biztosítékokat kell rendszeresíteni.

(28) Az Egyesült Királyság általános adatvédelmi rendelete és a 2018. évi adatvédelmi törvény különös szabályokat tartalmaz a különleges személyes adatok kategóriáinak kezelésére vonatkozóan, amelyeket az Egyesült Királyság általános adatvédelmi rendelete 9. szakaszának (1) bekezdése határoz meg ugyanúgy, mint az (EU) 2016/679 rendelet (lásd a (23) above preambulumbekezdést). Az Egyesült Királyság általános adatvédelmi rendeletének 9. cikke szerint a különleges adatok kategóriáinak feldolgozása elvileg tilos, kivéve, ha erre külön kivétel vonatkozik.

(29) Ezek a kivételek (az Egyesült Királyság általános adatvédelmi rendelete 9. szakaszának (2) és (3) bekezdésében felsoroltak) nem változtatnak érdemben az (EU) 2016/679 rendelet 9. cikkének (2) és (3) bekezdésében leírtakon. Amennyiben az érintett nem adott kifejezett hozzájárulást a személyes adatok kezeléséhez, a különleges személyes adatok kategóriáinak feldolgozása csak meghatározott és korlátozott körülmények között engedélyezett. A legtöbb esetben a különleges adatok kezelésének a vonatkozó rendelkezésben meghatározott célra szükségesnek kell lennie (lásd a 9. szakasz (2) bekezdésének b), c), f), g), h), i) pontját és (j)).

(30) Ezenkívül, ha az Egyesült Királyság általános adatvédelmi rendelete 9. szakaszának (2) bekezdése szerinti kivétel törvényi engedélyhez kötött vagy a közérdeken alapul, a 2018. évi adatvédelmi törvény 10. szakasza, valamint a 2018. évi adatvédelmi törvény 1. melléklete pontosítja azokat a feltételeket, amelyeknek teljesülniük kell a kivételek igénybevételéhez. Például különleges adatok „közegészség” védelme céljából történő feldolgozása esetén (az Egyesült Királyság általános adatvédelmi rendelete 9. szakasza (2) bekezdésének i) pontja) az 1. melléklet 1. része (3) bekezdésének b) pontja előírja a szükségességi teszt mellett, hogy az említett adatkezelést „egészségügyi szakember vagy annak felelősségére más végzi” vagy „egy másik személy, aki törvény vagy a jogállamiság alapján titoktartási kötelezettséggel tartozik”, ideértve a „common law” szerint kialakult titoktartási kötelezettségét .

(31) Amennyiben különleges adatokat jelentős közérdekből kezelnek (az Egyesült Királyság általános adatvédelmi rendelete 9. szakasza (2) bekezdésének g) pontja), a 2018. évi adatvédelmi törvény 1. mellékletének 2. része tételesen felsorolja azokat a célokat, amelyek jelentős közérdekűnek tekinthetők, és e célok mindegyikére külön további feltételeket határoz meg. Például a faji és etnikai sokféleség szervezetek felsőbb szintjein való előmozdítását jelentős közérdekként ismerik el. A különleges adatok e konkrét célú kezelésére részletes követelmények vonatkoznak, beleértve azt is, hogy az adatkezelés a vezető tisztség betöltésére alkalmas személyek azonosításának részeként történik, a faji és etnikai sokszínűség előmozdításához szükséges, és valószínűleg nem okoz jelentős kárt vagy sérelmet az érintett számára.

(32) A 2018. évi adatvédelmi törvény 11. szakaszának (1) bekezdése meghatározza a személyes adatok az Egyesült Királyság általános adatvédelmi rendeletének a titoktartási kötelezettségre vonatkozó 9. szakaszának (3) bekezdésében leírt körülmények közötti kezelésének feltételeit. Ez magában foglalja azokat a körülményeket, amelyekben az adatkezelést egészségügyi szakember vagy szociális területen dolgozó szakember vagy annak felelőssége alatt más hajtja végre, vagy más olyan személy, aki e körülmények között titoktartási kötelezettséggel tartozik törvény vagy jogállamiság alapján.

(33) Ezenkívül az Egyesült Királyság általános adatvédelmi rendelete 9. szakaszának (2) bekezdésében felsorolt számos kivétel igénybevételéhez megfelelő és konkrét biztosítékok szükségesek. Az adatkezelés jellegétől, valamint az érintettek jogait és szabadságait érintő kockázat mértékétől függően a 2018. évi adatvédelmi törvény 1. mellékletében előírt adatkezelési feltételek különböző biztosítékokat állapítanak meg. Az 1. melléklet viszont az egyes feldolgozási helyzetek feltételeit határozza meg.

(34) Bizonyos esetekben a 2018. évi adatvédelmi törvény szabályozza és korlátozza azon különleges adatok típusát, amelyeket egy adott jogalap alapján lehet kezelni. Például az 1. melléklet 8. pontja engedélyezi a különleges adatok kezelését az esélyegyenlőség vagy az egyenlő bánásmód előmozdítása céljából. Ez az adatkezelési feltétel csak akkor használható, ha az adatok faji vagy etnikai származást, vallási vagy filozófiai meggyőződéseket, szexuális irányultságot tárnak fel, vagy ha egészségügyi adatokról van szó.

(35) Bizonyos esetekben a 2018. évi adatvédelmi törvény korlátozza azon adatkezelő típusát, amely igénybe veheti ezt az adatkezelési feltételt. Például az 1. melléklet 23. pontja különleges adatok kezeléséről rendelkezik a megválasztott képviselők lakosságnak adott válaszaival kapcsolatban. Ez az adatkezelési feltétel csak akkor alkalmazható, ha az adatkezelő megválasztott képviselő, vagy az ő felügyelete alatt jár el.

(36) Néhány más esetben a 2018. évi adatvédelmi törvény korlátokat határoz meg az alkalmazandó feldolgozási feltétel szempontjából az érintettek kategóriáira vonatkozóan. Például az 1. melléklet 21. pontja szabályozza a foglalkozási nyugdíjrendszerek bizalmas adatainak kezelését. Ez a feltétel csak akkor alkalmazható, ha a szóban forgó érintett a nyugdíjrendszer tagjának testvére, szülője, nagyszülője vagy dédszülője.

(37) Ezen túlmenően az Egyesült Királyság általános adatvédelmi rendelete 9. szakaszának (2) bekezdésében szereplő kivételek – amelyeket a 2018. évi adatvédelmi törvény 10. szakasza, a 2018. évi adatvédelmi törvény 1. mellékletével együtt tovább részletez – igénybevételekor az adatkezelőnek a legtöbb esetben „megfelelő adatvédelmi szabályzatot" kell készítenie. Fel kell vázolnia az adatkezelő Egyesült Királyság általános adatvédelmi rendeletének 5. szakaszában foglalt elvek betartásának biztosítására szolgáló eljárásait. Meg kell határoznia a megőrzésre és a törlésre vonatkozó irányelveket is, feltüntetve a valószínű tárolási időt. Az adatkezelőknek szükség szerint felül kell vizsgálniuk és frissíteniük kell ezt a dokumentumot. Az adatkezelőnek az adatkezelés befejezését követően hat hónapig meg kell őriznie az adatvédelmi szabályzatot, és kérésre az információügyi biztos rendelkezésére kell bocsátania ([41]).

(38) A 2018. évi adatvédelmi törvény 1. mellékletének 41. pontja szerint az adatvédelmi szabályzatot mindig az adatkezelés bővített nyilvántartásának kell kísérnie. Ennek a nyilvántartásnak nyomon kell követnie az adatvédelmi szabályzatban foglalt kötelezettségvállalásokat, vagyis azt, hogy a szabályzatnak megfelelően törlik-e vagy megőrzik-e az adatokat. Ha az adatvédelmi szabályzatot nem tartották be, akkor a naplóban fel kell tüntetni ennek okait. A nyilvántartásnak azt is le kell írnia, hogy az adatkezelés miként teljesíti az Egyesült Királyság általános adatvédelmi rendeletének 6. szakaszát (az adatkezelés jogszerűsége), valamint a 2018. évi adatvédelmi törvény 1. mellékletében szereplő konkrét feltételt.

(39) Végül, hasonlóan az (EU) 2016/679 rendelethez, az Egyesült Királyság általános adatvédelmi rendelete is általános biztosítékokat ír elő a különleges adatok kategóriáin végzett egyes adatkezelési műveletekhez. Az Egyesült Királyság általános adatvédelmi rendeletének 35. szakasza előírja az adatvédelemre vonatkozó hatásvizsgálatot, ha különleges adatok kategóriáinak nagybani kezelését végzik. Az Egyesült Királyság általános adatvédelmi rendeletének 37. szakasza értelmében az adatkezelőnek vagy az adatfeldolgozónak ki kell jelölnie egy adatvédelmi tisztviselőt, ha fő tevékenysége a különleges adatok kategóriáinak nagybani kezelése.

(40) A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok tekintetében az Egyesült Királyság általános adatvédelmi rendeletének 10. szakasza megegyezik az (EU) 2016/679 rendelet 10. cikkével. Ez a büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelését csak a hatóság ellenőrzése alatt, vagy akkor teszi lehetővé, ha az adatkezelést az érintettek jogainak és szabadságainak megfelelő biztosítékokat biztosító nemzeti jogszabályok engedélyezik.

(41) Ha büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó adatok feldolgozása nem hatósági felügyelet alatt történik, a 2018. évi adatvédelmi törvény 10. szakaszának (5) bekezdése előírja, hogy az említett feldolgozás csak a 2018. évi adatvédelmi törvény 1. mellékletének 1., 2. és 3. részében meghatározott célokra/helyzetekben történhet, és arra vonatkoznak az egyes célokra/helyzetekre meghatározott külön követelmények. Például a büntetőjogi felelősség megállapítására vonatkozó határozatok adatait nonprofit szervezetek kezelhetik, ha az adatkezelést a) jogszerű tevékenysége során megfelelő biztosítékokkal végzi egy alapítvány, egyesület vagy más politikai, filozófiai, vallási vagy szakszervezeti célú nonprofit szerv, és b) azzal a feltétellel, hogy i. az adatkezelés kizárólag a testület tagjaira vagy korábbi tagjaira vagy olyan személyekre vonatkozik, akik rendszeres kapcsolatban állnak vele a céljaival kapcsolatban, és ii. a személyes adatokat az érintettek hozzájárulása nélkül nem adják ki a szervezeten kívül.

([41]) A 2018. évi adatvédelmi törvény 1. mellékletének 38–40. pontja.

(42) Emellett a 2018. évi adatvédelmi törvény 1. mellékletének 3. része további olyan körülményeket határoz meg, amelyek fennállása esetén a büntetőjogi felelősség megállapítására vonatkozó határozatokkal kapcsolatos adatok felhasználhatók, és ezek megfelelnek a különleges adatok kezelésére az (EU) 2016/679 rendelet 9. cikkének (2) bekezdésében szereplő jogalapoknak és az Egyesült Királyság általános adatvédelmi rendeletének (pl. az érintett hozzájárulása, magánszemély létfontosságú érdekei, ha az érintett jogilag vagy fizikailag nem képes hozzájárulást adni, ha az érintett már nyilvánvalóan nyilvánosságra hozta az adatokat, ha az adatkezelés jogi igény megalapozásához, érvényesítéséhez vagy védelméhez szükséges stb.).

2.5.3. *Célhoz kötöttség, pontosság, adattakarékosság, tárolás korlátozása és adatbiztonság*

(43) A személyes adatok kezelésének konkrét célra kell történnie, és később csak olyan mértékben használhatók fel, amely az adatkezelés céljával nem összeegyeztethetetlen.

(44) Ezt az elvet az (EU) 2016/679 rendelet 5. cikke (1) bekezdésének b) pontja tartalmazza, és az Egyesült Királyság általános adatvédelmi rendelete 5. szakasza (1) bekezdésének b) pontja változtatás nélkül megtartotta. Az (EU) 2016/679 rendelet 6. cikkének (4) bekezdése szerinti összeegyeztethető további feldolgozás feltételeit szintén fenntartották, az Egyesült Királyság általános adatvédelmi rendelete 6. szakasza (4) bekezdésének a)–e) pontjában nem történt lényeges módosítás.

(45) Emellett a személyes adatoknak pontosnak kell lenniük, és szükség esetén naprakésszé kell azokat tenni. Továbbá megfelelőnek, relevánsnak és nem eltúlzottnak kell lenniük az adatkezelés céljaihoz képest, és elvben csak addig tárolhatók, ameddig az a személyes adatok kezelésének céljaihoz szükséges.

(46) Az adattakarékosságra, a pontosságra és a tárolás korlátozására vonatkozó alapelveket az (EU) 2016/679 rendelet 5. cikke (1) bekezdésének c)–e) pontja tartalmazza, és az Egyesült Királyság általános adatvédelmi rendeletében az 5. szakasza (1) bekezdésének c)–e) pontja azokat módosítások nélkül megtartja.

(47) A személyes adatokat olyan módon kell kezelni, amely biztosítja a biztonságukat, többek között a jogosulatlan vagy jogellenes kezelés elleni védelmüket is, illetve az adatok véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmüket. A gazdasági szereplőknek ebből a célból megfelelő technikai vagy szervezeti intézkedéseket kell hozniuk, hogy megvédjék a személyes adatokat a lehetséges veszélyektől. Ezeket az intézkedéseket a csúcstechnológia és a kapcsolódó költségek figyelembevételével kell értékelni.

(48) Az adatbiztonságot az Egyesült Királyság jogszabályai az integritás és titkosság elvén keresztül rögzítik az Egyesült Királyság általános adatvédelmi rendelete 5. szakasza (1) bekezdésének f) pontjában és annak az adatkezelés biztonságáról szóló 32. szakaszában. Ezek a rendelkezések megegyeznek az (EU) 2016/679 rendelet vonatkozó rendelkezéseivel. Sőt az (EU) 2016/679 rendelet 33. és 34. cikkében meghatározott feltételekkel egyezően az Egyesült Királyság általános adatvédelmi rendelete előírja a személyes adatok megsértésének a felügyeleti hatóság számára történő bejelentését(az Egyesült Királyság általános adatvédelmi rendeletének 33. szakasza), és a személyes adatok megsértésének az érintettel való közlését (az Egyesült Királyság általános adatvédelmi rendeletének 34. szakasza).

2.5.4. *Átláthatóság*

(49) Az érintetteket tájékoztatni kell személyes adataik kezelésének főbb jellemzőiről.

(50) Ezt az Egyesült Királyság általános adatvédelmi rendeletének 13. és 14. szakasza biztosítja, amelyek az átláthatóság általános elvén túl szabályokat írnak elő az érintettnek nyújtandó tájékoztatásról ([42]). Az Egyesült Királyság általános adatvédelmi rendelete nem vezet be lényeges módosításokat ezekben a szabályokban az (EU) 2016/679 rendelet megfelelő cikkeihez képest. Ugyanakkor, az (EU) 2016/679 rendelethez hasonlóan, e cikkek átláthatósági követelményeire a 2018. évi adatvédelmi törvényben meghatározott számos kivétel vonatkozik (lásd az (55)–(72) preambulumbekezdést).

([42]) A 13. szakasz (1) bekezdésének f) pontjában és a 14. szakasz (1) bekezdésének f) pontjában a megfelelőségre vonatkozó bizottsági határozatokra történő hivatkozásokat felváltották az egyenértékű egyesült királyságbeli eszközre, azaz a 2018. évi adatvédelmi törvény szerinti megfelelőségi rendeletekre történő hivatkozások. Ezen túlmenően a 14. szakasz (5) bekezdésének c)–d) pontjában az uniós vagy tagállami jogra való hivatkozások helyébe a nemzeti jogra történő hivatkozások léptek (a 14. szakasz (5) bekezdése c) pontjának hatálya alá tartozó nemzeti jogszabályokra példaként az Egyesült Királyság megemlítette a Scrap Metal Dealers Act 2013 elnevezésű (a fémhulladék-kereskedőkről szóló 2013. évi) törvény 7. szakaszát, amely szabályokat tartalmaz a fémhulladék-engedélyek nyilvántartására, vagy a Companies Act 2006 elnevezésű (2006. évi társasági) törvény 35. részét, amely szabályokat ír elő a cégjegyzék vezetője számára. Hasonlóképpen, a 14. cikk (5) bekezdésének d) pontja alá tartozó nemzeti jogszabályokra példaként felhozhatók a szakmai titoktartásra vonatkozó szabályokat megállapító jogszabályok, a munkaszerződésekben tükröződő kötelezettségek vagy a „common law” szerinti titoktartási kötelezettség (például az egészségügyi szakemberek, emberi erőforrások, szociális munkások stb. esetében).

2.5.5. *Az egyének jogai*

(51) Az érintetteknek rendelkezniük kell bizonyos jogokkal, amelyek érvényesíthetők az adatkezelővel vagy az adatfeldolgozóval szemben, különös tekintettel az adatokhoz való hozzáférés jogára, az adatkezelés elleni tiltakozásra, valamint az adatok helyesbíttetéséhez és töröltetéséhez való jogra. Ugyanakkor az említett jogok korlátozás alá eshetnek, amennyiben ezek a korlátozások szükségesek és arányosak a közbiztonság vagy más fontos, általános közérdekű célok megóvása érdekében.

2.5.5.1. Alanyi jogok

(52) Az Egyesült Királyság általános adatvédelmi rendelete ugyanazokat az érvényesíthető jogokat biztosítja az egyének számára, mint az (EU) 2016/679 rendelet. Az egyének jogait biztosító rendelkezéseket az Egyesült Királyság általános adatvédelmi rendeletében lényeges változások nélkül megtartották.

(53) A jogok magukban foglalják az érintett hozzáférési jogát (az Egyesült Királyság általános adatvédelmi rendeletének 15. szakasza), a helyesbítéshez való jogot (az Egyesült Királyság általános adatvédelmi rendeletének 16. szakasza), a törléshez való jogot (az Egyesült Királyság általános adatvédelmi rendeletének 17. szakasza), a korlátozáshoz való jogot az adatkezelés (az Egyesült Királyság általános adatvédelmi rendeletének 18. szakasza), a személyes adatok helyesbítésével vagy törlésével vagy az adatkezelés korlátozásával kapcsolatos értesítési kötelezettség (az Egyesült Királyság általános adatvédelmi rendeletének 19. szakasza), az adatok hordozhatóságához való jog (az Egyesült Királyság általános adatvédelmi rendeletének 20. szakasza) és a tiltakozási jog (az Egyesült Királyság általános adatvédelmi rendeletének 21. szakasza) ([43]). Ez utóbbi magában foglalja az érintett tiltakozási jogát is a személyes adatoknak az (EU) 2016/679 rendelet 21. cikkének (2) és (3) bekezdésében előírtak szerinti direkt marketing célú feldolgozása ellen. Ezenkívül a 2018. évi adatvédelmi törvény 122. szakasza szerint az információügyi biztosnak a direkt marketing végzésével kapcsolatban az adatvédelmi jogszabályok (és a Privacy and Electronic Communications (EC Directive) Regulations 2003 elnevezésű [a magánélet védelméről és az elektronikus hírközlésről (EK irányelv) szóló 2003. évi] szabályozás) követelményeinek megfelelő gyakorlati kódexet és a direkt marketing helyes gyakorlatának előmozdítására vonatkozó egyéb, a biztos által megfelelőnek tartott útmutatót kell készítenie. Az információügyi biztos hivatala jelenleg végzi a direkt marketing kódex kidolgozását ([44]).

(54) Az érintett GDPR 22. cikkében előírtak szerinti azon joga, hogy ne hozzanak róla kizárólag automatizált feldolgozáson alapuló olyan döntést, amely joghatásokat vált ki rá nézve, vagy hasonlóan jelentősen érinti őt, az Egyesült Királyság általános adatvédelmi rendeletében is lényeges változások nélkül megmaradt. Ugyanakkor egy új (3A) bekezdéssel egészült ki arra hivatkozásként, hogy a 2018. évi adatvédelmi törvény 14. szakasza biztosítékokat határoz meg az érintettek jogai, szabadságai és jogos érdekei vonatkozásában, amikor az adatkezelés az Egyesült Királyság általános adatvédelmi rendelete 22. szakasza (2) bekezdésének b) pontja alapján történik. Ez csak akkor érvényes, ha egy ilyen döntés alapja az Egyesült Királyság jogszabályai szerinti engedély vagy követelmény, és nem alkalmazható, ha a döntés szerződés alapján szükséges, vagy azt az érintett kifejezett hozzájárulásával hozzák meg. Amennyiben a 2018. évi adatvédelmi törvény 14. szakasza alkalmazandó, az adatkezelőnek a lehető leghamarabb írásban értesítenie kell az érintettet arról, hogy kizárólag automatizált feldolgozáson alapuló döntés született. Az érintettnek joga van kérni az adatkezelőt – az értesítés kézhezvételétől számított egy hónapon belül –, hogy vizsgálja felül a döntést vagy hozzon olyan új döntést, amely nem kizárólag automatizált feldolgozáson alapul. A miniszter felhatalmazást kap arra, hogy további biztosítékokat fogadjon el az automatizált döntéshozatal tekintetében. Ezt a hatáskört még nem gyakorolták.

2.5.5.2. Az egyének jogainak korlátozása és egyéb rendelkezések

(55) A 2018. évi adatvédelmi törvény számos korlátozást állapít meg az egyének jogai vonatkozásában, az Egyesült Királyság általános adatvédelmi rendeletének 23. szakasza keretébe illeszkedően. Ebben a keretben nem vezetnek be korlátozásokat a direkt marketing elleni, az Egyesült Királyság általános adatvédelmi rendelete 21. szakaszának (2) és (3) bekezdésében előírt tiltakozás joga, vagy az Egyesült Királyság általános adatvédelmi rendeletének 22. szakaszában előírt, az automatizált döntéshozatal elutasításának joga tekintetében.

(56) A korlátozásokat a 2018. évi adatvédelmi törvény 2–4. melléklete részletezi. Az Egyesült Királyság hatóságai kifejtették, hogy két alapelv vezérli őket: a specialitás elve (az aprólékosan részletes megközelítés, az átfogó korlátozások több, speciálisabb rendelkezésre bontása) és a feltételesség elve (minden rendelkezést biztosítékok egészítenek ki korlátozások vagy a visszaélések megelőzésének feltételei formájában) ([45]).

([43]) A 17. szakasz (1) bekezdésének e) pontjában és a 17. szakasz (3) bekezdésének b) pontjában az uniós vagy tagállami jogra történő hivatkozások helyébe a nemzeti jogra történő hivatkozások léptek (például a 17. szakasz (1) bekezdésének e) pontja szerint, az Egyesült Királyság megemlítette a Education (Pupil Information) (England) Regulations 2006 elnevezésű (2006. évi oktatási [tanulói tájékoztató]) [Anglia]) szabályozást, amely előírja a tanulók nevének törlését az iskolai nyilvántartásokból, miután elhagyták az iskolát, vagy a Medical Act 1983 elnevezésű (1983. évi orvosi) törvény 34F. szakasza, amely szabályokat határoz meg a nevek háziorvosi nyilvántartásból és a szakorvosi nyilvántartásból való törlésére.

([44]) A gyakorlati kódex tervezete a következő linken érhető el: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf

([45]) Az Egyesült Királyság magyarázata a megfelelőségi megbeszélésekre, E. szakasz: Korlátozások, 1. o., elérhető a következő linken: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf

(57) Az Egyesült Királyság általános adatvédelmi rendelete 23. szakaszának (1) bekezdésében leírt korlátozások célja annak biztosítása, hogy csak meghatározott körülmények között alkalmazzák azokat, amennyiben ez egy demokratikus társadalomban szükséges és ha arányosak az elérni kívánt jogszerű céllal. Továbbá a korlátozások értelmezéséről kialakult ítélkezési gyakorlatnak megfelelően az adatvédelmi rendszer alóli kivétel bármely konkrét esetben csak akkor alkalmazható, ha ez szükséges és arányos ([46]). A szükségességi tesztnek szigorúnak kell lennie, és megköveteli, hogy az érintett jogaiba való bármilyen beavatkozás álljon arányban a közérdeket fenyegető veszély súlyosságával. A gyakorlatnak tehát része egy klasszikus arányossági elemzés ([47])."

(58) Ezeknek a korlátozásoknak a céljai megfelelnek az (EU) 2016/679 rendelet 23. cikkében felsoroltaknak, a nemzetbiztonsági és védelmi korlátozások kivételével, amelyeket ehelyett a 2018. évi adatvédelmi törvény 26. szakasza szabályoz, de azokra ugyanazok a szükségességi és arányossági követelmények vonatkoznak (lásd a (63)–(66) preambulumbekezdést).

(59) Néhány korlátozás, például a bűncselekmények megelőzésével vagy felderítésével, az elkövetők elfogásával vagy üldözésével, valamint az adó vagy vám megállapításával vagy beszedésével kapcsolatos korlátozások ([48]) engedélyezik az egyének valamennyi jogának és az átláthatósági kötelezettségeknek a korlátozását (a 21. szakasz (2) bekezdésében és a 22. cikkben foglalt jogok kivételével). Az egyéb korlátozások hatálya az átláthatósági kötelezettségekre és a hozzáférési jogokra korlátozódik, például az ügyvédi titoktartással kapcsolatos korlátozásokra ([49]), az önvádhoz vezető információszolgáltatás követelménye alóli való mentesség jogához ([50]) és a vállalati pénzügyekre, nevezetesen a bennfentes kereskedelem megakadályozására ([51]). Néhány korlátozás engedélyezi az adatkezelő azon kötelezettségének korlátozását, hogy az adatvédelmi jogsértést az érintettel közölje, valamint a célhoz kötöttség, az adatkezelés jogszerűségének, tisztességességének és átláthatóságának elve korlátozását ([52]).

(60) A korlátozások egy része automatikusan „teljes egészében" vonatkozik a személyes adatok bizonyos típusú kezelésére (például az átláthatósági kötelezettségeknek és az egyének jogainak alkalmazása kizárt, ha a személyes adatokat valamely személy bírósági tisztségre való alkalmasságának értékelése céljából kezelik, vagy a személyes adatokat bíróság, törvényszék vagy magánszemély kezeli, bírósági minőségében eljárva).

(61) Az esetek többségében azonban a 2018. évi adatvédelmi törvény 2. mellékletének vonatkozó pontja kimondja, hogy a korlátozás csak akkor (és annyiban) alkalmazandó, amikor a rendelkezések alkalmazása „valószínűleg sértené" a korlátozás jogszerű célját: például az Egyesült Királyság általános adatvédelmi rendeletének felsorolt rendelkezései nem vonatkoznak a bűncselekmények megelőzése vagy felderítése, az elkövetők elfogása vagy büntetőeljárás alá vonása, illetőleg adó vagy illeték megállapítása vagy beszedése céljából kezelt személyes adatokra „olyan mértékben, amennyire e rendelkezések alkalmazása valószínűleg sértené" e kérdéskörök bármelyikét ([53]).

(62) A „valószínűleg sértené" mércét az Egyesült Királyság bíróságai következetesen „az azonosított közérdek sérelmének nagyon jelentős és súlyos esélyeként" ([54]) értelmezik. A sérelemteszt alá tartozó korlátozásra ezért csak akkor és olyan mértékben lehet hivatkozni, ha igen jelentős és súlyos esélye van annak, hogy egy bizonyos jog megadása sértené a szóban forgó közérdeket. Az adatkezelő feladata annak eseti alapon történő értékelése, hogy ezek a feltételek teljesülnek-e ([55]).

(63) A 2018. évi adatvédelmi törvény 2. mellékletében foglalt korlátozások mellett a 2018. évi adatvédelmi törvény 26. szakasza kivételt biztosít, amely az Egyesült Királyság általános adatvédelmi rendelete és a 2018. évi adatvédelmi törvény egyes rendelkezéseire alkalmazható, ha ez a kivétel a nemzetbiztonság védelméhez vagy védelmi célokból

([46]) Open Rights Group & Anor, R (kérelmére) kontra Secretary of State for the Home Department & Anor ügy (2019 EWHC 2562 (Admin)), 40. és 41. pont.

([47]) Guriev kontra Community Safety Development (Egyesült Királyság) Ltd ügy (2016 EWHC 643 (QB)), 43. pont. Erről lásd még a Lin kontra Commissioner of Police for the Metropoli ügy (2015 EWHC 2484 (QB)), 80. pontját.

([48]) A 2018. évi adatvédelmi törvény 2. mellékletének 2. pontja.

([49]) A 2018. évi adatvédelmi törvény 2. mellékletének 19. pontja.

([50]) A 2018. évi adatvédelmi törvény 2. mellékletének 20. pontja.

([51]) A 2018. évi adatvédelmi törvény 2. mellékletének 21. pontja.

([52]) Például a személyes adatok megsértéséről történő értesítéshez való jog korlátozása csak a bűnözéssel és az adózással (a 2018. évi adatvédelmi törvény 2. mellékletének 2. pontja), a parlamenti kiváltságokkal (a 2018. évi adatvédelmi törvény 2. mellékletének 13. pontja) és az újságírói, tudományos, művészeti és irodalmi célokra (a 2018. évi adatvédelmi törvény 2. mellékletének 26. pontja) történő adatkezelés esetében megengedett.

([53]) A 2018. évi adatvédelmi törvény 2. mellékletének 2. pontja.

([54]) Az R (Lord) kontra Secretary of State for the Home Department ügy (2003 EWHC 2073 (Admin)) 100. pontja, és a Guriev kontra Community Safety Development (Egyesült Királyság) Ltd ügy (2016 EWHC 643 (QB)) 43. pontja.

([55]) Open Rights Group & Anor, R (kérelmére) kontra Secretary of State for the Home Department & Anor ügy, 31. pont.

szükséges. Ez a kivétel vonatkozik az adatvédelmi elvekre (a jogszerűség elvének kivételével), az átláthatósági kötelezettségekre, az érintett jogaira, az adatvédelmi jogsértés bejelentésének kötelezettségére, a nemzetközi adattovábbításra vonatkozó szabályokra, az információügyi biztos egyes feladataira és hatásköreire, valamint a jogorvoslatokra, a felelősségre és a büntetésekre vonatkozó szabályokra, kivéve az Egyesült Királyság általános adatvédelmi rendeletének 83. szakaszában szereplő, a közigazgatási bírság kiszabásának általános feltételeiről szóló rendelkezést és az Egyesült Királyság általános adatvédelmi rendeletének 84. szakaszában szereplő, a büntetésekre vonatkozó rendelkezést. Ezenkívül a 2018. évi adatvédelmi törvény 28. szakasza módosítja a 9. szakasz (1) bekezdésének alkalmazását annak érdekében, hogy lehetővé tegye az Egyesült Királyság általános adatvédelmi rendelete 9. szakaszának (1) bekezdésében szereplő különleges adatok kategóriáinak kezelését, amennyiben az adatkezelést a nemzetbiztonság védelméből vagy védelmi célokra végzik, az érintettek jogainak és szabadságainak megfelelő biztosítékai mellett ([56])

(64) A kivétel csak annyiban alkalmazható, amennyiben a nemzetbiztonság vagy a védelem védelméhez szükséges. Mivel ez vonatkozik a 2018. évi adatvédelmi törvény által előírt egyéb kivételekre is, az adatkezelőnek azt eseti alapon kell megfontolnia és igénybe vennie. Ezenkívül a kivétel minden alkalmazásának meg kell felelnie az emberi jogi normáknak (amelyeket az 1998. évi emberi jogi törvény támaszt alá), amelyek szerint egy demokratikus társadalomban a magánélethez való jog bármilyen zavarásának szükségszerűnek és arányosnak kell lennie ([57]).

(65) A biztos megerősítette a kivétel értelmezését a nemzetbiztonsági és védelmi kivétel alkalmazására vonatkozó részletes útmutató kiadásával, pontosítva, hogy az adatkezelőnek azt eseti alapon kell megfontolnia és igénybe vennie ([58]). Az útmutató hangsúlyozza különösen, hogy „[ez] nem általános mentesség", és annak igénybevételéhez „nem elegendő az, hogy az adatokat nemzetbiztonsági célokból kezelik". Ezzel szemben az erre hivatkozó adatkezelőnek „be kell mutatnia, hogy a nemzetbiztonságra gyakorolt kedvezőtlen hatás valóban fennáll", és az adatkezelőtől szükség szerint elvárható, hogy „bizonyítékot szolgáltasson a biztosnak arról, hogy miért vette igénybe a kivételt". Az útmutató tartalmaz egy ellenőrzőlistát és egy sor példát annak pontosítására, hogy milyen feltételek mellett lehet e kivételre hivatkozni.

(66) Az a tény, hogy az adatokat nemzetbiztonsági vagy védelmi célokból kezelik, önmagában nem elegendő a kivétel alkalmazásához. Az adatkezelőnek figyelembe kell vennie annak a nemzetbiztonságra jelentkező tényleges következményeit, ha be kell tartania az adott adatvédelmi rendelkezést. A kivétel csak azokra az egyedi rendelkezésekre alkalmazható, amelyekről megállapították, hogy kockázatot jelentenek, és azt a lehető legszűkebben kell alkalmazni ([59]).

(67) Ezt a felfogást az Information Tribunal (Információügyi Törvényszék) is megerősítette. ([60]) A Baker kontra Secretary of State ügyben („Baker kontra miniszter ügy") megállapította, hogy jogszerűtlen volt a nemzetbiztonsági kivétel általános kivételként történő alkalmazása a hírszerző ügynökséghez érkezett hozzáférési kérelmek esetében. Ehelyett a kivételt eseti alapon kellett alkalmazni, az egyes kérelmek érdemének figyelembevételével és az egyének magánélet tiszteletben tartásához fűződő jogára figyelemmel ([61]).

([56]) Az Egyesült Királyság hatóságai által szolgáltatott információk szerint, ha az adatkezelés nemzetbiztonsági összefüggésben történik, az adatkezelők általában fokozott biztosítékokat és biztonsági intézkedéseket alkalmaznak az adatkezelésre, tükrözve az adatkezelés különleges jellegét. Hogy mely biztosítékok megfelelőek, az attól függ, hogy milyen kockázatokkal jár az adatkezelés. Ez magában foglalhatja az adatokhoz való hozzáférés korlátozását, így azokhoz csak megfelelő biztonsági engedéllyel rendelkező jogosult személyek férhetnek hozzá, szigorú korlátozások vonatkoznak az adatok megosztására, valamint a tárolási és kezelési eljárások magas szintű biztonságára.

([57]) Lásd még: Guriev kontra Community Safety Development (Egyesült Királyság) Ltd (2016 EWHC 643 (QB)), 45. pont; Lin kontra Commissioner of the Police for the Metropolis ügy (2015 EWHC 2484 (QB)), 80. pont.

([58]) Lásd a biztos nemzetbiztonsági és védelmi kivétel alkalmazására vonatkozó útmutatóját, amely elérhető a következő linken: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/

([59]) Az Egyesült Királyság hatóságainak példája szerint, ha egy gyanúsított terrorista, akivel szemben az MI5 aktívan nyomoz, hozzáférési kérelmet nyújt be a Belügyminisztériumhoz (például azért, mert a Belügyminisztériummal vitát folytat bevándorlási ügyekben), akkor szükséges, hogy az érintettnek ne tárjanak fel az MI5 a Belügyminisztériummal a folyamatban lévő vizsgálatokkal kapcsolatban megosztott minden olyan adatot, amelyek sérthetik a különleges forrásokat, módszereket vagy technikákat és/vagy az egyén által jelentett fenyegetés növekedéséhez vezethetnek. Ilyen körülmények között valószínű, hogy a 26. szakasz szerinti kivétel alkalmazási küszöbe teljesülne, és a nemzetbiztonság védelme érdekében szükséges lenne a kivétel az információk közlése alól. Ha azonban a Belügyminisztérium olyan személyes adatokat is tartott az egyénről, amelyek nem kapcsolódtak az MI5 vizsgálatához, és ezeket az információkat a nemzetbiztonság sérelmének veszélye nélkül is meg lehet adni, a nemzetbiztonsági kivétel nem lenne alkalmazható az információk érintettel való közlésének mérlegelésekor. A biztos jelenleg készít útmutatót arról, hogy az adatkezelők miként közelítsék meg a 26. szakasz szerinti kivétel alkalmazását. Az útmutatót várhatóan 2021. március végén teszik közzé.

([60]) A Törvényszéket azért hozták létre, hogy elbírálja az 1984-es adatvédelmi törvény alapján benyújtott adatvédelmi fellebbezéseket. 2010-ben az Információügyi Törvényszék az Egyesült Királyság bírósági rendszere szerkezetátalakításának részeként a First Tier Tribunal általános szabályozási tanácsának része lett.

([61]) Lásd a Baker kontra Secretary of State for the Home Department ügyet (2001 UKIT NSA2) („Baker kontra miniszter ügy").

2.5.6. *Újságírói, művészeti, tudományos és irodalmi, valamint archiválási és kutatási célból kezelt személyes adatokra vonatkozó korlátozások*

(68) Az Egyesült Királyság általános adatvédelmi rendelete 85. szakaszának (2) bekezdése lehetővé teszi, hogy az újságírói, művészeti, tudományos és irodalmi célból kezelt személyes adatokat kivegyenek az Egyesült Királyság általános adatvédelmi rendeletének számos rendelkezése alól. A 2018. évi adatvédelmi törvény 2. mellékletének 5. része meghatározza az e célból történő adatkezelésre vonatkozó kivételeket. Kivételeket ír elő az adatvédelmi elvek (kivéve az integritás és a titoktartás elvét), az adatkezelés jogalapjai (ideértve a különleges adatok kategóriáit és a büntetőjogi felelősség megállapítására vonatkozó határozatokat stb.), a hozzájárulás feltételei, az átláthatósági kötelezettségek, az érintettek jogai, a személyes adatok megsértésének bejelentési kötelezettsége, az információügyi biztossal a magas kockázatú feldolgozás előtt való konzultáció követelménye, valamint a nemzetközi továbbításra vonatkozó szabályok ([62]) alól. Ebben a tekintetben az Egyesült Királyság általános adatvédelmi rendelete érdemben nem tér el az (EU) 2016/679 rendelettől, amely 85. cikkében lehetőséget biztosít az újságírási vagy akadémiai, művészeti vagy irodalmi célú feldolgozás tekintetében az (EU) 2016/679 rendelet számos követelménye alóli kivételre. A 2018. évi adatvédelmi törvény rendelkezései – nevezetesen a 2. melléklet 5. része – összeegyeztethetőek az Egyesült Királyság általános adatvédelmi rendeletével.

(69) Az Egyesült Királyság általános adatvédelmi rendeletének 85. szakasza alapján végrehajtandó legfontosabb kiegyensúlyozás ahhoz kapcsolódik, hogy a (68) preambulumbekezdésben említett adatvédelmi szabályok alóli kivétel „szükséges-e a személyes adatok védelméhez való jognak és a véleménynyilvánítás és az információ szabadságának egyeztetéséhez” ([63]). A 2018. évi adatvédelmi törvény 2. melléklete 26. szakaszának (2) és (3) bekezdése szerint az Egyesült Királyság az „észszerű meggyőződés” tesztjét alkalmazza ennek az egyensúlynak a megteremtése érdekében. A kivétel indokolásához az adatkezelőnek észszerűen meg kell győződnie arról, hogy i. a közzététel közérdeket szolgál; és ii. a vonatkozó GDPR-rendelkezés alkalmazása összeegyeztethetetlen lenne az újságírói, tudományos, művészeti vagy irodalmi célokkal. Amint azt az ítélkezési gyakorlat megerősítette ([64]), az „észszerű meggyőződés” tesztjének szubjektív és objektív összetevője is van: nem elegendő az adatkezelőnek bizonyítani, hogy ő maga úgy vélte, hogy a megfelelés összeegyeztethetetlen. A meggyőződésének észszerűnek kell lennie, vagyis egy észszerűen eljáró személy által a vonatkozó tények ismeretében hihetőnek kell lennie. Az adatkezelőnek ezért kellő gondossággal kell eljárnia meggyőződésének kialakításakor annak érdekében, hogy bizonyítani tudja az észszerűséget. Az Egyesült Királyság hatóságainak magyarázata szerint az „észszerű meggyőződés” tesztet minden egyes kivételre el kell elvégezni ([65]). Ha a feltételek teljesülnek, az Egyesült Királyság jogszabályai szerint a kivétel szükségesnek és arányosnak tekinthető.

(70) A 2018. évi adatvédelmi törvény 124. szakasza szerint a biztosnak el kell készítenie az adatvédelemről és az újságírásról szóló gyakorlati kódexet. A kódex jelenleg készül. Az 1998. évi adatvédelmi törvény szerinti útmutatót adtak ki erről a kérdésről, amely hangsúlyozza, hogy az e kivételre való hivatkozáshoz nem elegendő annak puszta kijelentése, hogy a megfelelés kényelmetlenséget jelentene az újságírói tevékenység szempontjából, hanem egyértelmű érvnek kell léteznie arra vonatkozóan, hogy a szóban forgó rendelkezés

([62]) Lásd az Egyesült Királyság általános adatvédelmi rendeletének 85. szakaszát és a 2018. évi adatvédelmi törvény 2. mellékletének 5. része 26. szakaszának (9) bekezdését.

([63]) A 2018. évi adatvédelmi törvény 2. melléklete 5. részének 26. pontja (2) bekezdésével összhangban a kivétel a személyes adatok különleges célokra (újságírás, akadémiai, művészeti és irodalmi célokra) történő kezelésére vonatkozik, ha az adatkezelést újságírói, tudományos, művészeti vagy irodalmi anyagok valamely személy általi közzététele céljából végzik, és az adatkezelő megalapozottan úgy véli, hogy az anyag közzététele közérdeket szolgálna. Annak eldöntése során, hogy egy publikáció közérdekű-e, az adatkezelőnek figyelembe kell vennie a közérdekvéleménynyilvánítás és az információszabadság szempontjából fennálló sajátos jelentőségét. Ezenkívül az adatkezelőnek figyelembe kell vennie a szóban forgó kiadvány szempontjából releváns gyakorlati kódexeket vagy irányelveket (a BBC szerkesztési irányelvei, az Ofcom közvetítési kódexe és a szerkesztői gyakorlati kódex). Ezenkívül a kivétel alkalmazásához az adatkezelőnek észszerűen meg kell győződnie arról, hogy a vonatkozó rendelkezés betartása összeegyeztethetetlen lenne a különleges célokkal (a 2018. évi adatvédelmi törvény 2. melléklete 26. pontjának (3) bekezdése).

([64]) Az NT1 kontra Google ügyben hozott ítélet (2018 EWHC 799 (QB)) 102. pontja azzal foglalkozik, hogy az adatkezelő megalapozottan vélte-e úgy, hogy a közlés közérdeket szolgál, és hogy a vonatkozó rendelkezések betartása összeegyeztethetetlen-e a különleges célokkal. A bíróság kimondta, hogy az 1998. évi adatvédelmi törvény 32. szakasza (1) bekezdésének b) és c) pontja szubjektív és objektív elemeket tartalmaz: az adatkezelőnek meg kell állapítania, hogy meggyőződése szerint a közlés közérdeket szolgál, és hogy ez a meggyőződés objektíven észszerű volt; szubjektív meggyőződést kell kialakítania arról, hogy annak a rendelkezésnek a teljesítése, amely alól kivételt kíván alkalmazni, összeegyeztethetetlen lenne a szóban forgó különleges céllal.

([65]) Az „észszerű meggyőződés” teszt alkalmazásának példája szerepel az információügyi biztos True Visions Productions bírságolására vonatkozó határozatában, amelyet az 1998. évi adatvédelmi törvény alapján fogadott el. A biztos elfogadta, hogy a média adatkezelő szubjektíven meggyőződött arról, hogy az első adatvédelmi elv (tisztesség és jogszerűség) betartása összeegyeztethetetlen az újságírói célokkal. A biztos azonban nem fogadta el e meggyőződés objektív észszerűségét. Az információügyi biztos határozata a következő linken érhető el: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf

akadályozza a felelősségteljes újságírást ([66]). A közérdekű teszt alkalmazásáról és a közérdek és az egyén magánélet iránti érdeke közötti egyensúly megteremtéséről az Egyesült Királyság telekommunikációs szabályozója, az OFCOM és a BBC a szerkesztési útmutatóiban is adott ki útmutatást ([67]). Az iránymutatások elsősorban a közérdek szempontjából figyelembe vehető információkra mutatnak be példákat, és elmagyarázzák, hogy bizonyíthatónak kell annak lennie, hogy az eset egyedi körülményei között a közérdek jelentősebb a magánélethez fűződő jogoknál.

(71) A GDPR 89. cikkében előírtakhoz hasonlóan a közérdekű, tudományos vagy történeti kutatási vagy statisztikai célra archiválási célból kezelt személyes adatok is mentesíthetők az Egyesült Királyság általános adatvédelmi rendeletének számos felsorolt rendelkezése alól ([68]). A kutatás és a statisztika tekintetében az Egyesült Királyság általános adatvédelmi rendeletének rendelkezései alól kivételek az alábbiakkal kapcsolatban lehetségesek: az adatkezelés megerősítése, az adatokhoz való hozzáférés és a harmadik országba történő adattovábbítások biztosítékai; helyesbítéshez való jog; az adatkezelés korlátozása és az adatkezelés elleni tiltakozás. Ami a közérdekű archiválást illeti, a személyes adatok helyesbítését vagy törlését, illetve az adatkezelés korlátozását érintő bejelentési kötelezettséget, valamint az adatok hordozhatóságához való jogot érintő kivétel is lehetséges.

(72) A 2018. évi adatvédelmi törvény 2. melléklete 27. szakaszának (1) bekezdése és 28. szakaszának (1) bekezdése szerint az Egyesült Királyság általános adatvédelmi rendelete felsorolt rendelkezései alóli kivételek akkor lehetségesek, ha a rendelkezések alkalmazása „megakadályozná vagy súlyosan hátrányosan érintené a (szóban forgó) célok elérését” ([69]).

(73) Tekintettel azok egyéni jogok hatékony gyakorlása szempontjából fennálló jelentőségére, a fent említett kivételek értelmezésével és gyakorlati alkalmazásával kapcsolatos bármely lényeges fejlemény (a határt átlépő személyforgalom hatékony ellenőrzése (6) preambulumbekezdésben kifejtett fenntartásával kapcsolatos fejlemények mellett), ideértve az ítélkezési gyakorlat, valamint a biztos útmutatásainak és végrehajtási intézkedéseinek további fejlődését, e határozat folyamatos nyomon követése során megfelelően figyelembe veszik ([70]).

2.5.7. *Az újbóli adattovábbítás korlátozása*

(74) Az Európai Unióból az egyesült királyságbeli adatkezelőknek vagy adatfeldolgozóknak továbbított személyes adatok védelmi szintjét nem veszélyeztetheti az említett adatok Egyesült Királyságon kívüli harmadik országokban található adatátvevők részére történő újbóli továbbítása. Az említett „újbóli adattovábbítás”, amely az egyesült királyságbeli adatkezelők vagy adatfeldolgozók szemszögéből Egyesült Királyságból történő nemzetközi adattovábbításnak számít, csak abban az esetben engedélyezett, ha az Egyesült Királyságon kívüli újabb adatátvevőre olyan szabályok vonatkoznak, amelyek biztosítják az Egyesült Királyság jogrendje szerint biztosított védelem szintjéhez hasonló szintű védelmet. Emiatt az Egyesült Királyság általános adatvédelmi rendelete és a 2018. évi adatvédelmi törvény személyes adatok nemzetközi továbbítására vonatkozó szabályainak alkalmazása fontos tényező a védelem folyamatosságának biztosításában az e határozat alapján az Európai Unióból az Egyesült Királyságba továbbított személyes adatok esetében a védelem folyamatosságának biztosításában.

([66]) Az útmutató alapján a szervezeteknek képesnek kell lenniük magyarázatot adni arra, hogy az 1998-as adatvédelmi törvény vonatkozó rendelkezéseinek való megfelelés miért nem egyeztethető össze az újságírás céljaival. Az adatkezelőknek különösen egyensúlyba kell hozniuk a megfelelésnek az újságírásra gyakorolt káros hatását és a megfelelés elmaradásának az érintett jogaira gyakorolt káros hatását. Ha az újságírók észszerűen elérhetik szerkesztési céljaikat oly módon, hogy azok megfeleljenek az adatvédelmi törvény szokásos rendelkezéseinek, azt kell tenniük. A szervezeteknek képesnek kell lenniük arra, hogy igazolják a korlátozás alkalmazását minden olyan rendelkezés vonatkozásában, amelyet nem tartottak be. „Adatvédelem és újságírás: útmutató a média számára”, a következő linken érhető el: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf

([67]) Közérdek például a bűncselekmények feltárása vagy felderítése, a közegészség vagy a biztonság védelme, az egyének vagy szervezetek megtévesztő állításainak leleplezése vagy a lakosságot érintő alkalmatlanság feltárása. Az OFCOM útmutatója a következő linken érhető el: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf és a BBC szerkesztési irányelvei a következő linken érhetők el: https://www.bbc.com/editorialguidelines/guidelines/privacy

([68]) Lásd az Egyesült Királyság általános adatvédelmi rendeletének 89. szakaszát, valamint a 2018. évi adatvédelmi törvény 2. mellékletek 6. része 27. szakaszának (2) bekezdését és 28. szakaszának (2) bekezdését.

([69]) Erre az a követelmény vonatkozik, hogy a személyes adatokat az Egyesült Királyság általános adatvédelmi rendelete 2018. évi adatvédelmi törvény 19. szakaszával kiegészített 89. szakaszának (1) bekezdésével összhangban kell kezelni.

([70]) Lásd a (281)–(287) preambulumbekezdést.

(75) Az Egyesült Királyságból származó személyes adatok nemzetközi továbbításának rendszerét az Egyesült Királyság általános adatvédelmi rendeletének 44–49. szakasza határozza meg, kiegészítve a 2018. évi adatvédelmi törvénnyel, és lényegében az (EU) 2016/679 rendelet V. fejezetében meghatározott szabályokat tükrözi ([71]). A személyes adatok harmadik országba vagy nemzetközi szervezetbe történő továbbítására csak megfelelőségi rendelet alapján kerülhet sor (az (EU) 2016/679 rendelet szerinti megfelelőségi határozat egyesült királyságbeli megfelelője), vagy megfelelőségi rendelet hiányában akkor, ha az adatkezelő vagy az adatfeldolgozó megfelelő biztosítékokat nyújtott az Egyesült Királyság általános adatvédelmi rendeletének 46. szakaszával összhangban. Megfelelőségi rendeletek vagy megfelelő biztosítékok hiányában az adattovábbítás csak az Egyesült Királyság általános adatvédelmi rendelete 49. szakaszában meghatározott eltérések alapján történhet.

(76) A miniszter által elfogadott megfelelőségi rendeletek előírhatják, hogy egy harmadik ország (vagy egy harmadik ország területén belüli terület vagy ágazat), egy nemzetközi szervezet vagy ([72]) az említett ország, terület, szektor, vagy szervezet leírása biztosítja a személyes adatok megfelelő szintű védelmét. A védelmi szint megfelelőségének értékelésekor a miniszternek ugyanazokat az elemeket kell figyelembe vennie, amelyeket a Bizottságnak az (EU) 2016/679 rendelet 45. cikke (2) bekezdésének a)–c) pontja alapján értékelnie kell, az (EU) 2016/679 rendelet (104) preambulumbekezdésével és a megtartott uniós ítélkezési gyakorlattal együtt értelmezve. Ez azt jelenti, hogy egy harmadik ország megfelelő szintű védelmének értékelésekor a vonatkozó mérce az, hogy a szóban forgó harmadik ország biztosítja-e az Egyesült Királyságban garantált védelemmel „lényegében megegyező" védelmi szintet.

(77) Ami az eljárást illeti, a megfelelőségi rendeletekre a 2018. évi adatvédelmi törvény 182. szakaszában előírt „általános" eljárási követelmények vonatkoznak. Ebben az eljárásban a miniszternek konzultálnia kell az információügyi biztossal, amikor javaslatot tesz az Egyesült Királyság megfelelőségi rendeleteinek elfogadására ([73]). Miután a miniszter elfogadta ezeket a rendeleteket, azokat a Parlament elé terjesztik, és a „negatív állásfoglalási" eljárás érvényesül, amelynek során a Parlament mindkét háza megvizsgálhatja a rendeletet, és 40 napos határidőn belül elfogadhat a rendelet megsemmisítésére vonatkozó indítványt ([74]).

(78) A 2018. évi adatvédelmi törvény 17B. szakaszának (1) bekezdése szerint a megfelelőségi rendeletet legfeljebb négyéves időközönként felül kell vizsgálni, a miniszternek pedig folyamatosan figyelemmel kell kísérnie a harmadik országokban és nemzetközi szervezetekben azokat a fejleményeket, amelyek befolyásolhatják a megfelelőségi rendeletek megalkotására, illetve az említett rendeletek módosítására vagy visszavonására vonatkozó döntéseket. Ha a miniszter tudomására jut, hogy egy konkrét ország vagy szervezet már nem biztosítja a személyes adatok megfelelő szintű védelmét, a szükséges mértékben módosítania vagy hatályon kívül kell helyeznie a szabályokat, és konzultációt kell folytatnia a harmadik országgal vagy nemzetközi szervezettel a megfelelő védelem hiányának orvoslása érdekében. Ezek az eljárási szempontok tükrözik az (EU) 2016/679 rendelet megfelelő követelményeit is.

([71]) Az (EU) 2016/679 rendelet 48. cikkének kivételével, amelynek esetében az Egyesült Királyság úgy döntött, hogy nem veszi fel az Egyesült Királyság általános adatvédelmi rendeletébe. E tekintetben először is emlékeztetni kell arra, hogy a megfelelő védelmi szintet biztosítónak tekintendő mérce a „lényegi egyenértékűség", nem pedig az azonosság, ahogyan azt az EUB egyértelművé tette (Schrems I., 73–74. pont) és az Európai Adatvédelmi Testület elismerte (megfelelőségi referencia, 3. oldal). Ezért, amint azt az Európai Adatvédelmi Testület megfelelőségi referenciájában kifejtette, „a cél nem az európai jogszabályok pontról pontra lemásolása, hanem a jogszabályok alapvető – lényegi követelményeinek meghatározása". Ebben a tekintetben fontos megjegyezni, hogy bár az Egyesült Királyság jogrendje formálisan nem tartalmaz a 48. cikkel azonos rendelkezést, ugyanezt a hatást garantálják más jogszabályi rendelkezések és elvek is, azaz hogy harmadik ország bírósága vagy közigazgatási hatósága kérésére személyes adatok csak akkor továbbíthatók ebbe a harmadik országba, ha nemzetközi megállapodás van érvényben – amelynek alapján a harmadik ország szóban forgó bírósági ítéletét vagy közigazgatási határozatát elismerik vagy végrehajtják a Egyesült Királyságban – vagy ha a továbbítás az Egyesült Királyság általános adatvédelmi rendeletének V. fejezetében előírt adattovábbítási mechanizmusok egyikén alapul. Konkrétabban: egy külföldi ítélet végrehajtása érdekében az Egyesült Királyság bíróságainak a „common law"-ra vagy egy olyan törvényre kell hivatkozniuk, amely lehetővé teszi annak végrehajthatóságát. Azonban sem a „common law" (lásd Adams és társai kontra Cape Industries Plc., [1990] 2 W.L.R 657), sem a törvények nem írják elő az adatok továbbítását igénylő külföldi ítéletek nemzetközi megállapodás hiányában történő végrehajtását. Ennek következtében ilyen nemzetközi megállapodás hiányában az adatigénylések az Egyesült Királyság joga szerint nem hajthatók végre. Továbbá a személyes adatok harmadik országba történő továbbítása – ideértve egy külföldi bíróság vagy közigazgatási hatóság kérésére történő továbbítást is – továbbra is az Egyesült Királyság általános adatvédelmi rendeletének V. fejezetében szereplő korlátozások hatálya alá tartozik, amelyek azonosak az (EU) 2016/679 rendelet megfelelő rendelkezéseivel, és ezért azok az V. fejezetben az adattovábbításra előírt valamely jogalapra hivatkozást írják elő, az adott fejezetben arra előírt konkrét feltételeknek megfelelően.

([72]) Az Egyesült Királyság hatóságai kifejtették, hogy egy ország vagy egy nemzetközi szervezet leírása arra a helyzetre utal, amikor a megfelelőség konkrét és részleges meghatározására van szükség, konkrét területre vonatkozó korlátozásokkal (például a megfelelőségi rendelet csak bizonyos típusú adattovábbításokra vonatkozik).

([73]) Lásd: a Digitális, Kulturális, Média- és Sportminisztérium minisztere (DCMS) és az információügyi biztos hivatala közötti egyetértési megállapodást, amely meghatározza a DCMS és a biztos közötti kölcsönösen elfogadott munkamódszereket az Egyesült Királyság jövőbeni megfelelőségértékelései tekintetében, elérhető a következő linken: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([74]) Az említett szavazás esetén a szabályozás további joghatása megszűnik.

(79) Megfelelőségi rendeletek hiányában nemzetközi adattovábbításra akkor kerülhet sor, amennyiben az adatkezelő vagy az adatfeldolgozó megfelelő biztosítékokat nyújtott az Egyesült Királyság általános adatvédelmi rendelete 46. szakaszával összhangban. A biztosítékok hasonlóak a 2016/679/EU rendelet 46. cikkében említettekhez. Ide tartoznak a hatóságok vagy szervek között jogilag kötelező érvényű és végrehajtható eszközök, kötelező érvényű vállalati szabályok ([75]), egységes adatvédelmi feltételek, jóváhagyott magatartási kódexek, jóváhagyott tanúsítási mechanizmusok és az információügyi biztos engedélyével az adatkezelők (vagy adatfeldolgozók) közötti szerződései feltételek vagy a hatóságok közötti igazgatási megállapodások. A szabályokat azonban eljárási szempontból úgy módosították, hogy az Egyesült Királyság keretén belül működjenek, különösen a 2018. évi adatvédelmi törvény szerint a miniszter (17C. szakasz) vagy az információügyi biztos (119A. szakasz) fogadhat el általános adatvédelmi záradékokat.

(80) Megfelelőségi rendelet vagy megfelelő biztosítékok hiányában az adattovábbításra csak az Egyesült Királyság általános adatvédelmi rendeletének 49. szakaszában ([76]) meghatározott eltérések alapján történhet. Az Egyesült Királyság általános adatvédelmi rendelete nem vezet be lényeges változásokat az eltérések terén az (EU) 2016/679 rendelet megfelelő szabályaihoz képest. Az Egyesült Királyság általános adatvédelmi rendeletében – az (EU) 2016/679 rendelethez hasonlóan – bizonyos eltérésekre csak akkor lehet támaszkodni, ha az adattovábbítás alkalmi jellegű ([77]). Ezenkívül a biztos a nemzetközi adattovábbításokra vonatkozó útmutatójában pontosítja, hogy: „Ezeket csak valódi »kivételként« használja az általános szabály alól, amely szerint csak akkor hajtható végre korlátozott adattovábbítás, ha arra megfelelőségi határozat vonatkozik vagy vannak megfelelő biztosítékok" ([78]). A fontos közérdekből (49. cikk (1) bekezdés d) pont) szükséges adattovábbítások tekintetében a miniszter rendeleteket hozhat annak meghatározása érdekében, hogy a személyes adatok harmadik országba vagy nemzetközi szervezetnek történő továbbítása fontos közérdekből szükséges/nem szükséges. Ezenkívül a miniszter rendeletekkel korlátozhatja a személyes adatok valamely kategóriájának harmadik országba vagy nemzetközi szervezetnek történő továbbítását, amennyiben az adattovábbítás a megfelelőségi rendeletek alapján nem történhet meg, és a miniszter fontos közérdekű ok miatt szükségesnek tartja a korlátozást. Ilyen rendeletet eddig nem fogadtak el.

(81) Ez a nemzetközi adattovábbítási keretrendszer az átmeneti időszak végén vált alkalmazhatóvá ([79]). Ugyanakkor a 2018. évi adatvédelmi törvény 21. mellékletének (a kilépéssel kapcsolatos adatvédelmi szabályozás által bevezetett) (4) pontja előírja, hogy az átmeneti időszak végétől kezdve a személyes adatok bizonyos továbbítását úgy kezelik, mintha azok megfelelőségi rendeleteken alapulnának. Ezek az adattovábbítások magukban foglalják az EGT-államokba, Gibraltár területére, az EU-Szerződés által vagy annak alapján létrehozott uniós intézménynek, szervnek, hivatalnak vagy ügynökségnek történő adattovábbításokat, valamint az olyan harmadik országokba történő adattovábbításokat, amelyekre uniós megfelelőségi határozat vonatkozott az átmeneti időszak végén. Következésképpen az ezekbe az országokba irányuló adattovábbítások ugyanúgy folytatódhatnak, mint az Egyesült Királyság EU-ból való kilépése előtt. Az

([75]) Az Egyesült Királyság általános adatvédelmi rendelete megtartja az (EU) 2016/679 rendelet 47. cikkében szereplő szabályokat, és csak a szabályok hazai kontextusba illesztése érdekében szükséges módosításokat hajtja végre, például az illetékes felügyeleti hatóságra utaló hivatkozások információügyi biztosra történő hivatkozásokkal felváltásával, az (1) bekezdésből az egységességi mechanizmusra való hivatkozás törlésével és az egész (3) bekezdés elhagyásával.

([76]) Az Egyesült Királyság általános adatvédelmi rendeletének 49. szakasza értelmében az adattovábbítás akkor lehetséges, ha az alábbi feltételek valamelyike teljesül: a) az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról; b) az adattovábbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges; c) az adattovábbítás az adatkezelő és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges; d) az adattovábbítás fontos közérdekből szükséges; e) az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges; f) az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására; g) a továbbítást olyan nyilvántartásból végzik, amely a hazai jognak megfelelően a nyilvánosság tájékoztatását szolgálja, és amely általában a nyilvánosság számára, vagy bármely, jogos érdekét igazoló személy számára betekintés céljából rendelkezésre áll, de csak olyan mértékben, amilyenben a hazai jog által a betekintésre megállapított feltételek az adott esetben teljesülnek. Ezenkívül, ha a fenti feltételek egyike sem alkalmazható, az adattovábbítás csak akkor történhet meg, ha az nem ismétlődő, csak korlátozott számú érintettet érint, és ez az adatkezelő által érvényesített kényszerítő jogos érdekek érdekében szükséges, amelyeknél az érintett érdekei vagy jogai és szabadságai nem jelentősebbek, és az adatkezelő értékelte az adattovábbítással kapcsolatos összes körülményt, és ezen értékelés alapján megfelelő biztosítékokat nyújtott a személyes adatok védelme tekintetében.

([77]) Az Egyesült Királyság általános adatvédelmi rendeletének (111) preambulumbekezdése meghatározza, hogy a szerződéssel vagy a jogi követeléssel kapcsolatos adattovábbításokra csak akkor kerülhet sor, ha azok alkalmi jellegűek.

([78]) Az információügyi biztos nemzetközi adattovábbításról szóló útmutatója elérhető a következő linken: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7

([79]) Ezen új keret alkalmazhatóságát a legkésőbb 2021. június 30-ig tartó hat hónapos időszak alatt az egyrészről az Európai Unió és az Európai Atomenergia-közösség, és másrészről Nagy-Britannia és Észak-Írország Egyesült Királysága közötti kereskedelmi és együttműködési megállapodás (az EU és az Egyesült Királyság közötti kereskedelmi és együttműködési megállapodás) (HL L 444, 2020.12.31., 14. o.) 782. cikkére figyelemmel kell értelmezni, amely az alábbi linken érhető el: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:22020A1231(01)

átmeneti időszak lejárta után a miniszternek négy éven belül, azaz 2024. december végéig felül kell vizsgálnia ezeket a megfelelőségi megállapításokat. Az Egyesült Királyság hatóságainak magyarázata szerint, bár a miniszternek 2024 december végéig el kell végeznie egy ilyen felülvizsgálatot, az átmeneti rendelkezések nem tartalmaznak „megszüntetési" rendelkezést, és a vonatkozó átmeneti rendelkezések hatálya nem szűnik meg automatikusan, ha a felülvizsgálat 2024. december végéig nem fejeződik be.

(82) Végül az Egyesült Királyság nemzetközi adattovábbítási rendszerének jövőbeli – új megfelelőségi rendeletek elfogadásával, nemzetközi megállapodások megkötésével vagy más adattovábbítási mechanizmusok kifejlesztésével történő – alakulását illetően a Bizottság szorosan figyelemmel kíséri a helyzetet, felméri, hogy a különböző adattovábbítási mechanizmusokat olyan módon használják-e, amely biztosítja a védelem folytonosságát, és szükség esetén megteszi a megfelelő intézkedéseket az említett folytonosság lehetséges káros hatásainak kezelésére (lásd a (278) – (287)preambulumbekezdést). Mivel az EU és az Egyesült Királyság szabályai hasonlóak a nemzetközi adattovábbításokkal kapcsolatban, várhatóan a problémás eltéréseket is el lehet kerülni együttműködéssel, információcserével és tapasztalatcserével, többek között a biztos és az Európai Adatvédelmi Testület között.

2.5.8. *Elszámoltathatóság*

(83) Az elszámoltathatóság elve értelmében az adatkezelőknek megfelelő technikai és szervezeti intézkedéseket kell hozniuk, hogy hatékonyan feleljenek meg adatvédelmi kötelezettségeiknek, és bizonyítani tudják ezt a megfelelést, különösen az illetékes felügyeleti hatóság felé.

(84) Az (EU) 2016/679 rendeletben előírt elszámoltathatóság elvét az Egyesült Királyság általános adatvédelmi rendelete 5. szakaszának (2) bekezdése lényeges változás nélkül megtartotta, és ugyanez vonatkozik az adatkezelő felelősségéről szóló 24. cikkre, a beépített adatvédelemről szóló 25. cikkre, valamint az adatkezelési tevékenységek nyilvántartásáról szóló 30. cikkre. Az adatvédelmi hatásvizsgálatokról és a felügyeleti hatósággal folytatott előzetes konzultációról szóló 35. és 36. cikket szintén megtartották. Az (EU) 2016/679 rendeletnek az adatvédelmi tisztviselők kijelöléséről és feladatairól szóló 37–39. cikkét az Egyesült Királyság általános adatvédelmi rendeletében lényeges változások nélkül megtartották. Továbbá megtartották az (EU) 2016/679 rendelet magatartási kódexekről és tanúsításról szóló 40. és 42. cikkének rendelkezéseit az Egyesült Királyság általános adatvédelmi rendeletében ([80]).

2.6. **Felügyelet és végrehajtás**

2.6.1. *Független felügyelet*

(85) Az adatvédelem megfelelő szintjének gyakorlati biztosítása érdekében létre kell hozni egy független felügyeleti hatóságot, amely hatáskörrel rendelkezik az adatvédelmi szabályoknak való megfelelés nyomon követésére és a nyomon követés érvényesítésére. Ennek a hatóságnak teljes egészében függetlenül és pártatlanul kell eljárnia feladatai ellátása és hatásköre gyakorlása során.

(86) Az Egyesült Királyság általános adatvédelmi rendeletének és a 2018. évi adatvédelmi törvénynek való megfelelés felügyeletét és kikényszerítését az Egyesült Királyságban az információügyi biztos végzi. Az információügyi biztos „Corporation Sole": egyetlen személyben megtestesülő önálló jogi személy. Az információügyi biztos munkáját egy hivatal támogatja. Az Információs Biztos Hivatalának 2020. március 31-én 768 állandó munkavállalója volt ([81]). Az információügyi biztos támogató minisztériuma a Digitális, Kulturális, Média- és Sportminisztérium ([82]).

(87) A biztos függetlenségét kifejezetten rögzíti az Egyesült Királyság általános adatvédelmi rendeletének 52. szakasza, amely nem tér el érdemben a GDPR rendelet 52. cikkének (1)–(3) bekezdésétől. A biztosnak teljesen függetlenül kell eljárnia feladatainak ellátása és hatásköreinek az Egyesült Királyság általános adatvédelmi rendeletével összhangban

([80]) Szükség esetén ezeket a hivatkozásokat az Egyesült Királyság hatóságaira történő hivatkozásokkal helyettesítik. Például a 2018. évi adatvédelmi törvény 17. szakasza szerint a tanúsítás betartásának figyelemmel kísérésére az információügyi biztos vagy az Egyesült Királyság nemzeti akkreditáló testülete akkreditálhat egy olyan személyt, aki megfelel az Egyesült Királyság általános adatvédelmi rendelete 43. szakaszában meghatározott követelményeknek.

([81]) Az információügyi biztos 2019–2020-es éves beszámolója és pénzügyi kimutatásai az alábbi linken érhetők el: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf

([82]) Egy ügyviteli megállapodás szabályozza a kettő kapcsolatát. Különösen a DCMS, mint támogató minisztérium fő feladatai közé tartoznak a következők: az információügyi biztos megfelelő finanszírozásának és forrásainak biztosítása; az információügyi biztos érdekeinek képviselete a Parlament és más kormányzati szervek előtt; szilárd nemzeti adatvédelmi keret biztosítása; valamint útmutatás és támogatás nyújtása a biztosnak olyan szervezeti kérdésekben, mint az ingatlanügyletek, a bérleti szerződések és a beszerzések (a 2018–2021-es ügyviteli megállapodás a következő linken érhető el: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

történő gyakorlása során, mentesnek kell maradnia bármiféle közvetlen vagy közvetett külső befolyástól e feladatok és hatáskörök tekintetében, és senkitől nem kérhet és nem fogadhat el utasításokat. A biztosnak tartózkodnia kell minden olyan feladattól is, amely összeegyeztethetetlen a feladataival, és hivatali idejében nem folytathat összeegyeztethetetlen foglalkozást, legyen az fizetett vagy önkéntes munka.

(88) Az információügyi biztos kinevezésének és visszahívásának feltételeit a 2018. évi adatvédelmi törvény 12. melléklete tartalmazza. Az információügyi biztost a királynő nevezi ki a kormány ajánlása alapján, tisztességes és nyílt verseny alapján. A jelöltnek rendelkeznie kell a megfelelő képesítéssel, készségekkel és kompetenciákkal. A Governance Code on Public Appointments (állami kinevezések irányítása kódexe) elnevezésű dokumentummal összhangban ([83]) a kinevezhető jelöltek listáját egy tanácsadó értékelő testület állítja össze. Mielőtt a Digitális, Kulturális, Média- és Sportminisztérium minisztere véglegesíti döntését, az illetékes parlamenti válogató bizottságnak kinevezés előtti ellenőrzést kell lefolytatnia. A bizottság álláspontját nyilvánosságra hozzák ([84]).

(89) Az információügyi biztos hivatali ideje legfeljebb hét év. Egy személyt nem lehet több alkalommal információügyi biztosnak kinevezni. Őfelsége a Parlament mindkét házának beszédét követően felmentheti hivatalából ([85]). Az információügyi biztos felmentésére vonatkozó kérelem nem terjeszthető be a Parlament egyik házához sem, ha egy miniszter nem terjesztett elő jelentést, amelyben kijelenti, hogy meg van győződve arról, hogy az információügyi biztos súlyos kötelességszegésben vétkes és/vagy a biztos már nem felel meg a biztos feladatainak ellátásához szükséges feltételeknek ([86]).

(90) Az információügyi biztos finanszírozása három forrásból származik: i. az adatkezelők által fizetett adatvédelmi díjak, amelyeket a miniszter rendeletei határoznak meg ([87]) (a Data Protection (Charges and Information) Regulations 2018 elnevezésű (2018. évi adatvédelmi (díjak és információk) szabályozás), és a Hivatal éves költségvetésének 85–90 %-át teszi ki ([88]); ii. a kormány által az információügyi biztos részére kifizetett támogatás. A támogatást elsősorban az információügyi biztos adatvédelemhez nem kapcsolódó feladatai tekintetében felmerülő működési költségeinek finanszírozására fordítják ([89]); és iii. a szolgáltatásokért felszámított díjak ([90]). Jelenleg ilyen díjakat nem számítanak fel.

(91) Az információügyi biztos az Egyesült Királyság általános adatvédelmi rendelete körébe tartozó személyes adatok kezelésével kapcsolatos általános feladatait az Egyesült Királyság általános adatvédelmi rendeletének 57. szakasza határozza meg, szorosan tükrözve az (EU) 2016/679 rendelet megfelelő szabályait. Feladatai közé tartozik az Egyesült Királyság általános adatvédelmi rendeletének nyomon követése és végrehajtása, a közvélemény tudatosságának elősegítése, az érintettek által benyújtott panaszok kezelése, vizsgálatok lefolytatása stb. Ezenkívül a 2018. évi adatvédelmi törvény 115. szakasza meghatározza a biztos egyéb általános feladatait, amelyek magukban foglalják a Parlament, a kormány és más intézmények és szervek számára a tanácsadás kötelezettségét az egyének jogainak és szabadságainak a személyes adatok kezelése tekintetében történő védelmével kapcsolatos törvényi és közigazgatási intézkedésekről, valamint arra vonatkozó hatáskör, hogy a biztos saját kezdeményezésére

([83]) Governance Code on Public Appointments, elérhető a következő linken: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf

([84]) Az alsóház kulturális, média- és sportbizottsága 2015–2016-os ülésszakának második jelentése, az alábbi linken érhető el: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf

([85]) A „beszéd” a Parlament elé terjesztett indítvány, amelynek célja, hogy az uralkodót megismertesse a Parlament véleményével egy adott kérdésben.

([86]) A 2018. évi adatvédelmi törvény 12. melléklete 3. pontjának (3) bekezdése.

([87]) Lásd a 2018. évi adatvédelmi törvény 137. szakaszát, lásd a (17) preambulumbekezdést.

([88]) A 2018. évi adatvédelmi törvény 137. és 138. szakasza számos biztosítékot tartalmaz annak biztosítására, hogy a díjakat megfelelő szinten állapítsák meg. Különösen, a 137. szakasz (4) bekezdése felsorolja azokat a kérdéseket, amelyekre a miniszternek tekintettel kell lennie, amikor a különböző szervezetek által fizetendő összeget meghatározó rendeleteket elfogadja. Másodszor, a 2018. évi adatvédelmi törvény 138. szakaszának (1) bekezdése és 182. cikke szintén előírja, hogy a miniszternek konzultálnia kell az információügyi biztossal és a rendeletek által valószínűleg érintett személyek más képviselőivel, a rendeletek elfogadása előtt, hogy véleményüket figyelembe lehessen venni. Ezenkívül a 2018. évi adatvédelmi törvény 138. szakaszának (2) bekezdése értelmében az információügyi biztos köteles felülvizsgálni a díjakról szóló rendeletek működését, és javaslatokat nyújthat be a miniszterhez a rendeletek módosítására. Végül a rendeletekre „pozitív állásfoglalási” eljárás vonatkozik – kivéve azokat az eseteket, amikor a rendelet pusztán a kiskereskedelmi árindex növekedésének figyelembevétele érdekében készül (ebben az esetben a „negatív állásfoglalási” eljárás irányadó) –, és csak akkor fogadhatók el, ha a Parlament mindegyik háza azokat határozattal jóváhagyta.

([89]) Az ügyviteli megállapodás egyértelművé teszi, hogy „a miniszter az információügyi biztosnak teljesíthet kifizetéseket a Parlament által a 2018. évi adatvédelmi törvény 12. mellékletének 9. pontja alapján biztosított forrásokból. Az információügyi biztossal folytatott konzultációt követően a DCMS kifizeti (támogatásként átadja) a megfelelő összegeket az információügyi biztosnak a biztos igazgatási költségeire és a biztos számos konkrét feladatkörével kapcsolatos funkcióinak gyakorlásáért, ideértve az információszabadságot is (a 2018–2021-es ügyviteli megállapodás, 1.12. pont, lásd a 82. lábjegyzetet).

([90]) Lásd a 2018. évi adatvédelmi törvény 134. szakaszát.

vagy kérésre véleményt adjon a Parlamentnek, a kormánynak vagy más intézményeknek és szerveknek, valamint a lakosságnak a személyes adatok védelmével kapcsolatos bármely kérdésben. Az igazságszolgáltatás függetlenségének fenntartása érdekében az információügyi biztos nem jogosult feladatait a személyes adatok bírói minőségben eljáró egyén, vagy bírósági minőségében eljáró bíróság vagy törvényszék általi kezelésével kapcsolatban ellátni. Az igazságszolgáltatás felügyeletét szakosított testületek biztosítják (lásd a (99)–(103) preambulumbekezdést.

2.6.2. *Jogérvényesítés, ezen belül a jogsértés megszüntetésére irányuló eljárások*

(92) Az információügyi biztos hatáskörét az Egyesült Királyság általános adatvédelmi rendeletének 58. szakasza rögzíti, amely nem vezet be lényeges változásokat az (EU) 2016/679 rendelet megfelelő cikkéhez képest. A 2018. évi adatvédelmi törvény kiegészítő szabályokat határoz meg e hatáskörök gyakorlásának módjáról. A biztos hatáskörrel rendelkezik különösen az alábbiakra: a) az adatkezelő és az adatfeldolgozó (és bizonyos körülmények között bármely más személy) számára a szükséges információk megadásának elrendelése tájékoztatás kérésével („adatkérési felhívás") ([91]); b) vizsgálat és ellenőrzés végzése vizsgálati felhívás útján, amelyben elrendelheti az adatkezelő vagy az adatfeldolgozó számára, hogy engedélyezze a biztos számára a belépést meghatározott helyiségekbe, dokumentumok vagy berendezések megtekintését vagy vizsgálatát, a személyes adatokat az adatkezelő nevében feldolgozó emberek kihallgatását („vizsgálati felhívás") ([92]); c) egyébként hozzáférés az adatkezelők és az adatfeldolgozók dokumentumaihoz, valamint belépés helyiségeikbe a 2018. évi adatvédelmi törvény 154. szakaszának („belépési és ellenőrzési jogkör") megfelelően; d) korrekciós hatáskör gyakorlása, többek között jogérvényesítési felhívás útján figyelmeztetések és megrovások, vagy utasítás adása révén, amelyben megköveteli az adatkezelőktől/adatfeldolgozóktól az Egyesült Királyság általános adatvédelmi rendeletének 58. szakasza (2) bekezdésének c), g) és j) pontjában írt bármely intézkedés megtételét vagy azoktól tartózkodást („jogérvényesítési felhívás") ([93]); e) bírságértesítő formájában közigazgatási bírságot szab ki („bírságértesítő") ([94]). Ez utóbbit akkor is ki lehet adni, ha egy hatóság nem tartotta be az Egyesült Királyság általános adatvédelmi rendeletében foglalt rendelkezéseket ([95]).

(93) A biztos szabályozási cselekvési politikája meghatározza azokat a körülményeket, amelyek mellett a biztos adatkérési, vizsgálati, jogérvényesítési felhívást és bírságértesítőt fog kiadni ([96]). Az adatkezelő vagy az adatfeldolgozó mulasztására adott jogérvényesítési felhívás csak olyan követelményeket támaszthat, amelyeket a biztos a mulasztás orvoslása érdekében megfelelőnek tart. Végrehajtási felhívásokat és bírságértesítőket az adatkezelőnek vagy az adatfeldolgozónak az Egyesült Királyság általános adatvédelmi rendelete II. fejezetének (az adatkezelés elvei), a 12–22. szakaszának (az érintett jogai), a 25–39. szakaszának (az adatkezelők és az adatkezelők kötelezettségei) és az Egyesült Királyság általános adatvédelmi rendeletének 44–49. szakasza (nemzetközi adattovábbítások) megsértésével kapcsolatban lehet kiadni. Jogérvényesítési felhívás akkor is kiadható, ha az adatkezelő nem teljesítette a 2018. évi adatvédelmi törvény 137. szakasza alapján elfogadott rendeletben előírt díjfizetési követelményt. Ezenkívül a 41. cikk szerinti ellenőrző szerv vagy egy tanúsító szolgáltató akkor kaphat jogérvényesítési felhívást, ha nem teljesíti az Egyesült Királyság általános adatvédelmi rendeletéből eredő kötelezettségeit. Bírságértesítő olyan személynek adható, aki nem tett eleget adatkérési, vizsgálati vagy jogérvényesítési felhívásnak.

(94) A bírságértesítő előírja a személynek, hogy az értesítésben meghatározott összeget fizesse meg az információügyi biztosnak. Annak eldöntésekor, hogy küldjön-e valakinek bírságértesítőt, és a büntetés összegének meghatározásakor az információügyi biztosnak figyelembe kell vennie az Egyesült Királyság általános adatvédelmi rendelete 83. szakaszának (1) és (2) bekezdésében felsorolt kérdéseket, amelyek megegyeznek az (EU) 2016/679 rendelet megfelelő szabályaival ([97]). A 83. szakasz (4) és (5) bekezdése szerint az e rendelkezésekben említett

([91]) A 2018. évi adatvédelmi törvény 142. szakasza (a 2018. évi adatvédelmi törvény 143. szakaszában foglalt korlátozásokra figyelemmel).

([92]) A 2018. évi adatvédelmi törvény 146. szakasza (a 2018. évi adatvédelmi törvény 147. szakaszában foglalt korlátozásokra figyelemmel).

([93]) A 2018. évi adatvédelmi törvény 149–151. szakasza (a 2018. évi adatvédelmi törvény 152. szakaszában foglalt korlátozásokra figyelemmel).

([94]) A 2018. évi adatvédelmi törvény 155. szakasza és az Egyesült Királyság általános adatvédelmi rendeletének 83. szakasza.

([95]) Ez következik a 2018. évi adatvédelmi törvény 155. szakaszának (1) bekezdéséből, a 2018. évi adatvédelmi törvény 149. szakaszának (2) és (5) bekezdésével együttes olvasatban, valamint a 2018. évi adatvédelmi törvény 156. szakaszának (4) bekezdéséből, amely csak a bírságértesítők kiadását korlátozza a Crown Estate (állami vagyonkezelő) biztosai és a királyi háztartás ellenőrei tekintetében a 2018. évi adatvédelmi törvény 209. szakaszának (4) bekezdése alapján.

([96]) Szabályozási cselekvési politika, elérhető a következő linken: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

([97]) Beleértve a jogsértés jellegét és súlyosságát (figyelembe véve az érintett adatkezelés jellegét, terjedelmét és célját, valamint az érintettek számát és az általuk elszenvedett kár mértékét), a jogsértés szándékos vagy gondatlan jellegét, az adatkezelő által az érintettek által elszenvedett kár enyhítése érdekében esetlegesen tett lépések, az adatkezelő vagy az adatfeldolgozó felelősségének mértéke (figyelembe véve az adatkezelő vagy az adatfeldolgozó által végrehajtott technikai és szervezési intézkedéseket), az adatkezelő vagy az adatfeldolgozó bármely korábbi releváns jogsértése; a biztossal való együttműködés mértéke, a mulasztás által érintett személyes adatok kategóriái, az eset körülményeire alkalmazható egyéb súlyosító vagy enyhítő tényezők, például a jogsértésből közvetlenül vagy közvetetten elért pénzügyi előnyök vagy elkerült veszteségek.

kötelezettségek elmulasztása esetén az adminisztratív bírságok maximális összege 8 700 000 GBP, illetve 17 500 000 GBP. Vállalkozás esetében az információügyi biztos a világszintű éves árbevétel százalékában is kiszabhatja a bírságokat, ha az magasabb. Az (EU) 2016/679 rendelet megfelelő rendelkezéseihez hasonlóan ezeket az összegeket a 83. cikk (4) bekezdésében 2 %-ban, illetve (5) bekezdésében 4 %-ban határozták meg. Az adatkérési, vizsgálati vagy jogérvényesítési felhívás be nem tartásával kapcsolatban a bírságértesítővel kiszabható büntetés maximális összege 17 500 000 GBP, vagy vállalkozás esetében a világszintű éves árbevétel 4 %-a.

(95) Az Egyesült Királyság általános adatvédelmi rendelete és a 2018. évi adatvédelmi törvény együttesen megerősítette az információügyi biztos egyéb hatásköreit is. Például a biztos most kötelező ellenőrzéseket hajthat végre valamennyi adatkezelő és adatfeldolgozó vonatkozásában vizsgálati felhívások használata révén, míg a korábbi jogszabályok, az 1998. évi adatvédelmi törvény értelmében a biztosnak csak a központi kormányzat és az egészségügyi szervezetek vonatkozásában volt ilyen hatásköre, másoknak bele kellett egyezniük az ellenőrzésbe.

(96) Az (EU) 2016/679 rendelet bevezetése óta a biztos évente mintegy 40 000, az érintettektől érkező panaszt intéz ([98]) és ezenfelül körülbelül 2 000 hivatalból indított vizsgálatot ([99]) folytat le. A panaszok többsége az adatokhoz való hozzáférés jogával és az adatok közlésével kapcsolatos. Vizsgálatait követően a biztos végrehajtási intézkedéseket hoz ágazatok széles körében. Pontosabban, az információügyi biztos legújabb éves jelentése (2019–2020) szerint ([100]) a biztos 54 jelentést, 8 értékelő közleményt, 7 végrehajtási közleményt, 4 figyelmeztetést adott ki, 8 büntető feljelentést tett és 15 bírságot szabott ki a beszámolási időszak alatt ([101]).

(97) Ennek része az (EU) 2016/679 rendelet és a 2018. évi adatvédelmi törvény alapján kiszabott számos jelentős pénzbüntetés. Az információügyi biztos különösen 2020 októberében 20 millió GBP összegre bírságolt egy brit légitársaságot, egy több mint 400 000 ügyfelet érintő személyesadat-sértés miatt. 2020 októberének végén egy nemzetközi szállodaláncot 18,4 millió GBP összegre büntettek, mivel nem tartotta biztonságban ügyfelek millióinak személyes adatait, 2020 novemberében pedig egy jegyeket online értékesítő brit rendezvényszervező szolgáltatót 1,25 millió GBP összegre büntetett meg az ügyfelek fizetési adatai védelmének elmaradása miatt. ([102])

(98) Az információügyi biztosnak a (92) preambulumbekezdésben leírt végrehajtási hatáskörein túl az adatvédelmi jogszabályok bizonyos megsértései bűncselekménynek minősülnek, ezért büntetőjogi szankciókkal sújthatók (a 2018. évi adatvédelmi törvény 196. szakasza). Ez vonatkozik például a személyes adatok adatkezelő hozzájárulása nélkül szándékos vagy gondatlan gyűjtésére vagy közlésére, a személyes adatok más személlyel közlésére az adatkezelő hozzájárulása nélkül ([103]), az anonimizált személyes adatok újbóli azonosítása a személyes adatok anonimizálásáért felelős adatkezelő hozzájárulása nélkül ([104]), a biztos személyes adatok nemzetközi kötelezettségekkel összhangban történő ellenőrzésével kapcsolatos hatásköre gyakorlásának szándékos akadályozása ([105]), hamis állítások megtétele egy adatkérési felhívásra, vagy információk megsemmisítése az adatkérési és vizsgálati felhívások kapcsán ([106]).

([98]) Az Egyesült Királyság hatóságai által szolgáltatott információk szerint az információügyi biztos 2019–2020-as éves jelentése által lefedett időszakban az esetek körülbelül 25 %-ában nem találtak jogsértést, az esetek körülbelül 29 %-ában az érintettet felkérték, hogy az aggályt először az adatkezelőnél vesse fel, az adatkezelő válaszát várja be vagy folytassa az adatkezelővel folyamatban lévő párbeszédet, az esetek körülbelül 17 %-ában nem találtak jogsértést, de tanácsot adtak az adatkezelőnek, az esetek körülbelül 25 %-ában az információügyi biztos jogsértést állapított meg, vagy az adatkezelőnek tanácsot adott, illetve az adatkezelőnek bizonyos intézkedéseket kellett tennie, az esetek körülbelül 3 %-ában megállapították, hogy a panasz nem tartozik az (EU) 2016/679 rendelet hatálya alá, és az esetek körülbelül 1 %-át az Európai Adatvédelmi Testület keretében egy másik adatvédelmi hatósághoz utalták.

([99]) A biztos különféle forrásokból kapott információk alapján kezdeményezheti ezeket a vizsgálatokat, ideértve a személyes adatok megsértésével kapcsolatos értesítéseket, az Egyesült Királyság más hatóságaitól vagy külföldi adatvédelmi hatóságoktól érkezett felkéréseket, valamint az egyének vagy a civil társadalmi szervezetek panaszait.

([100]) Az információügyi biztos 2019–2020-as éves jelentése és pénzügyi kimutatásai (lásd a 81. lábjegyzetet).

([101]) Az előző, 2018 és 2019 közötti időszakra vonatkozó éves jelentés szerint az információügyi biztos a beszámolási időszak alatt 22 bírságértesítőt adott ki az 1998. évi adatvédelmi törvény alapján, összesen 3 010 610 GBP bírságra, köztük két 500 000 GBP bírsággal (az 1998. évi adatvédelmi törvény szerint megengedett legmagasabb összeg). 2018-ban az információügyi biztos különösen a Cambridge Analytica leleplezéseit követően folytatott vizsgálatot az adatelemzés politikai célokra történő felhasználása miatt. A vizsgálat eredménye szakpolitikai jelentés, ajánláscsomag, 500 000 GBP bírság kirovása a Facebookra, valamint jogérvényesítési felhívás kiküldése az Aggregate IQ kanadai adatközvetítőnek, és a vállalat kötelezése arra, hogy törölje az Egyesült Királyság állampolgárairól és lakóiról tartott személyes adatokat (lásd: az információügyi biztos 2018–2019-es éves jelentése és pénzügyi kimutatása a következő linken érhető el https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf).

([102]) A megtett végrehajtási intézkedések összefoglalását lásd a biztos webhelyén, amely a következő linken érhető el: https://ico.org.uk/action-weve-taken/enforcement/

([103]) A 2018. évi adatvédelmi törvény 170. szakasza.

([104]) A 2018. évi adatvédelmi törvény 171. szakasza.

([105]) A 2018. évi adatvédelmi törvény 119. szakasza.

([106]) A 2018. évi adatvédelmi törvény 144. és 148. szakasza.

2.6.3. *Az igazságszolgáltatás felügyelete*

(99) A személyes adatok bíróságok és igazságszolgáltatás általi kezelésének felügyelete kettős. Ha egy igazságügyi tisztségviselő vagy bíróság nem bírói minőségben jár el, a felügyeletet az információügyi biztos látja el. Amennyiben az adatkezelő bírói minőségben jár el, a biztos nem gyakorolhatja felügyeleti funkcióit ([107]) és a felügyeletet speciális szervek végzik. Ez az (EU) 2016/679 rendeletben alkalmazott megközelítést (55. cikk (3) bekezdés) tükrözi.

(100) A második esetkörben az angliai és walesi bíróságok, valamint az angliai és walesi első és felsőbb bíróságok esetében az említett felügyeletet konkrétan a bírói adatvédelmi testület biztosítja ([108]). Ezenkívül a Lord Chief Justice és a Senior President of Tribunals adatkezelési tájékoztatót adott ki ([109]) amely meghatározza, hogy az angliai és walesi bíróságok miként kezelik a személyes adatokat bírósági funkciók ellátása céljából. Hasonló nyilatkozatot adott ki az északír ([110]) és a skót bírói kar is ([111]).

(101) Sőt, Észak-Írországban az északír Lord Chief Justice kinevezett egy legfelsőbb bírósági bírót adatvédelmi felügyelő bírónak (Data Supervisory Judge – DSJ) ([112]). Ugyancsak útmutatót adtak ki az északír bírói karnak arról, hogy mit kell tenniük adatok elvesztése vagy potenciális elvesztése esetén, valamint az ebből adódó kérdések kezelésének folyamatáról ([113]).

(102) Skóciában a Lord President nevezett ki egy adatvédelmi felügyelő bírót az adatvédelmi alapon tett esetleges panaszok kivizsgálására. Ezt a bírósági panaszokra vonatkozó szabályok rögzítik, amelyek az Anglia és Wales vonatkozásában megállapított szabályokat tükrözik ([114]).

(103) Végül a Legfelsőbb Bíróságon az egyik legfelsőbb bírósági bírót nevezik ki az adatvédelem felügyeletére.

2.6.4. *Jogorvoslat*

(104) A megfelelő védelem biztosítása és különösen a személyhez fűződő jogok érvényesítésének biztosítása érdekében az érintettet hatékony közigazgatási és bírósági jogorvoslatban kell részesíteni, beleértve a kártérítést.

([107]) A 2018. évi adatvédelmi törvény 117. szakasza.

([108]) A testület feladata a bírói kar számára útmutatás és képzés nyújtása. Foglalkozik továbbá az érintettektől a személyes adatok bíróságok, törvényszékek és bírósági minőségben eljáró egyének általi feldolgozása kapcsán érkező panaszokkal. A testület célja, hogy eszközt biztosítson az esetleges panaszok megoldására. Ha egy panaszos nem elégedett a testület döntésével, és további bizonyítékokat szolgáltat, a testület felülvizsgálhatja határozatát. Noha a testület maga nem szab ki pénzügyi szankciókat, ha a testület úgy ítéli meg, hogy a 2018. évi adatvédelmi törvény kellően súlyos sérelme történt, a panaszt a Bírói Magatartást Vizsgáló Hivatalhoz (JCIO) utalhatja, amely azt kivizsgálja. Ha a panaszt helybenhagyják, a Lord Chancellor és a Lord Chief Justice (vagy a nevében eljáró vezető bíró) feladata annak eldöntése, hogy milyen intézkedést hozzanak a tisztségviselővel szemben. Ez súlyosság szerinti sorrendben az alábbi lehet: hivatalos tanácsadás, hivatalos figyelmeztetés és megrovás, végső soron hivatalból való felmentés. Ha egy személy elégedetlen azzal, ahogyan a JCIO kivizsgálta a panaszt, további panaszt tehet a bírói kinevezésekkel és magatartással foglalkozó ombudsmannál (lásd https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Az ombudsman hatáskörrel rendelkezik arra, hogy felkérje a JCIO-t a panasz újbóli kivizsgálására, és javaslatot tehet a panaszos részére kártérítés fizetésére, amennyiben úgy véli, hogy hivatali visszásság miatt kárt szenvedett.

([109]) A Lord Chief Justice és a Senior President of Tribunals adatkezelési tájékoztatója a következő linken érhető el: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([110]) Az észak-írországi Lord Chief Justice által kiadott adatkezelési tájékoztató a következő linken érhető el: https://judiciaryni.uk/data-privacy

([111]) A skót bíróságok adatkezelési tájékoztatója a következő linken érhető el: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([112]) A DSJ útmutatást nyújt a bírói kar számára, és kivizsgálja a személyes adatok bíróságok vagy bírói minőségben eljáró egyének általi kezelésével kapcsolatos jogsértéseket és/vagy panaszokat.

([113]) Amennyiben a panasz vagy a jogsértés súlyosnak minősül, azt továbbítják az igazságügyi panaszügyi tisztviselőhöz további vizsgálat céljából, az észak-írországi Lord Chief Justice panaszokkal kapcsolatos gyakorlati kódexének megfelelően. Az említett panasz kimenetele lehet: további intézkedés mellőzése, tanácsadás, képzés vagy mentorálás, informális figyelmeztetés, hivatalos figyelmeztetés, utolsó figyelmeztetés, a gyakorlat korlátozása vagy a törvényszék elé utalás. Az észak-írországi Lord Chief Justice panaszokkal kapcsolatos gyakorlati kódexe a következő linken érhető el:hhttps://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]) Az adatvédelmi felügyelő bíró minden megalapozott panaszt kivizsgál, és a Lord Presidenthez továbbítja, aki jogosult tanácsot, hivatalos figyelmeztetést vagy megrovást kiadni, ha szükségesnek ítéli (a bíróság tagjaira egyenértékű szabályok léteznek, amelyek a következő linken érhetőek el: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

(105) Először is, az érintettnek joga van panaszt benyújtani az információügyi biztoshoz, ha úgy ítéli meg, hogy a rá vonatkozó személyes adatokkal kapcsolatban megszegték az Egyesült Királyság általános adatvédelmi rendeletét ([115]). Az Egyesült Királyság általános adatvédelmi rendelete lényeges módosítások nélkül fenntartja az e jogra vonatkozó, az (EU) 2016/679 rendelet 77. cikkében szereplő szabályokat. Ugyanez vonatkozik az 57. cikk (1) bekezdésének f) pontjára és (2) bekezdésére, amelyek meghatározzák a biztos panaszok kezelésével kapcsolatos feladatait. A (92)–(98) above preambulumbekezdésben leírtak szerint az információügyi biztos hatáskörrel rendelkezik annak értékelésére, hogy az adatkezelő és az adatfeldolgozó megfelel-e az Egyesült Királyság általános adatvédelmi rendeletének és a 2018. évi adatvédelmi törvénynek, megkövetelheti tőlük, hogy tegyék meg a szükséges lépéseket, vagy tartózkodjanak azoktól meg nem felelés esetén és bírságot szab ki.

(106) Másodszor, az Egyesült Királyság általános adatvédelmi rendelete és a 2018. évi adatvédelmi törvény jogot biztosít az információügyi biztos elleni jogorvoslatra. Az Egyesült Királyság általános adatvédelmi rendelete 78. szakaszának (1) bekezdése értelmében az egyénnek joga van hatékony bírósági jogorvoslathoz a biztos rá vonatkozó, jogilag kötelező érvényű határozatával szemben. A bírósági felülvizsgálat keretében a bíró megvizsgálja a keresetben megtámadott döntést, és megvizsgálja, hogy az információügyi biztos jogszerűen járt-e el. Ezenkívül az Egyesült Királyság általános adatvédelmi rendelete 78. szakaszának (2) bekezdése szerint, ha a biztos nem kezeli megfelelően az érintett panaszát, ([116]) a panaszos bírósági jogorvoslatot vehet igénybe. A First Tier Tribunal előtt kérheti a biztos arra kötelezését, hogy tegye meg a megfelelő lépéseket a panasz elintézésére, vagy tájékoztassa a panaszost a panasz állásáról ([117]). Ezenkívül bárki, aki a biztostól a fenti bármelyik felhívást (adatkérési, vizsgálati, jogérvényesítési felhívás vagy bírságértesítő) megkapja, fellebbezést nyújthat be a First Tier Tribunalhoz ([118]). Ha ez a bíróság úgy ítéli meg, hogy a biztos döntése nincs összhangban a jogszabályokkal, vagy az információügyi biztosnak másként kellett volna gyakorolnia mérlegelési jogkörét, akkor engedélyeznie kell a fellebbezést, vagy olyan másik felhívást vagy határozatot kell elfogadnia, amelyet az információügyi biztos elfogadhatott volna.

(107) Harmadszor: az egyének az adatkezelőkkel és az adatfeldolgozókkal szemben közvetlenül a bírósághoz fordulva is bírósági jogorvoslatot nyerhetnek az Egyesült Királyság általános adatvédelmi rendelete 79. szakasza és a 2018. évi adatvédelmi törvény 167. szakasza alapján. Ha az érintett kérelmére a bíróság meggyőződik arról, hogy megsértették az érintett adatvédelmi jogszabályok szerinti jogait, a bíróság kötelezheti az adatkezelésben érintett adatkezelőt, vagy az adatkezelő nevében eljáró adatfeldolgozót a kötelezésben maghatározott intézkedések megtételére, vagy az abban meghatározott lépésektől való tartózkodásra.

(108) Ezenkívül az Egyesült Királyság általános adatvédelmi rendeletének 82. szakasza és a 2018. évi adatvédelmi törvény 168. szakasza alapján minden olyan személynek, aki az Egyesült Királyság általános adatvédelmi rendeletének megsértése miatt anyagi vagy nem vagyoni kárt szenvedjen, joga van arra, hogy az adatkezelőtől vagy az adatfeldolgozótól az elszenvedett kárért kártérítést kapjon. Az Egyesült Királyság általános adatvédelmi rendelete 82. szakaszának (1)–(5) bekezdésében szereplő, a kártérítésre és a felelősségre vonatkozó szabályok megegyeznek az (EU) 2016/679 rendelet megfelelő szabályaival. A 2018. évi adatvédelmi törvény 168. szakasza szerint a nem vagyoni károk magukban foglalják a sérelemdíjat is. Az Egyesült Királyság általános adatvédelmi rendeletének 80. szakasza alapján az érintettnek joga van egy érdekképviseleti testületet vagy szervezetet is meghatalmazni a panasz biztoshoz történő benyújtására (az Egyesült Királyság általános adatvédelmi rendeletének 77. szakasza alapján) és az Egyesült Királyság általános adatvédelmi rendelete 78. szakaszában (a biztos elleni hatékony bírósági jogorvoslat), 79. szakaszában (az adatkezelővel vagy az adatfeldolgozóval szembeni hatékony bírósági jogorvoslat joga) és 82. szakaszában (a kártérítéshez és helytállási kötelezettséghez való jog) említett jogok képviseletében történő gyakorlására.

(109) Negyedszer, és a fentebb ismertetett jogorvoslati lehetőségek mellett, amennyiben bárki úgy ítéli meg, hogy a hatóságok megsértették jogait, beleértve a magánélethez és az adatvédelemhez fűződő jogokat, az 1998. évi emberi jogi törvény alapján jogorvoslatot kaphat az Egyesült Királyság bíróságai előtt ([119]). Az a személy, aki azt állítja, hogy egy hatóság olyan módon járt el (vagy olyan eljárást javasol), amely összeegyeztethetetlen az egyezmény szerinti joggal, következésképpen az 1998. évi emberi jogi törvény 6. szakaszának (1) bekezdése alapján jogellenes, eljárást indíthat a hatóság ellen a megfelelő bíróság vagy törvényszék előtt, vagy bármely bírósági eljárásban hivatkozhat az érintett jogokra, amennyiben a jogellenes cselekmény áldozata (vagy az lenne).

(110) Ha a bíróság valamely hatóság valamely cselekményét jogellenesnek találja, hatáskörein belül olyan kártérítést vagy jogorvoslatot adhat, illetve határozatot hozhat, amelyet igazságosnak és megfelelőnek tart ([120]). A bíróság összeegyeztethetetlennek nyilváníthatja az elsődleges jogszabályok valamely rendelkezését az Egyezmény által biztosított jogokkal is.

([115]) Az Egyesült Királyság általános adatvédelmi rendeletének 77. szakasza.

([116]) A 2018. évi adatvédelmi törvény 166. szakasza konkrétan az alábbi helyzetekre utal: a) a biztos nem tesz megfelelő intézkedéseket a panasz megválaszolására, b) a biztos nem ad a panaszosnak tájékoztatást a panasz állásáról vagy kimeneteléről a panasz biztos általi kézhezvételétől számított 3 hónapos időszak végéig, vagy c) ha a panasz biztos általi vizsgálata ebben az időszakban nem fejeződik be, a következő három hónapos időszak alatt nem ad tájékoztatást erről a panaszosnak.

([117]) Az Egyesült Királyság általános adatvédelmi rendelete 78. szakaszának (2) bekezdése és a 2018. évi adatvédelmi törvény 166. szakasza.

([118]) Az Egyesült Királyság általános adatvédelmi rendelete 78. szakaszának (1) bekezdése és a 2018. évi adatvédelmi törvény 162. szakasza.

([119]) Az 1998. évi emberi jogi törvény 7. szakaszának (1) bekezdése. A 7. szakasz (7) bekezdése szerint egy személy csak akkor válik jogellenes cselekmény áldozatává, ha az Emberi Jogok Európai Egyezményének 34. cikke értelmében áldozatnak minősülne, ha az Emberi Jogok Európai Bíróságán eljárás indulna az adott intézkedés miatt.

([120]) Az 1998. évi emberi jogi törvény 8. szakaszának (1) bekezdése.

(111) Végül, a nemzeti jogorvoslatok kimerülése után az egyén az Emberi Jogok Európai Bíróságánál kérhet jogorvoslatot az emberi jogok európai egyezménye által biztosított jogok megsértése miatt.

3. AZ EURÓPAI UNIÓBÓL TOVÁBBÍTOTT SZEMÉLYES ADATOKHOZ VALÓ HOZZÁFÉRÉS ÉS AZ ILYEN ADATOK FELHASZNÁLÁSA AZ EGYESÜLT KIRÁLYSÁG HATÓSÁGAI ÁLTAL

(112) A Bizottság emellett értékelte az Egyesült Királyság jogi kereteit az Egyesült Királyság hatóságai által közérdekből – különösen büntetőjogi és nemzetbiztonsági célokból – az Egyesült Királyság gazdasági szereplői számára az Egyesült Királyságban továbbított személyes adatok gyűjtésére és későbbi felhasználására (a továbbiakban: mint „kormányzati hozzáférés") vonatkozóan. Annak értékelése során, hogy azok a feltételek, amelyek mellett az e határozat alapján az Egyesült Királyságba továbbított adatokhoz való kormányzati hozzáférés megfelel-e az (EU) 2016/679 rendelet 45. cikkének (1) bekezdése szerinti „lényegi egyenértékűségi" teszten, az Európai Unió Bíróságának az Alapjogi Chartára figyelemmel adott értelmezése szerint a Bizottság különösen a következő kritériumokat vette figyelembe.

(113) Először is, a személyes adatok védelméhez való jog gyakorlása csak a törvény által korlátozható, és a beavatkozást lehetővé tevő jogalapnak magának kell meghatároznia az érintett jog gyakorlásával kapcsolatos korlátozás terjedelmét ([121]).

(114) Másodszor, az arányosság követelményének való megfelelés érdekében, amely szerint egy demokratikus társadalomban a személyes adatok védelme alóli eltéréseknek és e védelem korlátozásainak a feltétlenül szükséges mérték határain belül kell maradniuk az Unió által elismert elismertekkel egyenértékű általános érdekű célok teljesítéséhez, az érintett harmadik ország beavatkozást lehetővé tevő jogszabályainak egyértelmű és pontos szabályokat kell meghatározniuk a szóban forgó intézkedések alkalmazási körét és alkalmazását illetően, és elő kell írniuk minimumbiztosítékokat annak érdekében, hogy azok a személyek, akiknek az adatait továbbították, elegendő garanciákkal rendelkezzenek, amelyek lehetővé teszik a személyes adataiknak a visszaélések veszélyeivel szembeni hatékony védelmét ([122]). A jogszabályoknak meg kell jelölniük különösen, hogy milyen körülmények között és milyen feltételek mellett lehet az ilyen adatok kezelését előíró intézkedést megtenni ([123]), valamint az említett követelmények teljesítését független felügyeletnek kell alávetni ([124]).

(115) Harmadszor, ennek a jogszabálynak a nemzeti jog szerint jogilag kötelezőnek kell lennie, és ezeknek a jogi követelményeknek nemcsak a hatóságokra nézve kell kötelezőnek lenniük, hanem a szóban forgó harmadik ország hatóságaival szemben bíróság előtt is végrehajthatónak ([125]). Az érintetteknek különösen rendelkezniük kell azzal a lehetőséggel, hogy független és pártatlan bíróság előtt éljenek jogorvoslati lehetőségekkel abból a célból, hogy a rájuk vonatkozó személyes adatokhoz hozzáférést kapjanak, vagy az ilyen adatokat helyesbíttetni vagy töröltetni tudják ([126]).

3.1. **Általános jogi keret**

(116) A kormányzati hozzáférést a hatóság hatáskörének gyakorlásaként az Egyesült Királyságban a törvények teljes tiszteletben tartásával kell végezni. Az Egyesült Királyság ratifikálta az emberi jogok európai egyezményét (lásd a (9) preambulumbekezdést) és az Egyesült Királyság összes hatóságának az egyezménynek megfelelően kell eljárnia ([127]). Az egyezmény 8. cikke előírja, hogy a magánéletbe való bármiféle beavatkozásnak összhangban kell állnia a jogszabályokkal, a 8. cikk (2) bekezdésében meghatározott célok valamelyikének érdekében, és e célra figyelemmel arányosnak kell lennie. A 8. cikk azt is előírja, hogy a beavatkozásnak „előreláthatónak" kell lennie, vagyis egyértelmű, hozzáférhető jogalapjának kell lennie, és hogy a törvénynek megfelelő biztosítékokat kell tartalmaznia a visszaélések megelőzésére.

(117) Emellett az Emberi Jogok Európai Bírósága ítélkezési gyakorlatában meghatározta, hogy a magánélethez és az adatvédelemhez való jogba való bármiféle beavatkozásra hatékony, független és pártatlan felügyeleti rendszernek kell vonatkoznia, amelyet bírónak, bíróságnak vagy más független testületnek ([128]) (pl. közigazgatási hatóságnak vagy parlamenti szervnek) kell biztosítania.

([121]) Lásd a Schrems II. ügy 174–175. pontját és a hivatkozott ítélkezési gyakorlatot. Lásd még a tagállami hatóságok hozzáférését illetően: a C-623/17. sz. Privacy International ügy, ECLI:EU:C:2020:790, 65. pont; és a C-511/18., a C-512/18. és a C-520/18. sz., La Quadrature du Net és társai egyesített ügyekben hozott ítélet, ECLI:EU:C:2020:791, 175. pont.

([122]) Lásd a Schrems II. ügy 176. és 181. pontját, valamint az ott hivatkozott ítélkezési gyakorlatot. Lásd még a tagállami hatóságok hozzáférését illetően: Privacy International ügy, 68. pont; és a La Quadrature du Net és társai ügy, 132. pont.

([123]) Lásd: Schrems II. ügy, 176. pont. Lásd még a tagállami hatóságok hozzáférését illetően: Privacy International ügy, 68. pont; és a La Quadrature du Net és társai ügy, 132. pont.

([124]) Lásd: Schrems II. ügy, 179. pont.

([125]) Lásd a Schrems II. ügy 181–182. pontját.

([126]) Lásd a Schrems I. ügy 95. pontját és a Schrems II. ügy 194. pontját. E tekintetben az EUB hangsúlyozta, hogy az Alapjogi Charta 47. cikkének való megfelelés, amely garantálja a független és pártatlan bíróság előtti, hatékony jogorvoslathoz való jogot, „szintén része az Unión belül megkövetelt védelmi szintnek, és amelynek tiszteletben tartását a Bizottságnak meg kell állapítania, mielőtt az (EU) 2016/679 rendelet 45. cikkének (1) bekezdése alapján megfelelőségi határozatot fogadna el" (Schrems II. ügy, 186. pont).

([127]) Az 1998. évi emberi jogi törvény 6. szakasza.

([128]) Emberi Jogok Európai Bírósága, Klass és társai kontra Németország, kérelem sz. 5029/71, 17–51. pont.

(118) Ezenkívül az egyének számára hatékony jogorvoslatot kell biztosítani, és az Emberi Jogok Európai Bírósága pontosította, hogy a jogorvoslatot egy olyan független és pártatlan testületnek kell nyújtania, amely elfogadta saját eljárási szabályzatát, tagjai hivatalban lévő vagy volt magas rangú bírák vagy tapasztalt ügyvédek, és a kérelem benyújtásához bizonyítási teher teljesítése nem írható elő. A magánszemélyek panaszainak vizsgálata során a független és pártatlan testület részére hozzáférést kell biztosítani minden lényeges információhoz, ideértve a zárt anyagokat is. Végül hatáskörrel kell rendelkeznie a meg nem felelés orvoslására ([129]).

(119) Az Egyesült Királyság 2018-ban ratifikálta Európa Tanács az egyéneknek a személyes adatok gépi feldolgozása során való védelméről szóló egyezményét (108. egyezmény), és az egyéneknek a személyes adatok gépi feldolgozása során való védelméről szóló egyezményt módosító jegyzőkönyvet (az úgynevezett 108+ egyezményt) ([130]). A 108. egyezmény 9. cikke előírja, hogy az Egyezmény általános adatvédelmi elveitől (5. cikk Az adatok minősége), különleges adatokra vonatkozó szabályoktól (6. cikk Különleges adatok) és az érintettek jogaitól (8. cikk Az adatalanyt védő további garanciák) rendelkezéseitől való eltérés csak akkor megengedett, ha erről az adott Fél törvénye rendelkezik, és a szükséges intézkedések egy demokratikus társadalomban az állam biztonsága, a közbiztonság, az állam pénzügyi érdekének a védelme vagy a bűncselekmények megelőzése érdekében, vagy az adatalany vagy mások jogainak vagy szabadságjogainak védelme érdekében szükségesek ([131]).

(120) Ezért az Egyesült Királyságra számos, a nemzetközi jogban rögzített kötelezettség vonatkozik az Európa Tanácsban fennálló tagsága, az Emberi Jogok Európai Egyezményéhez való csatlakozása és az Emberi Jogok Európai Bírósága joghatóságának való alávetése révén, amelyek az uniós jog által garantált és a tagállamokra alkalmazandó elvekhez, biztosítékokhoz és egyéni jogokhoz hasonlóan foglalják keretbe a kormányzati hozzáférési rendszerét. Amint azt a (19) preambulumbekezdés hangsúlyozta, az említett eszközök folyamatos betartása ezért különösen fontos eleme az e határozat alapjául szolgáló értékelésnek.

(121) Ezenkívül a konkrét adatvédelmi biztosítékokat és jogokat a 2018. évi adatvédelmi törvény garantálja, amikor az adatokat hatóságok, többek között a bűnüldöző szervek és a nemzetbiztonsági szervek is kezelik.

(122) A személyes adatok bűnüldözéssel összefüggésben történő kezelésének rendjét különösen a 2018. évi adatvédelmi törvény 3. része határozza meg, amelyet az (EU) 2016/680 irányelv átültetésére fogadtak el. A 2018. évi adatvédelmi törvény 3. része a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása – többek között a közbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése – céljából végzett kezelésére vonatkozik ([132]).

(123) Az „illetékes hatóság” az adatvédelmi törvény 30. szakaszának fogalommeghatározása szerint a 2018. évi adatvédelmi törvény 7. mellékletében felsorolt személy, valamint bármely más személy, amennyiben bármely bűnüldözési célból jogszabályi feladatai vannak ([133]). Amint az alábbiakban kifejtésre került (lásd a (139) preambulumbekezdést), bizonyos illetékes hatóságok (például a Nemzeti Bűnügyi Ügynökség) bizonyos feltételek mellett igénybe vehetik a nyomozati hatáskörökről szóló 2016. évi törvény (a nyomozati hatáskörökről szóló 2016. évi törvény) által biztosított hatásköröket. Ebben az esetben a 2018. évi adatvédelmi törvény 3. részében előírt biztosítékok mellett érvényesülnek a nyomozati hatáskörökről szóló 2016. évi törvényben előírt biztosítékok is. A hírszerző ügynökségek (Secret Intelligence Service – titkosszolgálat, Security Service – biztonsági szolgálat és a Government Communications Headquarters – kormányzati kommunikációs központ) nem a 2018. évi adatvédelmi törvény 3. részének hatálya alá tartozó „illetékes hatóságok” ([134]), és ezért az ott előírt szabályok egyetlen tevékenységükre sem vonatkoznak. A 2018. évi adatvédelmi törvényben egy külön (a 4.) részt szenteltek személyes adatok hírszerző ügynökségek általi kezelésének (részletesebben lásd a (125) preambulumbekezdést).

([129]) Emberi Jogok Európai Bírósága, Kennedy kontra Egyesült Királyság, kérelem sz. 26839/05 („Kennedy-ügy”), 167. és 190. pont.

([130]) Az emberi jogok európai egyezményéről és annak az Egyesült Királyság jogába az 1998. évi emberi jogi törvény révén történő beépítéséről, valamint a 108. egyezményről lásd a (9) preambulumbekezdést.

([131]) Hasonlóképpen, a 108+ egyezmény 11. cikke értelmében az egyezmény egyes sajátos jogainak és kötelezettségeinek korlátozása nemzetbiztonsági vagy bűncselekmények megelőzése, kivizsgálása és büntetőeljárás alá vonása, valamint büntetőjogi szankciók végrehajtása csak akkor megengedett, ha az említett korlátozást törvény írja elő, tiszteletben tartja az alapvető jogok és szabadságok lényegét, és egy demokratikus társadalomban szükséges és arányos intézkedést jelent. A nemzetbiztonsági és védelmi célú feldolgozási tevékenységekre szintén független és hatékony felülvizsgálatnak és felügyeletnek kell vonatkoznia az egyezmény részes felének nemzeti jogszabályai alapján.

([132]) A 2018. évi adatvédelmi törvény 31. szakasza.

([133]) A 7. mellékletben felsorolt illetékes hatóságok nemcsak a rendőrséget, hanem az egész Egyesült Királyság minisztériumi kormányzati szerveit, valamint egyéb nyomozati feladatokkal rendelkező hatóságokat (pl. Commissioner for Her Majesty's Revenue and Customs – Őfelsége Adó- és Vámügyi Biztosa, a Nemzeti Bűnügyi Ügynökség, a Welsh Revenue Authority – a walesi adóhatóság, a Competition and Markets Authority – Verseny- és Piacfelügyelet vagy Her Majesty's Land Register – Őfelsége Ingatlannyilvántartása), ügyészségi szerveket, más büntető igazságszolgáltatási szerveket és egyéb bűnüldözési tevékenységet folytató személyeket vagy szervezeteket is magukban foglalják (ezek között a 2018. évi adatvédelmi törvény 7. melléklete felsorolja az ügyészségi igazgatókat, az északírországi ügyészség igazgatóját vagy az Információügyi Bizottságot).

([134]) A 2018. évi adatvédelmi törvény 30. szakaszának (2) bekezdése.

(124) Az (EU) 2016/680 irányelvhez hasonlóan a 2018. évi adatvédelmi törvény 3. része meghatározza a jogszerűség és a tisztességesség ([135]), a célhoz kötöttség ([136]), az adattakarékossága ([137]), a pontosság ([138]), a tárolási korlátozás ([139]) és a biztonság ([140]) elvét. A jogszabály külön átláthatósági kötelezettségeket ír elő ([141]) és hozzáférési ([142]), helyesbítési és törlési ([143]) jogot biztosít az egyének számára, valamint azt a jogot, hogy ne hozzanak róluk automatizált döntéseket ([144]). Az illetékes hatóságok kötelesek továbbá megvalósítani a tervezett és beépített adatvédelmet, nyilvántartást vezetni az adatkezelési tevékenységekről, egyes adatkezelési műveletek esetében pedig adatvédelmi hatásvizsgálatokat kell végezniük, és előzetesen konzultálniuk kell az információügyi biztossal ([145]). A 2018. évi adatvédelmi törvény 56. szakasza szerint a megfelelést bizonyítaniuk kell. Ezenkívül megfelelő intézkedéseket kell bevezetniük az adatkezelés biztonságának biztosítása érdekében ([146]) és külön kötelezettségek vonatkoznak rájuk a személyes adatok megsértése esetén, ideértve az említett jogsértések az információügyi biztosnak való bejelentését és az érintettek tájékoztatását ([147]). Ahogyan az (EU) 2016/680 irányelvben szerepel, az adatkezelőre is előírás az adatvédelmi tisztviselő kijelölése (kivéve, ha az adatkezelő bíróság vagy más bírói minőségben eljáró igazságügyi hatóság) ([148]), aki segíti az adatkezelőt kötelezettségei teljesítésében, valamint a megfelelés figyelemmel kísérésében ([149]). Ezenkívül a jogszabályok külön követelményeket írnak elő a személyes adatok bűnüldözési célú, harmadik országoknak vagy nemzetközi szervezeteknek történő nemzetközi továbbítására a védelem folyamatosságának biztosítása érdekében ([150]). E határozattal egy időben a Bizottság az (EU) 2016/680 irányelv 36. cikkének (3) bekezdése alapján megfelelőségi határozatot fogad el, amelyben megállapította, hogy az Egyesült Királyság bűnüldöző hatóságai általi adatkezelésre alkalmazandó adatvédelmi rendszer biztosítja az (EU) 2016/680 irányelv által garantálttal lényegében azonos szintű védelmet.

(125) A 2018. évi adatvédelmi törvény 4. része a hírszerző ügynökség által vagy nevében végzett minden adatkezelésre vonatkozik, meghatározza különösen a fő adatvédelmi elveket (jogszerűség, tisztességesség és átláthatóság ([151]); célhoz kötöttség ([152]); adattakarékosság ([153]); pontosság ([154]); tárolás korlátozása ([155]) és biztonság ([156])), feltételeket szab a különleges adatok kategóriáinak kezelésére ([157]), rendelkezik az érintettek jogairól ([158]), megköveteli a

([135]) A 2018. évi adatvédelmi törvény 35. szakasza.
([136]) A 2018. évi adatvédelmi törvény 36. szakasza.
([137]) A 2018. évi adatvédelmi törvény 37. szakasza.
([138]) A 2018. évi adatvédelmi törvény 38. szakasza.
([139]) A 2018. évi adatvédelmi törvény 39. szakasza.
([140]) A 2018. évi adatvédelmi törvény 40. szakasza.
([141]) A 2018. évi adatvédelmi törvény 44. szakasza.
([142]) A 2018. évi adatvédelmi törvény 45. szakasza.
([143]) A 2018. évi adatvédelmi törvény 46. és 47. szakasza.
([144]) A 2018. évi adatvédelmi törvény 49. és 50. szakasza.
([145]) A 2018. évi adatvédelmi törvény 56–65. szakasza.
([146]) A 2018. évi adatvédelmi törvény 66. szakasza.
([147]) A 2018. évi adatvédelmi törvény 67–68. szakasza.
([148]) A 2018. évi adatvédelmi törvény 69-71. szakasza.
([149]) A 2018. évi adatvédelmi törvény 67–68. szakasza.
([150]) A 2018. évi adatvédelmi törvény 3. részének 5. fejezete.
([151]) A 2018. évi adatvédelmi törvény 86. szakaszának (6) bekezdése értelmében az adatkezelés tisztességességének és átláthatóságának meghatározása érdekében figyelembe kell venni az adatok gyűjtésének módját. Ebben az értelemben a méltányosság és az átláthatóság követelménye akkor teljesül, ha az adatokat olyan személytől szerzik be, aki az adatszolgáltatásra jogszerűen felhatalmazott vagy köteles.
([152]) A 2018. évi adatvédelmi törvény 87. szakasza szerint az adatkezelés céljait meg kell határozni, azoknak egyértelműnek és jogszerűnek kell lenniük. Az adatokat tilos olyan módon kezelni, amely összeegyeztethetetlen azokkal a célokkal, amelyekre azokat gyűjtik. A 2018. évi adatvédelmi törvény 87. szakaszának (3) bekezdése értelmében a személyes adatok összeegyeztethető további kezelése csak akkor engedélyezhető, ha az adatkezelőt törvény hatalmazza fel az adatok e célból történő kezelésére, és az adatkezelés szükséges és arányos e másik célra. Az adatkezelést összeegyeztethetőnek kell tekinteni, ha az adatkezelés közérdekű, tudományos vagy történelmi kutatási vagy statisztikai célú archiválási célú feldolgozásból áll, és megfelelő biztosítékok vonatkoznak arra (a 2018. évi adatvédelmi törvény 87. szakaszának (4) bekezdése).
([153]) A személyes adatoknak megfelelőnek, relevánsnak és nem eltúlzott mértékűnek kell lenniük (a 2018. évi adatvédelmi törvény 88. szakasza).
([154]) A személyes adatoknak pontosnak és naprakésznek kell lenniük (a 2018. évi adatvédelmi törvény 89. szakasza).
([155]) A személyes adatokat tilos a szükségesnél tovább tárolni (a 2018. évi adatvédelmi törvény 90. szakasza).
([156]) A hatodik adatvédelmi elv az, hogy a személyes adatokat olyan módon kell kezelni, amely magában foglalja a személyes adatok kezeléséből eredő kockázatokkal kapcsolatos megfelelő biztonsági intézkedések meghozatalát. A kockázatok közé tartozik (a teljesség igénye nélkül) a személyes adatokhoz véletlenszerű vagy illetéktelenek általi hozzáférés, illetve azok megsemmisítése, elvesztése, felhasználása, módosítása vagy közlése (a 2018. évi adatvédelmi törvény 91. szakasza). A 107. szakasz előírja továbbá, hogy (1) minden adatkezelőnek be kell vezetnie a személyes adatok kezeléséből eredő kockázatoknak megfelelő biztonsági intézkedéseket, és (2) automatizált feldolgozás esetén minden adatkezelő és minden adatfeldolgozó a kockázat értékelése alapján megelőző vagy enyhítő intézkedéseket hajt végre.
([157]) A 2018. évi adatvédelmi törvény 86. szakasza (2) bekezdésének b) pontja és 10. melléklete.
([158]) A 2018. évi adatvédelmi törvény 4. részének 3. fejezete, nevezetesen az alábbiakra vonatkozó jogok: hozzáférés, helyesbítés és törlés, tiltakozás az adatkezelés ellen, és az automatizált döntéshozatal elutasítása, beavatkozás az automatizált döntéshozatalba és tájékoztatás a döntéshozatalról. Ezenkívül az adatkezelőnek tájékoztatást kell adnia az érintettnek személyes adatainak kezeléséről. A biztos titkosszolgálatok általi adatkezelésről szóló útmutatójában kifejtettek szerint az egyének minden jogukat (ideértve a helyesbítés iránti kérelmet is) gyakorolhatják, ha panaszt tesznek a biztosnak vagy bíróság elé viszik az ügyet (lásd: a biztos hírszerző szolgálatok általi adatkezelésről szóló útmutatóját, elérhető a következő linken: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

beépített adatvédelmet ([159]) és szabályozza a személyes adatok nemzetközi továbbítását ([160]). A biztos nemrégiben adott ki részletes útmutatást a hírszerző ügynökségek által a 2018. évi adatvédelmi törvény 4. része alapján történő adatkezelésről ([161]).

(126) Ugyanakkor a 2018. évi adatvédelmi törvény 110. szakasza kivételt ír elő a 2018. évi adatvédelmi törvény 4. részének meghatározott rendelkezései alól ([162]), amennyiben az említett kivételre a nemzetbiztonság megőrzése érdekében van szükség. Ezt a kivételt eseti elemzés alapján lehet igénybe venni ([163]). Amint azt az Egyesült Királyság hatóságai kifejtették és az ítélkezési gyakorlat megerősítette, „a) az adatkezelőnek mérlegelnie kell a nemzetbiztonságra vagy a védelemre gyakorolt tényleges következményeket, ha be kellene tartaniuk az adott adatvédelmi rendelkezést, és ha észszerűen eleget tudnak tenni a szokásos szabálynak a nemzetbiztonság vagy a védelem befolyásolása nélkül" ([164]). Az, hogy a kivételt megfelelően alkalmazzák-e, a biztos felügyelete alá tartozik ([165]).

(127) Ezenkívül a fent meghatározott rendelkezések alkalmazásának a „nemzetbiztonság" védelme érdekében történő korlátozásának lehetősége kapcsán az adatkezelő kérhet a 2018. évi adatvédelmi törvény 111. szakasza szerint a miniszter vagy a legfőbb ügyész (vagy a skóciai főügyész) által aláírt tanúsítványt, amely tanúsítja, hogy az említett jogok korlátozása szükséges és arányos intézkedés a nemzetbiztonság védelme érdekében ([166]).

(128) Az Egyesült Királyság kormánya útmutatót adott ki az adatkezelők számára a 2018. évi adatvédelmi törvény szerint a nemzeti biztonsági tanúsítványok kérelmezése mérlegelésében történő segítségnyújtás céljából, amely kiemeli, hogy az érintettek jogai korlátozásának a nemzetbiztonság védelme érdekében arányosnak és szükségesnek kell lennie ([167]). Valamennyi nemzeti biztonsági tanúsítványt közzé kell tenni a biztos honlapján ([168]).

([159]) A 2018. évi adatvédelmi törvény 103. szakasza.

([160]) A 2018. évi adatvédelmi törvény 109. szakasza. Személyes adatok továbbítása nemzetközi szervezeteknek vagy az Egyesült Királyságon kívüli országoknak akkor lehetséges, ha az adattovábbítás szükséges és arányos intézkedés, amelyet az adatkezelő jogszabályi funkcióinak vagy a biztonsági szolgálatról szóló 1989. évi törvény és a hírszerző ügynökségekről szóló 1994. évi törvény egyes szakaszaiban előírt egyéb céloknak megfelelően hajtanak végre.

([161]) A biztos útmutatója, lásd a 158. lábjegyzetet.
A 2018. évi adatvédelmi törvény 30. szakasza és a 2018. évi adatvédelmi törvény 7. melléklete.

([162]) A 2018. évi adatvédelmi törvény 110. szakaszának (2) bekezdése sorolja fel azokat a rendelkezéseket, amelyek alól kivétel engedélyezhető. Ide tartoznak az adatvédelmi elvek (a jogszerűség elvének kivételével), az érintettek jogai, az információügyi biztos tájékoztatásának kötelezettsége a személyes adatok megsértéséről, az információügyi biztos nemzetközi kötelezettségeknek megfelelő ellenőrzési hatásköre, az információügyi biztos bizonyos végrehajtási hatáskörei, az egyes adatvédelmi megsértéseket bűncselekménnyé nyilvánító rendelkezések, valamint az adatkezelés speciális, például újságírói, tudományos vagy művészeti céljaira, vonatkozó rendelkezések.

([163]) Lásd a Baker kontra miniszter ügyet, lásd a 61. lábjegyzetet.

([164]) Az Egyesült Királyság magyarázata a megfelelőségi megbeszélésekre, H. szakasz: Nemzetbiztonsági adatvédelmi és nyomozati hatásköri keret, 15–16. oldal (lásd a 31. lábjegyzetet.). Lásd még Baker kontra miniszter ügyet (lásd a 61. lábjegyzetet), amelyben a bíróság megsemmisítette a belügyminiszter által kiállított és a nemzetbiztonsági kivétel alkalmazását megerősítő nemzetbiztonsági tanúsítványt, mivel úgy ítélte meg, hogy nincs oka általános mentesség megadására a hozzáférési kérelmek megválaszolásának kötelezettsége alól, és hogy az említett kivétel eseti elemzés nélkül minden körülmények között történő alkalmazása meghaladná a nemzetbiztonság védelméhez szükséges és arányos mértéket.

([165]) Lásd a biztos és az UKIC közötti egyetértési megállapodást, amely szerint „amikor a biztos panaszt kap egy érintettől, az információügyi biztos meg kíván győződni arról, hogy a kérdést helyesen kezelték, és adott esetben a mentesség alkalmazását megfelelően vették igénybe". Az Információügyi Bizottság Irodája és az Egyesült Királyság Hírszerző Közössége közötti egyetértési megállapodás 16. pontja, elérhető az alábbi linken: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf

([166]) A 2018. évi adatvédelmi törvény megszüntette a tanúsítványoknak az 1998. évi adatvédelmi törvény 28. cikkének (2) bekezdése alapján történő kiállításának lehetőségét. A „régi tanúsítványok" kiadásának lehetősége azonban továbbra is fennáll annyiban, amennyiben az 1998. évi törvény szerinti történelmi kihívás áll fenn (lásd a 2018. évi adatvédelmi törvény20. melléklete 5. részének 17. pontját). Ez a lehetőség azonban nagyon ritkának tűnik, és csak korlátozott esetekben fog érvényesülni, például, amikor az érintett kihívást jelent a nemzetbiztonsági mentesség olyan hatóság általi adatkezeléshez kapcsolódó alkalmazásával kapcsolatban, amely az adatkezelést az 1998. évi törvény szerint végezte. Meg kell jegyezni, hogy ezekben az esetekben az 1998. évi adatvédelmi törvény 28. szakasza teljes egészében alkalmazandó, ideértve a tanúsítvány érintett általi, íróságon történő megtámadásának lehetőségét is.

([167]) Az Egyesült Királyság kormányának útmutatója a nemzetbiztonsági tanúsítványokról a 2018. évi adatvédelmi törvény alapján, amely a következő linken érhető el: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf Az Egyesült Királyság hatóságainak magyarázata szerint, bár a tanúsítvány meggyőző bizonyíték arra, hogy a tanúsítványban leírt adatok vagy feldolgozás tekintetében a kivétel alkalmazható, nem mentesíti az adatkezelőt azon követelmény alól, hogy esetenkénti alapon mérlegelje, szükség van-e a kivétel igénybevételére.

([168]) A 2018. évi adatvédelmi törvény 130. szakasza szerint a biztos dönthet úgy, hogy nem teszi közzé a tanúsítvány szövegét vagy annak egy részét, ha az ellentétben állna a nemzetbiztonsági érdekkel vagy a közérdekkel, vagy veszélyeztethetné bármely személy biztonságát. Ezekben az esetekben a biztos a tanúsítvány kiállításának tényét teszi közzé.

(129) A tanúsítvány meghatározott időtartamra, legfeljebb öt évre szólhat, ezért azt a végrehajtó hatalom rendszeresen felülvizsgálja ([169]). A tanúsítványban meg kell jelölni a kivétel hatálya alá tartozó személyes adatokat vagy személyesadat-kategóriákat, valamint a 2018. évi adatvédelmi törvény azon rendelkezéseit, amelyekre a kivétel vonatkozik ([170]).

(130) Fontos megjegyezni, hogy a nemzetbiztonsági tanúsítványok nem jelentenek további alapot az adatvédelmi jogok nemzetbiztonsági okokból történő korlátozásához. Másként megfogalmazva: az adatkezelő vagy az adatfeldolgozó csak akkor veheti igénybe a tanúsítványt, ha megállapítást nyert, hogy szükség van a nemzetbiztonsági kivételre, amelyet – a fentebb kifejtettek szerint – esetenkénti alapon kell alkalmazni ([171]). Még ha nemzetbiztonsági tanúsítvány is vonatkozik a szóban forgó kérdésre, a biztos megvizsgálhatja, hogy a nemzetbiztonsági kivételre hivatkozás egy adott esetben indokolt volt-e ([172]).

(131) Bármely személy, akit a tanúsítvány kiállítása közvetlenül érint, fellebbezést nyújthat be az Upper Tribunalhoz (Felsőbb Törvényszék) ([173]) a tanúsítvány ellen ([174]) vagy ha a tanúsítvány általános leírás alapján azonosítja az adatokat, megtámadhatja a tanúsítvány konkrét adatokra való alkalmazását ([175]). A törvényszék felülvizsgálja a tanúsítvány kiadásáról szóló határozatot, és dönt, hogy volt-e észszerű indok a tanúsítvány kiadására ([176]). Számos kérdést mérlegelhet, beleértve a szükségességet, az arányosságot és a jogszerűséget, figyelemmel az érintettek jogaira gyakorolt hatásra, és a nemzetbiztonság védelme szükségességének kiegyensúlyozására. Ennek eredményeként a bíróság megállapíthatja, hogy a tanúsítvány nem vonatkozik a fellebbezés tárgyát képező konkrét személyes adatokra ([177]).

(132) A lehetséges korlátozások egy másik csoportja a 2018. évi adatvédelmi törvény 11. melléklete alapján a 2018. évi adatvédelmi törvény 4. részének egyes rendelkezéseire ([178]) egyéb fontos általános közérdekű vagy védett érdekek – például parlamenti kiváltságok, jogi szakmai kiváltságok (ügyvédi titoktartás), bírósági eljárások lefolytatása vagy a fegyveres erők harci hatékonysága – védelmére alkalmazott korlátozásokat ([179]) érinti. Ezeknek a rendelkezéseknek az alkalmazása alóli kivétel bizonyos adatkategóriákra vonatkozik („csoportalapú"), vagy pedig a kivétel annyiban érvényesül, amennyiben e rendelkezések alkalmazása valószínűleg sérti a védett érdekeket („sérelem alapú") ([180]). A sérelmen alapuló kivételekre csak akkor lehet hivatkozni, amennyiben a felsorolt adatvédelmi rendelkezések

([169]) Az Egyesült Királyság kormányának útmutatója a nemzetbiztonsági tanúsítványokról, 15. pont, lásd a 167. lábjegyzetet.

([170]) Az Egyesült Királyság kormányának útmutatója a nemzetbiztonsági tanúsítványokról, 5. pont, lásd a 167. lábjegyzetet.

([171]) Lásd a 164. lábjegyzetet.

([172]) A 2018. évi adatvédelmi törvény 102. szakasza előírja, hogy az adatkezelőnek képesnek kell lennie annak bizonyítására, hogy betartotta a 2018. évi adatvédelmi törvényt. Ez azt jelenti, hogy egy hírszerző ügynökségnek igazolnia kell a biztosnak, hogy a kivétel igénybevételekor figyelembe vette az eset sajátos körülményeit. A biztos egyben közzéteszi a nemzetbiztonsági tanúsítványok nyilvántartását, amely a következő linken érhető el: elérhető az alábbi linken: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/

([173]) A Felső Törvényszék az alsóbb közigazgatási bíróságok által hozott határozatok elleni fellebbezések elbírálására illetékes bíróság, és különleges hatáskörrel rendelkezik bizonyos kormányzati szervek határozatai elleni közvetlen fellebbezésekre.

([174]) A 2018. évi adatvédelmi törvény 111. szakaszának (3) bekezdése.

([175]) A 2018. évi adatvédelmi törvény 111. szakaszának (5) bekezdése.

([176]) A Baker kontra miniszter ügyben (lásd a 61. lábjegyzetet) a Törvényszék megsemmisítette a belügyminiszter által kiadott nemzetbiztonsági tanúsítványt, mivel úgy ítélte meg, hogy nincs ok a hozzáférési kérelmek megválaszolásának kötelezettsége alóli általános mentesség megadására, és hogy az említett kivétel eseti elemzés nélkül minden körülmények között történő alkalmazása meghaladná a nemzetbiztonság védelméhez szükséges és arányos mértéket.

([177]) Az Egyesült Királyság kormányának útmutatója a nemzetbiztonsági tanúsítványokról, 25. pont, lásd a 167. lábjegyzetet.

([178]) Ez az alábbiakat foglalja magában: i. a 4. rész adatvédelmi elvei, kivéve az adatkezelés jogszerűségének első elv szerinti követelményét és azt a tényt, hogy az adatkezelésnek meg kell felelnie a 9. és 10. mellékletben meghatározott vonatkozó feltételek egyikének; ii. az érintettek jogai; és iii. a jogsértések biztosnak történő bejelentésével kapcsolatos kötelezettségek.

([179]) A 2018. évi adatvédelmi törvény 4. része írja elő azt a jogi keretet, amely a személyes adatok titkosszolgálatok által végzett minden típusú (és nem csak nemzetbiztonsági feladataik ellátása céljából történő) kezelésére vonatkozik. Ezért a 4. rész akkor is irányadó, amikor a hírszerző ügynökségek adatokat például humánerőforrás-gazdálkodás céljából, peres ügyekben vagy közbeszerzés keretében kezelnek. A 11. mellékletben felsorolt korlátozásokat elsősorban ezekben az egyéb összefüggésekben történő alkalmazásra szánták. Például egy alkalmazottal folyó perben hivatkozni lehet a „bírósági eljárás" céljából történő korlátozásra, vagy a közbeszerzés keretében a „tárgyalási" célú korlátozásra stb. Ezt tükrözi a biztos hírszerző szolgálatok általi adatkezelésről szóló útmutatója, amely példaként említi a hírszerző ügynökség és egy volt munkavállaló közötti megállapodás letárgyalását a 11. melléklet szerinti korlátozások vonatkozásában (lásd a 161. lábjegyzetet). Megjegyzendő továbbá, hogy ugyanezek a korlátozások más hatóságok által is igénybe vehetők a 2018. évi adatvédelmi törvény 2. részének 2. melléklete szerint.

([180]) Az Egyesült Királyság magyarázata szerint a „csoportalapú" kivételek a következők: i. információk a korona kitüntetéseinek és méltóságainak elnyeréséről; ii. ügyvédi titoktartási kötelezettség; iii. bizalmas foglalkoztatási, képzési vagy oktatási referenciák; és iv. vizsgalapok és jegyek. A „sérelmen alapuló" kivételek a következő kérdéseket érintik: i. bűncselekmények megelőzése vagy felderítése; az elkövetők visszatartása és üldözése; ii. parlamenti kiváltság; iii. bírósági eljárások; iv. az állami fegyveres erők harci hatékonysága; v. az Egyesült Királyság gazdasági jóléte; vi. az érintettel folytatott tárgyalás; vii. tudományos vagy történelmi kutatás vagy statisztikai célok; viii. közérdekű archiválás. Az Egyesült Királyság magyarázata a megfelelőségi megbeszélésekre, H. szakasz: Nemzetbiztonság, 13. oldal, lásd a 31. lábjegyzetet.

alkalmazása valószínűleg sérti a szóban forgó konkrét érdekeket. A kivétel alkalmazását ezért mindig indokolni kell az adott esetben valószínűleg bekövetkező, releváns sérelemre való hivatkozással. Csoportalapú kivételekre csak azon konkrét, szűken meghatározott adatkategóriák esetében lehet hivatkozni, amelyekre a mentességet megadják. Ezek célja és hatása hasonló az Egyesült Királyság általános adatvédelmi rendelete alóli számos kivételhez (a 2018. évi adatvédelmi törvény 2. melléklete alapján), amelyek viszont tükrözik a GDPR 23. cikkében foglaltakat.

(133) A fentiekből következik, hogy az alkalmazandó brit jogszabályi rendelkezések tekintetében – a bíróságok és az Információügyi Bizottság által is értelmezett – korlátozások és feltételek érvényesülnek annak biztosítása érdekében, hogy ezek a kivételek és korlátozások a nemzetbiztonság védelméhez szükséges és arányos határokon belül maradjanak.

3.2. **Az egyesült királyságbeli hatóságok hozzáférése az adatokhoz és az adatok használata bűnüldözés céljából**

(134) Az Egyesült Királyság törvényei számos korlátozást állapítanak meg a személyes adatokhoz való hozzáférésre és azok bűnüldözési célokra történő felhasználására, és ezen a területen felügyeleti és jogorvoslati mechanizmusokat biztosítanak, amelyek összhangban állnak az e határozat (113)–(115) preambulumbekezdésében említett követelményekkel. Az említett hozzáférés feltételeit és az e hatáskörök alkalmazására vonatkozó biztosítékokat a következő szakaszok részletesen értékelik.

3.2.1. *Jogalapok és az alkalmazandó korlátozások/biztosítékok*

(135) A 2018. évi adatvédelmi törvény 35. szakaszában garantált jogszerűség elve szerint a személyes adatok bármely bűnüldözési célból történő kezelése csak akkor jogszerű, ha az törvényen alapul, és vagy az érintett hozzájárult az e célból történő adatkezeléshez ([181]), vagy az adatkezelés az illetékes hatóság által e célból ellátott feladat ellátásához szükséges.

3.2.1.1. Körözési parancsok és közlésre kötelezések

(136) Az Egyesült Királyság jogi kereteiben megengedett a személyes adatok gyűjtése az gazdasági szereplőktől, beleértve azokat is, amelyek a megfelelőségre vonatkozó jelenlegi határozat alapján az EU-ból továbbított adatokat kezelnek bűnüldözési célból, körözési parancsok ([182]) és közlésre kötelezések alapján. ([183])

(137) A körözési parancsokat a bíróság adja ki, általában a nyomozótiszt kérelmére. Ez lehetővé teszik a tiszt számára a helyiségekbe belépést, a nyomozás szempontjából releváns anyagok vagy személyek keresése céljából, és bármit elvigyen, amelyre engedélyezték a körözést, beleértve az összes vonatkozó dokumentumot vagy személyes adatokat tartalmazó anyagot ([184]). A közlésre kötelezés – amelyet szintén bíróságnak kell kiadnia – megköveteli, hogy az abban meghatározott személy átadja a birtokában lévő vagy általa ellenőrzött anyagot, vagy ahhoz hozzáférést adjon. A kérelmezőnek meg kell indokolnia a bíróság előtt, hogy miért van szükség a parancsra vagy a kötelezésre,

([181]) A hozzájárulás használata nem tűnik relevánsnak a megfelelőségi esetkörben, mivel egy adattovábbítási helyzetben az Egyesült Királyság bűnüldöző hatóságai nem hozzájárulás alapján gyűjtik az adatokat közvetlenül egy uniós érintettől.

([182]) A vonatkozó jogalaphoz lásd az 1984. évi rendőrségi törvény 8. és azt követő szakaszait (Anglia és Wales esetében), a Police and Criminal Evidence Order (Észak-Írország) 1989 elnevezésű (a rendőrségről és büntetőügyekben történő bizonyításfelvételről szóló 1989. évi) rendelet 10. és azt követő szakaszait, Skócia esetében pedig a „common law" alapján történik (lásd a Criminal Justice (Scotland) Act 2016 elnevezésű, a büntető igazságszolgáltatásról (Skócia) szóló 2016. évi törvény 46. szakaszát) és a Criminal Law (Consolidation) (Scotland) elnevezésű (büntetőjogi (konszolidációs) (Skócia)) törvény 23B. szakaszát. A letartóztatás után kiadott körözési parancs jogalapja az 1984. évi rendőrségi törvény 18. szakasza (Anglia és Wales esetében), a rendőrségről és büntetőügyekben történő bizonyításfelvételről szóló 1989. évi rendelet (Észak-Írország) 20. és azt követő szakaszai, Skócia esetében pedig a „common law" alapján történik (lásd a büntető igazságszolgáltatásról (Skócia) szóló 2016. évi törvény 46. szakaszát). Az Egyesült Királyság hatóságai egyértelművé tették, hogy a bíróság a nyomozótiszt kérelmére bírósági határozatot ad ki. Ez lehetővé teszi a tiszt számára a helyiségekbe belépést, a nyomozás szempontjából releváns anyagok vagy személyek keresése céljából; a parancs végrehajtása gyakran rendőri segítséget igényel.

([183]) Ha a nyomozás pénzmosásra vonatkozik (ideértve az elkobzást és a polgári behajtási eljárást is), a közlésre kötelezés kérelmezésének releváns jogalapja Anglia, Wales és Észak-Írország esetében a 345. és azt követő szakaszok, valamint Skócia esetében a Proceeds of Crime Act 2002 elnevezésű (a bűncselekményekből származó bevételekről szóló) törvény 380. és azt követő szakaszai. Ha a vizsgálat a pénzmosástól eltérő kérdésekre vonatkozik, a közlésre kötelezés iránti kérelmet Anglia és Wales esetében az 1984. évi rendőrségi törvény 9. szakaszának és 1. mellékletének, valamint Észak-Írország esetében a rendőrségről és büntetőügyekben történő bizonyításfelvételről szóló 1989. évi rendelet 10. és azt követő szakaszainak megfelelően lehet benyújtani. Skócia esetében ez a „common law" alapján történik (lásd a 2016. évi büntető igazságszolgáltatásról [Skócia] szóló törvény 46. szakaszát és a büntetőjogi [konszolidációs] [Skócia] törvény 23B. szakaszát). Az Egyesült Királyság hatóságai egyértelművé tették, hogy a közlésre kötelezés megköveteli, hogy az abban meghatározott személy átadja a birtokában lévő vagy ellenőrzése alatt álló anyagot vagy ahhoz hozzáférést adjon (lásd az 1984. évi rendőrségi törvény 1. mellékletének 4. pontját).

([184]) Például az 1984. évi rendőrségi törvény a 8. és 18. szakaszban felhatalmazást ad minden olyan dolog lefoglalására és elvitelére, amelyre a körözést engedélyezték.

és az miért képez közérdeket. Számos olyan törvényi hatáskör létezik, amelyek lehetővé teszik a körözési parancsok és a közlésre kötelezések kiadását. Minden rendelkezésnek megvannak a maga törvényi feltételei, amelyeknek meg kell felelni a parancs ([185]) vagy közlésre kötelezés ([186]) kiadásához.

(138) A közlésre kötelezéseket és a körözési parancsokat bírósági felülvizsgálat útján lehet megtámadni ([187]). Ami a biztosítékokat illeti, a 2018. évi adatvédelmi törvény 3. része szerinti összes illetékes bűnüldöző hatóság személyes adatokhoz csak a 2018. évi adatvédelmi törvényben meghatározott elveknek és követelményeknek megfelelően férhet hozzá – ami az adatkezelés egyik formája – (lásd a (122) és (124) above a preambulumbekezdést). Ezért a bűnüldöző hatóság által benyújtott minden

([185]) Például a rendőrségi törvény 8. és 18. szakasza szabályozza a békebíró jogát arra, hogy parancsot engedélyezzen, és a rendőrt ingatlanok átvizsgálására. Az első esetben (8. szakasz) a végzés kiadása előtt a békebírónak meg kell győződnie arról, hogy van-e észszerű oka feltételezni, hogy i. üldözendő bűncselekményt követtek el; ii. a helyszínen található olyan anyag, amely valószínűleg jelentős értéket képvisel (akár önmagában, akár más anyaggal együtt) a bűncselekmény nyomozása szempontjából; iii. az anyag valószínűleg releváns bizonyíték; iv. nem tartalmaz ügyvédi titoktartási kötelezettség alá eső tételeket, kizárt anyagokat vagy különleges eljárások alá tartozó anyagokat; és v. a parancs igénybevétele nélkül a belépés nem lenne lehetséges. A második esetben a 18. szakasz lehetővé teszi a rendőr számára, hogy az üldözendő bűncselekmény miatt letartóztatott személy helyiségében ügyvédi titoktartási kötelezettség alá nem eső anyagokat keressen, ha megalapozott oka van feltételezni, hogy a helyiségben az adott bűncselekményhez vagy más hasonló vagy kapcsolódó üldözendő bűncselekményre utaló bizonyíték van. Az említett átkutatásnak csak az anyag megtalálására kell korlátozódnia, és azt írásban engedélyeznie kell legalább felügyelő rendfokozatú rendőrnek, kivéve, ha ez a bűncselekmény nyomozásához szükséges. Ebben az esetben egy legalább felügyelő rendfokozatú tisztet a végrehajtást követően a lehető leghamarabb tájékoztatni kell. A kutatás okait és a keresett bizonyítékok jellegét rögzíteni kell. Ezenkívül az 1984. évi rendőrségi törvény 15. és 16. szakasza törvényi biztosítékokat tartalmaz, amelyeket be kell tartani a körözési parancs kérelmezése során. A 15. szakasz meghatározza a házkutatási parancs megszerzésére vonatkozó követelményeket (ideértve a rendőr által benyújtott kérelem tartalmát és azt a tényt, hogy a parancsnak egyebek mellett meg kell határoznia azt a jogszabályt, amely alapján kiadták, és lehetőség szerint meg kell határoznia a keresendő dolgokat és személyeket, valamint az átvizsgálandó helyiségeket). A 16. szakasz szabályozza, hogy a végzés alapján történő keresést miként kell végrehajtani (például: a 16. szakasz (5) bekezdése előírja, hogy a parancsot végrehajtó tiszt átadja az ott tartózkodó személynek a parancs másolatát; a 16. cikk (11) bekezdése előírja, hogy a végrehajtás után a parancsot 12 hónapig meg kell őrizni; A 16. szakasz (12) bekezdése lehetőség ad az ott tartózkodó személy számára, hogy ebben az időszakban ellenőrizze a parancsot, ha úgy kívánja. Ezek a szakaszok segítenek az EJEE 8. cikkének betartásában (lásd például: Kent Pharmaceuticals kontra Súlyos Csalásokkal foglalkozó Hivatal igazgatója ügyet, Lord Woolf CJ (2002 EWHC 3023 (QB)), 30. pont). Ezen biztosítékok be nem tartása azt eredményezheti, hogy a keresést jogszerűtlennek nyilvánítják (például az R (Brook) kontra Preston Crown Court ügyben (2018 EWHC 2024 (Admin)), 2018) ACD 95; az R (Superior Import/Export Ltd) kontra Revenue and Customs Commissioners ügyben (2017 EWHC 3172 (Admin)), 2018, Lloyd's Rep FC 115; és az R (F) kontra Blackfriars Crown Court ügyben (2014 EWHC 1541 (Admin)). Az 1984. évi rendőrségi törvény 15. és 16. szakaszát kiegészíti a rendőrségi törvény B kódexe, egy olyan gyakorlati kódex, amely a helyiségek átkutatására vonatkozó rendőri hatáskörök gyakorlását szabályozza.

([186]) Például a bűncselekményekből származó jövedelemről szóló 2002. évi törvény alapján közlésre kötelezés kiadásakor azon túlmenően, hogy észszerű okokra van szükség a bűncselekményekből származó jövedelemről szóló törvény 346. szakaszának (2) bekezdésében meghatározott feltételek teljesítéséhez, ésszerű alapjának kell lennie annak, hogy a személy az így meghatározott anyag birtokában van vagy az az ellenőrzése alatt áll, és az anyag valószínűleg jelentős értéket képvisel. Ezenkívül a közlésre kötelezés kiadásának másik követelménye, hogy megalapozott oknak kell lennie annak feltételezésére, hogy közérdeket szolgál az anyag átadása vagy ahhoz hozzáférés biztosítása, figyelembe véve a) a nyomozásban az anyag megszerzésétől várható előnyt; és b) azok a körülmények, amelyek között a kérelemben megjelölt személy valószínűleg az információt hordozó anyag birtokában van vagy az ellenőrzése alatt áll. Hasonlóképpen, az 1984. évi rendőrségi törvény 1. számú mellékletében előírt közlésre kötelezés iránti kérelmet elbíráló bíróságnak meg kell győződnie arról, hogy a meghatározott feltételek teljesülnek. Különösen a rendőrségi törvény 1. melléklete két különálló alternatív feltételcsoportot határoz meg, amelyek közül az egyiknek teljesülnie kell, mielőtt a bíró kiadhatná a közlésre kötelezést. Az első csoport megköveteli, hogy a bírónak észszerű indoka legyen annak feltételezésére, hogy i. üldözendő bűncselekményt követtek el; ii. a helyszínen keresett anyag különleges eljárás hatálya alatt áll, vagy ilyen eljárással érintett, de nem minősül kizárt anyagnak; iii. valószínűleg önmagában vagy más anyaggal együtt jelentős értéket képvisel a vizsgálat szempontjából; iv. és valószínűleg releváns bizonyíték; v. az anyag megszerzésének egyéb módszereit megkísérelték, vagy azok valószínű kudarca miatt meg sem kísérelték; és vi. figyelembe véve a nyomozási hasznot és az egyén általi birtoklás körülményeit, közérdek az, hogy az anyagot átadják, vagy hogy hozzáférést biztosítsanak hozzá. A második feltételcsoport megköveteli az alábbiakat: i. a helyszínen legyen olyan anyag, amely különleges eljárás alatt áll vagy kizárt anyag; ii. ha nem lenne keresési tilalom a rendőrségi törvény előtt elfogadott jogszabályok alapján történő keresésre a különleges eljárás alatt álló vagy ügyvédi titoktartási kötelezettséggel érintett anyagokra vonatkozóan, a körözési parancsot az anyagra kiadhatták volna; és iii. ez helyénvaló lett volna.

([187]) A bírósági felülvizsgálat az a jogi eljárás, amelyen keresztül egy állami szerv határozatai megtámadhatók a High Court előtt. A bíróságok „felülvizsgálják" a megtámadott határozatot, és eldöntik, hogy a „common law" szerinti fogalmak/elvek figyelembevételével vitatható-e a határozat jogi hibája. A bírósági felülvizsgálat legfőbb indokai a jogszerűtlenség, az észszerűtlenség, az eljárási szabálysértés, a jogszerű elvárások és az emberi jogok. A sikeres bírósági felülvizsgálatot követően a bíróság számos különféle jogorvoslatot rendelhet el; ezek közül a leggyakoribb a megsemmisítés (amely hatályon kívül helyezi vagy érvényteleníti az eredeti határozatot – azaz a körözési parancs kiadásáról szóló határozatot), bizonyos körülmények között ennek része lehet a pénzbeni kártérítés megítélése is. Az egyesült királyságbeli bírósági felülvizsgálatról további részletek a kormány jogi főosztályának „Judge Over Your Shoulder – a guide to good decision-making" (Bírói felügyelet – útmutató a megfelelő döntéshozatalhoz) című kiadványban találhatók, amely elérhető a következő linken: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf

kérelemnek meg kell felelnie annak az elvnek, amely szerint az adatkezelés céljait meg kell határozni, azoknak egyértelműnek és jogosnak kell lenniük ([188]), és hogy az illetékes hatóság által kezelt személyes adatoknak e cél szempontjából relevánsnak és nem eltúlzott mértékűeknek kell lenniük ([189]).

3.2.1.2. Bűnüldözési célú nyomozati hatáskörök

(139) Egyes bűnüldöző hatóságok – például a Nemzeti Bűnügyi Ügynökség vagy a rendőrfőkapitány ([190]) – a nyomozati hatáskörökről szóló 2016. évi törvény szerinti célzott nyomozati hatásköröket használhat kizárólag súlyos bűncselekmények megelőzése vagy felderítése céljából ([191]). Ebben az esetben a 2018. évi adatvédelmi törvény 3. részében előírt biztosítékok mellett érvényesülnek a nyomozati hatáskörökről szóló 2016. évi törvényben előírt biztosítékok is. A konkrét nyomozati hatáskörök, amelyeket a bűnüldöző hatóságok igénybe vehetnek, a következők: célzott lehallgatás (a nyomozati hatáskörökről szóló 2016. évi törvény 2. része), kommunikációs adatok gyűjtése (a nyomozati hatáskörökről szóló 2016. évi törvény 3. része), kommunikációs adatok megőrzése (a nyomozati hatáskörökről szóló 2016. évi törvény 4. része) és a berendezések célzott zavarása (a nyomozati hatáskörökről szóló 2016. évi törvény 5. része). A lehallgatás a kommunikáció tartalmának megszerzésére terjed ki ([192]), míg a kommunikációs adatok gyűjtése és megőrzése nem a kommunikáció tartalmának gyűjtésére, hanem a kommunikáció alanyaira, idejére, helyére és módjára irányul. Ez magában foglalja például a kommunikáció időpontját és időtartamát, a kommunikáció kezdeményezőjének és címzettjének telefonszámát vagy e-mail-címét, és esetenként azoknak az eszközöknek a helyét, amelyekről a kommunikációt folytatták, a telefonos szolgáltatás előfizetőjét vagy a tételes számla részleteit ([193]). A berendezések zavarása olyan technikák összessége, amelyeket berendezésekből különféle adatok gyűjtésére használnak, ideértve a számítógépeket, a táblagépeket és az okostelefonokat, valamint a kábeleket, a vezetékeket és a tárolóeszközöket ([194]).

(140) A célzott lehallgatási hatáskörök akkor is felhasználhatók, amikor „az EU kölcsönös segítségnyújtási eszközének vagy egy nemzetközi kölcsönös segítségnyújtási megállapodás rendelkezéseinek kell érvényt szerezni” (úgynevezett „kölcsönös segítségnyújtási parancs” ([195])). Kölcsönös segítségnyújtási parancsot csak lehallgatással kapcsolatban adnak, a kommunikációs adatok gyűjtésére vagy berendezés zavarására nem. Ezeket a célzott hatásköröket a nyomozati hatáskörről szóló 2016. évi törvény (a nyomozati hatáskörökről szóló 2016. évi törvény) szabályozza ([196]), amely az Anglia, Wales és Észak-Írország vonatkozásában a nyomozati hatáskörökről szóló 2000. évi törvénnyel és Skócia esetében a Regulation of Investigatory Powers (Scotland) Act 2000 elnevezésű (a nyomozati hatáskörök szabályozásáról (Skócia) szóló 2000. évi) törvénnyel (a nyomozati hatáskörök szabályozásáról (Skócia) szóló 2000. évi törvény) együtt előírja az említett hatáskörök felhasználására a jogalapot és meghatározza az alkalmazandó korlátozásokat és biztosítékokat. A nyomozati hatáskörökről szóló 2016. évi törvény a tömeges nyomozati hatáskörök alkalmazásának rendszerét is előírja, bár ezek a bűnüldöző hatóságok számára nem állnak rendelkezésre (csak a hírszerző ügynökségek vehetik igénybe azokat) ([197]).

([188]) A 2018. évi adatvédelmi törvény 36. szakaszának (1) bekezdése.

([189]) A 2018. évi adatvédelmi törvény 37. szakasza.

([190]) Különösen a következő bűnüldöző hatóságok kérhetnek célzott lehallgatási parancsot: a Nemzeti Bűnügyi Ügynökség főigazgatója, a Police of the Metropolis biztosa, az észak-ír rendőrség főkapitánya, a skóciai rendőrség főkapitánya, a királynő bevételi és vámügyi biztosa, a védelmi hírszerzés és olyan személyek, akik az Egyesült Királyságon kívüli ország vagy terület illetékes hatóságának minősülnek az Unió valamely kölcsönös segítségnyújtási eszköze vagy nemzetközi kölcsönös segítségnyújtási megállapodás alkalmazásában (a nyomozati hatáskörökről szóló 2016. évi törvény 18. szakaszának (1) bekezdése).

([191]) A nyomozati hatáskörökről szóló 2016. évi törvény 263. szakaszának (1) bekezdése előírja, hogy „súlyos bűncselekmény” olyan bűncselekmény, amely várhatóan legalább 3 éves időtartamú szabadságvesztéssel büntetendő nem bűnismétlő felnőtt esetében, vagy a cselekmény erőszakos, jelentős anyagi hasznot eredményez, vagy csoportosan követték el. Ezenkívül a nyomozati hatáskörökről szóló 2016. évi törvény 4. része szerinti kommunikációs adatok gyűjtése alkalmazásában a 87. cikk (10B) bekezdése előírja, hogy „súlyos bűncselekmény” olyan bűncselekmény, amely legalább 12 hónapos szabadságvesztéssel büntethető, vagy bűncselekményt nem magánszemély követte el, vagy amelynek szerves része a kommunikáció küldése vagy az egyén magánéletének sérelme.

([192]) Lásd a nyomozati hatáskörökről szóló 2016. évi törvény 4. szakaszát.

([193]) Lásd a nyomozati hatáskörökről szóló 2016. évi törvény 261. szakaszának (5) bekezdését és a kommunikációs adatok tömeges beszerzésének gyakorlati kódexét, amely a következő linken érhető el: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, 2.9. pont.

([194]) Gyakorlati kódex a berendezések zavarásáról, elérhető a következő linken: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, 2.2. pont.

([195]) A kölcsönös segítségnyújtási parancs felhatalmazza az Egyesült Királyság hatóságát arra, hogy az Egyesült Királyság területén kívüli hatóságnak segítséget nyújtson a lehallgatáshoz és a lehallgatott anyag ilyen hatóság számára történő közlésére, egy nemzetközi kölcsönös segítségnyújtási eszközzel összhangban (a nyomozati hatáskörökről szóló 2016. évi törvény 15. szakaszának (4) bekezdése).

([196]) A nyomozati hatáskörökről szóló 2016. évi törvény (lásd: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) felváltotta a kommunikáció lehallgatására, a berendezések zavarására és a kommunikációs adatok gyűjtésére vonatkozó különféle törvényeket, különösen a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény I. részét, amely a korábbi általános jogi keretet biztosította a nyomozati hatáskörök bűnüldöző és nemzetbiztonsági hatóságok általi felhasználásához.

([197]) A nyomozati hatáskörökről szóló 2016. évi törvény 138. szakaszának (1) bekezdése, 158. szakaszának (1) bekezdése, 178. szakaszának (1) bekezdése, 199. szakaszának (1) bekezdése.

(141) E hatáskörök gyakorlásához a hatóságoknak parancsot kell beszerezniük ([198]), amelyet az illetékes hatóság állít ki ([199]), és egy független igazságügyi biztos hagyja jóvá ([200]) (úgynevezett duplán ellenőrzött, „double-lock" eljárás). Az említett parancs megszerzésére szükségességi és arányossági teszt vonatkozik ([201]). Mivel a nyomozati hatáskörökről szóló 2016. évi törvény által biztosított célzott nyomozati hatáskörök megegyeznek a nemzetbiztonsági ügynökségek rendelkezésére álló jogokkal, az említett hatáskörökre alkalmazandó feltételekkel, korlátozásokkal és biztosítékokkal a személyes adatokhoz az Egyesült Királyság hatóságai által nemzetbiztonsági célokból való hozzáférésről és azok felhasználásáról szóló szakasz részletesen foglalkozik (lásd a (177) és azt követő preambulumbekezdéseket).

3.2.2. *Az összegyűjtött információk további felhasználása*

(142) Az adatok bűnüldöző hatóság által másik hatósággal, a gyűjtés eredeti céljától eltérő célra történő megosztása (úgynevezett „további megosztás") bizonyos feltételekhez kötött.

(143) Az (EU) 2016/680 irányelv 4. cikkének (2) bekezdésében előírtakhoz hasonlóan a 2018. évi adatvédelmi törvény 36. szakaszának (3) bekezdése lehetővé teszi az illetékes hatóságok által bűnüldözési célból gyűjtött személyes adatokat további feldolgozását (akár az eredeti adatkezelő vagy egy másik adatkezelő által) bármely más bűnüldözési célra, feltéve, hogy az adatkezelőt törvény felhatalmazza az adatok más célú kezelésére, és az adatkezelés szükséges és arányos az említett célra ([202]). Ebben az esetben a 2018. évi adatvédelmi törvény 3. része által biztosított, a (122) és (124) preambulumbekezdésben említett összes biztosíték vonatkozik az átvevő hatóság által végzett adatkezelésre.

(144) Az Egyesült Királyság jogrendjében különféle törvények kifejezetten megengedik a további megosztást. Különösen: i. a Digital Economy Act 2017 elnevezésű (a digitális gazdaságról szóló 2017. évi) törvény lehetővé teszi a hatóságok közötti megosztást többféle célra, például az állami szektorral szembeni bármilyen csalás esetén, amely egy hatóság számára veszteséggel vagy veszteség kockázatával járna ([203]) vagy hatósággal vagy az állammal szemben fennálló tartozás esetén ([204]); ii. a Crime and Courts Act 2013 elnevezésű (a bűncselekményekről és bíróságokról szóló 2013. évi) törvény lehetővé teszi az információk Nemzeti Bűnügyi Ügynökséggel (NCA) ([205]) való megosztását a súlyos bűncselekmények és a szervezett bűnözés elleni küzdelem, azok nyomozása és a büntetőeljárás lefolytatása érdekében; iii. a Serious Crime Act 2007 elnevezésű (a súlyos bűncselekményekről szóló 2007. évi) törvény, amely lehetővé teszi a hatóságok számára, hogy csalás megelőzése céljából információkat közöljenek a csalásellenes szervezetekkel ([206]).

(145) Ezek a törvények kifejezetten előírják, hogy az információmegosztásnak meg kell felelnie a 2018. évi adatvédelmi törvényben meghatározott elveknek. Emellett a Rendészeti Főiskola kiadta az információmegosztás engedélyezett szakmai gyakorlatát ([207]) a rendőrségnek az Egyesült Királyság általános adatvédelmi rendelete, adatvédelmi törvény és 1998. évi emberi jogi törvény szerinti adatvédelmi kötelezettségeik teljesítésében történő segítségnyújtás céljából.

([198]) A nyomozati hatáskörökről szóló 2016. évi törvény 2. részének 2. fejezete korlátozott számú olyan esetről rendelkezik, amikor a lehallgatás parancs nélkül elvégezhető. Ez az alábbiakat foglalja magában: lehallgatás a küldő vagy a címzett hozzájárulásával, adminisztratív vagy végrehajtási célú lehallgatás, bizonyos intézményekben (börtönökben, pszichiátriai kórházakban és bevándorlási őrizetet nyújtó létesítményekben) zajló lehallgatás, valamint a vonatkozó nemzetközi megállapodásnak megfelelően végrehajtott lehallgatás.

([199]) Az esetek többségében a miniszter az a hatóság, amely a nyomozati hatáskörökről szóló 2016. évi törvény alapján kiadja a parancsokat, míg a skót miniszterek felhatalmazást kapnak célzott lehallgatási parancsok, kölcsönös segítségnyújtási parancsok és berendezések célzott zavarására vonatkozó parancsok kiadására, amennyiben a lehallgatandó személyek vagy helyiségek és berendezések Skóciában találhatók (lásd a nyomozati hatáskörökről szóló 2016. évi törvény 22. és 103. szakaszát). Berendezések célzott zavarása esetén a rendvédelmi vezető (a nyomozati hatáskörökről szóló 2016. évi törvény 6. mellékletének 1. és 2. részében leírtak szerint) adhatja ki a parancsot a nyomozati hatáskörökről szóló 2016. évi törvény 106. szakaszának feltételei szerint.

([200]) Az igazságügyi biztosok segítik a nyomozati hatáskörök biztosát (nyomozási biztos), egy független testületet, amely felügyeleti feladatokat lát el a hírszerző ügynökségek nyomozati hatáskörének felhasználása felett (további részletekért lásd: (162) és azt követő preambulumbekezdések).

([201]) Lásd különösen a nyomozati hatáskörökről szóló 2016. évi törvény 19. és 23. szakaszát.

([202]) A 2018. évi adatvédelmi törvény 36. szakaszának (3) bekezdése.

([203]) A digitális gazdaságról szóló 2017. évi törvény 56. szakasza, elérhető az alábbi linken: https://www.legislation.gov.uk/ukpga/2017/30/section/56

([204]) A digitális gazdaságról szóló 2017. évi törvény 48. szakasza.

([205]) A bűncselekményekről és bíróságokról szóló 2013. évi törvény 7. szakasza az alábbi linken érhető el: https://www.legislation.gov.uk/ukpga/2013/22/section/7

([206]) A súlyos bűncselekményekről szóló 2007. évi törvény 68. szakasza, elérhető az alábbi linken: https://www.legislation.gov.uk/ukpga/2007/27/contents

([207]) Az információmegosztás engedélyezett szakmai gyakorlata, a következő linken érhető el: https://www.app.college.police.uk/app-content/information-management/sharing-police-information

A megosztás irányadó adatvédelmi jogi keretnek való megfelelése tekintetében természetesen bírósági felülvizsgálatnak van helye ([208]).

(146) Ezenkívül az (EU) 2016/680 irányelv 9. cikkében foglaltakhoz hasonlóan a 2018. évi adatvédelmi törvény előírja, hogy a bűnüldözési célokból gyűjtött személyes adatokat a bűnüldözés céljától eltérő célból is fel lehet dolgozni, amennyiben az adatkezelést törvény engedélyezi ([209]).

(147) Ez a típusú megosztás két esetkört ölel fel: 1) amikor a bűnüldöző hatóság az adatokat egy hírszerző ügynökségnek nem minősülő, nem bűnüldöző végrehajtó hatósággal osztja meg (például pénzügyi vagy adóhatóság, versenyhatóság, ifjúsági jóléti hivatal, stb.); és 2) amikor a bűnüldöző hatóság az adatokat hírszerző ügynökséggel osztja meg. Az első esetkör szerint a személyes adatok feldolgozása az Egyesült Királyság általános adatvédelmi rendeletének, valamint a 2018. évi adatvédelmi törvény 2. részének hatálya alá tartozik. A Bizottság a (12)–(111) preambulumbekezdésben értékelte az Egyesült Királyság általános adatvédelmi rendelete és a 2018. évi adatvédelmi törvény 2. része által biztosított biztosítékokat, és arra a következtetésre jutott, hogy az Egyesült Királyság biztosítja az (EU) 2016/679 rendelet hatálya alá tartozó, az Európai Unióból az Egyesült Királyságba továbbított személyes adatok megfelelő szintű védelmét.

(148) A második esetkörben a bűnüldöző hatóságok által nemzetbiztonsági célokból gyűjtött adatok hírszerző ügynökséggel történő megosztása tekintetében az említett megosztás jogalapja a Counter Terrorism Act 2008 elnevezésű (terrorizmus elleni 2008. évi) törvény 19. szakasza ([210]). E törvény alapján bárki információt adhat bármely hírszerző ügynökségnek az ügynökség bármely feladatának ellátása céljából, beleértve a „nemzetbiztonságot" is.

(149) Az adatok nemzetbiztonsági célú megosztását illetően a hírszerző ügynökségekről szóló törvény ([211]) és a biztonsági szolgálatokról szóló törvény ([212]) a törvényi funkcióik ellátásához szükséges mértékre korlátozza a hírszerző ügynökségek adatszerzési képességét. Az adatoknak a hírszerző ügynökséggel történő megosztására törekvő bűnüldöző szerveknek az ügynökségek jogszabályi funkcióin túlmenően számos tényezőt/korlátozást is figyelembe kell venniük, amelyeket a hírszerző ügynökségekről szóló törvény és a biztonsági szolgálatokról szóló törvény ([213]) határoz meg. A terrorizmus elleni 2008. évi törvény 20. szakasza egyértelművé teszi, hogy a 19. szakasz szerinti adatmegosztásnak továbbra is meg kell felelnie az adatvédelmi jogszabályoknak; ami azt jelenti, hogy a 2018. évi adatvédelmi törvény 3. részének összes korlátozása és követelménye érvényesül. Továbbá, mivel az illetékes hatóságok az 1998. évi emberi jogi törvény alkalmazásában hatóságok, biztosítaniuk kell, hogy az egyezmény szerinti jogoknak – ideértve az EJEE 8. cikkét is – összhangban járjanak el. Ezek a korlátok biztosítják, hogy a bűnüldöző szervek és a hírszerző ügynökség közötti minden adatmegosztás megfeleljen az adatvédelmi jogszabályoknak és az EJEE-nek.

([208]) Lásd például az M kontra the Chief Constable of Sussex Police ügyet (2019 EWHC 975 (Admin)), amelyben a Legfelsőbb Bíróságot arra kérték, hogy fontolja meg az adatok megosztását a rendőrség és az üzleti bűncselekmények visszaszorítását célzó partnerség (Business Crime Reduction Partnership - BCRP) között, amely szervezet felhatalmazást kapott a kitiltási értesítési rendszer kezelésére, megtiltva személyeknek tagjaik üzleti helyiségeibe való belépést. A bíróság felülvizsgálta az adatmegosztást, amely a lakosság védelme és a bűncselekmények megelőzése céljából létrejött megállapodás alapján zajlott, és végül arra a következtetésre jutott, hogy az adatmegosztás legtöbb vonatkozása jogszerű volt, a rendőrség és a BCRP között megosztott néhány különleges adat kivételével. Egy másik példa a Cooper kontra NCA ügy (2019 EWCA Civ 16), amelyben a fellebbviteli bíróság helybenhagyta az adatok rendőrség és a Súlyos Szervezett Bűnözés Elleni Ügynökség (SOCA, amely egy bűnüldöző szerv, amely jelenleg az NCA része) között megosztását.

([209]) A 2018. évi adatvédelmi törvény 36. szakaszának (4) bekezdése.

([210]) A terrorizmus elleni 2008. évi törvény a következő linken érhető el: https://www.legislation.gov.uk/ukpga/2008/28/section/19

([211]) A hírszerző ügynökségekről szóló 1994. évi törvény a következő linken érhető el: https://www.legislation.gov.uk/ukpga/1994/13/contents

([212]) A biztonsági szolgálatokról szóló 1989. évi törvény a következő linken érhető el: https://www.legislation.gov.uk/ukpga/1989/5/contents

([213]) A hírszerző ügynökségekről szóló 1994. évi törvény 2. szakaszának (2) bekezdése kimondja, hogy „A hírszerző ügynökség vezetője felelős a szolgálat hatékonyságáért, és kötelessége gondoskodni arról, hogy a) azt biztosító szabályozás legyen érvényben, hogy a hírszerző ügynökség ne gyűjtsön olyan adatokat, amelyek a feladatai megfelelő ellátásához nem szükségesek, és hogy semmiféle információt ne hozzon nyilvánosságra, kivéve ha az szükséges i. feladatai megfelelő ellátásának céljából; ii. a nemzetbiztonság érdekében; iii. súlyos bűncselekmények megelőzése vagy felderítése céljából; vagy a) bármely büntetőeljárás céljaira; és b) a hírszerző ügynökség ne tegyen semmilyen lépést az Egyesült Királyság valamely politikai pártja érdekeinek érvényre juttatása érdekében", míg a biztonsági szolgálatokról szóló 1989. évi törvény 2. szakaszának (2) bekezdése kimondja, hogy „A főigazgató felelős a szolgálat hatékonyságáért, és kötelessége biztosítani, hogy a) azt biztosító szabályozás legyen érvényben, hogy a szolgálat ne gyűjtsön olyan adatokat, amelyek a feladatai megfelelő ellátásához nem szükségesek, és hogy semmiféle információt ne hozzon nyilvánosságra, kivéve, ha ez súlyos bűncselekmények megelőzése vagy felderítése, vagy bármely büntetőeljárás céljából szükséges; és b) a szolgálat ne tegyen semmilyen lépést az Egyesült Királyság valamely politikai pártja érdekeinek érvényre juttatása érdekében; és c) a Nemzeti Bűnügyi Ügynökség főigazgatójával egyeztetett szabályozás létezzen a szolgálat tevékenységének e törvény 1. szakasza (4) bekezdésének megfelelően a rendőrség, a Nemzeti Bűnügyi Ügynökség tevékenységével és más bűnüldöző szervek tevékenységével történő összehangolására".

(150) Amennyiben az illetékes hatóság meg kívánja osztani a 2018. évi adatvédelmi törvény 3. része alapján kezelt személyes adatokat egy harmadik ország bűnüldöző hatóságaival, külön követelmények érvényesülnek ([214]). Ilyen adattovábbításokra akkor kerülhet sor, amennyiben azok a miniszter megfelelőségi rendeletein alapulnak, vagy ezek hiányában megfelelő biztosítékokról kell gondoskodni. A 2018. évi adatvédelmi törvény 75. szakasza előírja, hogy megfelelő biztosítékok vannak érvényben, ha azt a címzettre kötelező érvényű jogi aktus állapítja meg, vagy ha az adatkezelő – miután értékelte az említett típusú személyes adatok harmadik országba vagy nemzetközi szervezetbe történő továbbításával kapcsolatos összes körülményt – arra a következtetésre jut, hogy megfelelő biztosítékok léteznek az adatok védelmére.

(151) Ha az adattovábbítás nem megfelelőségi rendeleten vagy megfelelő biztosítékokon alapul, akkor arra csak bizonyos, meghatározott körülmények között kerülhet sor, amelyeket „kivételes körülményeknek" nevezünk ([215]). Ez a helyzet áll fen, ha az adattovábbítás az alábbiak miatt szükséges: a) az érintett vagy egy másik személy létfontosságú érdekeinek védelme érdekében; b) az érintett jogos érdekeinek biztosításához; c) valamely tagállam vagy harmadik ország közbiztonságát közvetlenül és komolyan fenyegető veszély elhárítása érdekében szükséges; d) egyedi esetekben bármely bűnüldözési célból; vagy e) egyedi esetekben jogi célból (például jogi eljárásokkal vagy jogi tanács kikérésével kapcsolatban). Megjegyzendő, hogy a d) és e) pont nem alkalmazandó, ha az érintett jogai és szabadságai felülírják az adattovábbítással kapcsolatos közérdeket. Ezek a körülmények megfelelnek az (EU) 2016/680 irányelv 38. cikke alapján „eltérésnek" minősülő kivételes eseteknek és feltételeknek.

(152) Emellett, amennyiben a bűnüldöző hatóságok által a lehallgatás vagy a berendezés zavarásának használatát engedélyező határozat alapján megszerzett anyagot harmadik országnak adják át, a nyomozati hatáskörökről szóló 2016. évi törvény további biztosítékokat ír elő. Különösen az említett, „tengerentúli közlésként" meghatározott közlés csak akkor engedélyezett, ha a kibocsátó hatóság úgy ítéli meg, hogy olyan speciális megfelelő intézkedések vannak érvényben, amelyek korlátozzák azoknak a személyeknek a számát, akikkel az adatokat közlik, illetve az anyagok közlésének vagy hozzáférhetővé tételének mértékét, valamint bármely anyag lemásolásának mértékét és az elkészített másolatok számát. Ezenkívül a kiállító hatóság úgy ítélheti meg, hogy megfelelő intézkedésekre van szükség annak biztosítására, hogy az anyag bármely részéből készült minden másolatot megsemmisítsék, amint annak megőrzésére már nincs releváns ok (ha korábban azt nem semmisítették meg) ([216]).

(153) Végül az Egyesült Királyságból az Egyesült Államokba történő újbóli adattovábbítás meghatározott formái a jövőben a 2019 októberében megkötött ([217]), a Nagy-Britannia és Észak-Írország Egyesült Királyságának kormánya és az Amerikai Egyesült Államok kormánya közötti, az elektronikus adatokhoz a súlyos bűncselekmények elleni küzdelem céljából történő hozzáférésről szóló megállapodás (az „Egyesült Királyság – Egyesült Államok megállapodás" vagy „Megállapodás") ([218]) alapján történhetnek. Noha az Egyesült Királyság és az Egyesült Államok közötti megállapodás e határozat elfogadásakor még nem lépett hatályba, annak előreláthető hatálybalépése befolyásolhatja a határozat alapján először az Egyesült Királyságba továbbított adatok az Egyesült Államokba történő újbóli továbbítását. Pontosabban, az EU-ból az egyesült királyságbeli szolgáltatóknak továbbított adatokra az Egyesült Államok illetékes bűnüldöző hatóságai által kiadott, elektronikus bizonyítási végzései vonatkozhatnak, amelyeket az Egyesült Királyságban a megállapodás hatálybalépése után juttathatnak érvényre. Ezen okok miatt releváns e határozat szempontjából azoknak a feltételeknek és biztosítékoknak az értékelése, amelyek mellett az említett végzéseket ki lehet adni és végre lehet hajtani.

([214]) Lásd a 2018. évi adatvédelmi törvény 3. részének 5. fejezetét.

([215]) A 2018. évi adatvédelmi törvény 76. szakasza.

([216]) A nyomozati hatáskörökről szóló 2016. évi törvény 54. és 130. szakasza. A kiállító hatóságoknak mérlegelniük kell a külföldi hatóságoknak átadott anyagokra vonatkozó különleges biztosítékok bevezetésének szükségességét annak biztosítása érdekében, hogy az adatokra az adatok megőrzése, megsemmisítése és közlése tekintetében hasonló védelem vonatkozzon, mint amelyet a nyomozati hatáskörökről szóló 2016. évi törvény 53. és 129. szakasza előír.

([217]) Ez az első megállapodás, amelyet az Egyesült Államok a Clarifying Lawful Overseas Use of Data (CLOUD) Act elnevezésű, az adatok jogszerű tengerentúli felhasználásáról szóló CLOUD törvény alapján kötött. Az Egyesült Államok CLOUD törvénye egy 2018. március 23-án elfogadott szövetségi törvény, amely az 1986. évi, Stored Communications Act elnevezésű, a tárolt kommunikációról szóló törvény módosítása révén pontosítja, hogy az amerikai szolgáltatók kötelesek teljesíteni az egyesült államokbeli, tartalmi és a nem tartalmi adatok közlésére vonatkozó végzéseket, függetlenül az említett adatok tárolási helyétől. A CLOUD törvény lehetővé teszi végrehajtási megállapodások megkötését külföldi kormányokkal is, amelyek alapján az amerikai szolgáltatók képesek lesznek tartalmi adatokat közvetlenül ezeknek a külföldi kormányoknak eljuttatni (a CLOUD törvény szövege a következő linken érhető el: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

([218]) Megállapodás Nagy-Britannia és Észak-Írország Egyesült Királyságának kormánya és az Amerikai Egyesült Államok kormánya között az elektronikus adatokhoz a súlyos bűncselekmények elleni küzdelem céljából történő hozzáférésről, elérhető a következő linken: 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

(154) Ebben a tekintetben meg kell jegyezni, hogy először is tárgyi hatályát tekintve a megállapodás csak olyan bűncselekményekre alkalmazandó, amelyek felső büntetési tétele legalább három évig terjedő szabadságvesztés („súlyos bűncselekmény" definíciója) ([219]), beleértve a „terrorista tevékenységet" is. Másodszor a másik joghatóságban kezelt adatok e megállapodás alapján csak akkor szerezhetők be, ha „a végzés végrehajthatóságáról egy bíróság, bíró, békebíró vagy más független hatóság előzetes vagy a rendelet végrehajtására vonatkozó eljárásokban […] a kibocsátó fél belső joga szerint felülvizsgálható vagy felügyelhető végzést hoz" ([220]). Harmadszor, minden végzésnek „észszerű indokok követelményein kell alapulnia, amelyek a vizsgált magatartás egyértelmű és hiteles tényállásán, sajátosságain, jogszerűségén és súlyosságán alapulnak" ([221]) és „meghatározott számlákra kell irányulnia, valamint meg kell jelölnie egy adott személyt, fiókot, címet vagy személyes eszközt, vagy bármilyen más egyedi azonosítót" ([222]). Negyedszer, az e megállapodás alapján nyert adatok az úgynevezett „EU – USA keretmegállapodás" által biztosított különleges biztosítékokkal egyenértékű védelemben részesülnek ([223]) – ez egy átfogó adatvédelmi megállapodás, amelyet az EU és az Egyesült Államok 2016 decemberében kötött, és amely meghatározza az adattovábbításra alkalmazandó biztosítékokat és jogokat a bűnüldözési együttműködés területén –, amelyeket hivatkozásként beépítettek e megállapodásba *mutatis mutandis* alapon, nevezetesen az adattovábbítások sajátos jellegének (azaz a magánszolgáltatóktól a bűnüldöző szervekhez történő adattovábbításokat, nem pedig a bűnüldöző hatóságok közötti adattovábbításokat) ([224]) figyelembevételére. Az Egyesült Királyság – Egyesült Államok megállapodás kifejezetten előírja, hogy az EU – USA keretmegállapodásban foglaltakkal egyenértékű védelmet alkalmaznak „minden olyan személyes adatra, amelyet a Megállapodás hatálya alá tartozó végzések végrehajtása során hoztak létre azonos védelem elérése céljából" ([225]).

(155) Az Egyesült Államok hatóságainak az Egyesült Királyság – Egyesült Államok megállapodás alapján továbbított adatoknak ezért részesülniük kell egy uniós jogi eszköz által biztosított védelemből, a szóban forgó adattovábbítások jellegének megjelenítéséhez szükséges kiigazításokkal. Az Egyesült Királyság hatóságai megerősítették továbbá, hogy a keretmegállapodás oltalma minden, a megállapodás alapján előállított vagy megőrzött személyes adatra vonatkozik, függetlenül a kérelmet benyújtó szerv jellegétől vagy típusától (pl. az Egyesült Államok szövetségi és állami rendvédelmi hatóságai egyaránt lehetnek), így minden esetben egyenértékű védelmet kell biztosítani. Az Egyesült Királyság hatóságai azonban azt is kifejtették, hogy az adatvédelmi biztosítékok konkrét végrehajtásának részleteiről az Egyesült Királyság és az Egyesült Államok még mindig megbeszéléseket folytatnak. Az Európai Bizottság szolgálataival erről a határozatról folytatott tárgyalások keretében az Egyesült Királyság hatóságai megerősítették, hogy csak akkor engedik a Megállapodást hatályba lépni, ha meg vannak győződve arról, hogy annak végrehajtása megfelel az abban előírt jogi kötelezettségeknek, beleértve az e megállapodás alapján kért adatokra vonatkozó adatvédelmi előírásoknak való megfelelés egyértelműségét. Mivel a Megállapodás lehetséges hatálybalépése hatással lehet az e határozatban értékelt védelmi szintre, az Egyesült Királyságnak a lehető leghamarabb, de mindenképpen a Megállapodás hatályba lépése előtt tájékoztatnia kell az Európai Bizottságot arról, hogy az Egyesült Államok milyen módon fogja teljesíteni a Megállapodás szerinti kötelezettségeit, e határozat megfelelő, az (EU) 2016/679 rendelet 45. cikkének (4) bekezdésével összhangban történő nyomon követésének biztosítása érdekében. Különös figyelmet fordítanak a keretmegállapodás garanciáinak az Egyesült Királyság – Egyesült Államok megállapodás hatálya alá tartozó adattovábbítások konkrét típusaira alkalmazására és azokhoz hozzáigazítására.

(156) Általánosságban elmondható, hogy a Megállapodás hatálybalépésével és alkalmazásával kapcsolatos minden lényeges fejleményt megfelelően figyelembe vesznek e határozat folyamatos nyomon követése során, ideértve azokat a következményeket is, amelyeket minden arra utaló jelzés esetén le kell vonni, hogy a lényegében azonos szintű védelem már nem biztosított.

3.2.3. *Felügyelet*

(157) Attól függően, hogy az illetékes hatóságok milyen jogköröket vesznek igénybe a személyes adatok bűnüldözési célú feldolgozása során (akár a 2018. évi adatvédelmi törvény, akár a nyomozati hatáskörökről szóló 2016. évi törvény alapján), különböző testületek biztosítják e hatáskörök felhasználásának felügyeletét. Az információügyi biztos felügyeli különösen a személyes adatok kezelését, amennyiben az a 2018. évi adatvédelmi törvény 3. részének

([219]) A Megállapodás 1. cikkének (14) bekezdése.
([220]) A Megállapodás 5. cikkének (2) bekezdése.
([221]) A Megállapodás 5. cikkének (1) bekezdése.
([222]) A Megállapodás 4. cikkének (5) bekezdése. A valós idejű lehallgatásra egy további és szigorúbb mérce vonatkozik: a végzéseknek korlátozott időtartamúnak kell lenniük, amely nem lehet hosszabb annál, ami a megbízás céljainak megvalósításához észszerűen szükséges, és csak akkor adhatók ki, ha ugyanazt az információt kevésbé tolakodó módszerrel nem lehetett észszerűen megszerezni (a Megállapodás 5. cikkének (3) bekezdése).
([223]) Megállapodás az Amerikai Egyesült Államok és az Európai Unió közötti, a bűncselekmények megelőzésével, nyomozásával, felderítésével és a vádeljárás lefolytatásával kapcsolatos személyes adatok védelméről, HL L 336, 2016.12.10., 3. o., elérhető a következő linken: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:22016A1210(01)&from=HU
([224]) A Megállapodás 9. cikkének (1) bekezdése.
([225]) A Megállapodás 9. cikkének (1) bekezdése.

hatálya alá tartozik ([226]). A nyomozati hatásköröknek a nyomozati hatáskörökről szóló 2016. évi törvény szerinti felhasználására vonatkozó független és bírósági felügyeletet a Nyomozati Szervek Biztosának Hivatala (nyomozási biztos hivatala) biztosítja ([227]) (ezt a részt a (250)–(255) preambulumbekezdés tárgyalja). Ezenkívül a további felügyeletet a Parlament, valamint más szervek garantálják.

3.2.3.1. A 2018. évi adatvédelmi törvény 3. részére vonatkozó felügyelet

(158) Az információügyi biztos általános feladatairól – függetlenségét és szervezetét a (87) preambulumbekezdés ismerteti – a 2018. évi adatvédelmi törvény 13. melléklete rendelkezik a 2018. évi adatvédelmi törvény 3. részének hatálya alá tartozó személyes adatok kezelésével kapcsolatban. Az információügyi biztos fő feladata a 2018. évi adatvédelmi törvény 3. részének figyelemmel kísérése és betartatása, valamint a közvélemény tudatosságának elősegítése, a Parlament, a kormány és más intézmények és szervek részére történő tanácsadás. Az igazságszolgáltatás függetlenségének fenntartása érdekében az információügyi biztos nem jogosult feladatait a személyes adatok bírói minőségben eljáró egyén, vagy bírósági minőségében eljáró bíróság vagy törvényszék általi kezelésével kapcsolatban ellátni. Ilyen körülmények között más szervek látják el a felügyeleti feladatokat, ahogyan azt a (99)–(103) preambulumbekezdés kifejti.

(159) A biztos általános nyomozati, korrekciós, engedélyezési és tanácsadói hatáskörrel rendelkezik azon személyes adatok kezelésével kapcsolatban, amelyekre a 3. rész vonatkozik. A biztos hatáskörrel rendelkezik arra, hogy értesítse az adatkezelőt vagy az adatfeldolgozót a 2018. évi adatvédelmi törvény 3. részének állítólagos megsértéséről, figyelmeztetéseket vagy megrovást adjon ki olyan adatkezelőnek vagy adatfeldolgozónak, amely megsértette a törvény 3. részének rendelkezéseit, saját kezdeményezésére vagy kérésre véleményeket ad ki a Parlamentnek, a kormánynak vagy más intézményeknek és szerveknek, valamint a lakosságnak a személyes adatok védelmével kapcsolatos bármely kérdésben ([228]).

(160) Ezenkívül a biztos hatáskörrel rendelkezik adatkérési felhívások ([229]), vizsgálati felhívások ([230]) és jogérvényesítési felhívások ([231]) kiadására, valamint az adatkezelők és az adatfeldolgozók dokumentumaihoz való hozzáférésre, a helyiségeikbe való belépésre ([232]), és közigazgatási bírságok bírságértesítők formájában történő kiszabására ([233]). A biztos szabályozási cselekvési politikája meghatározza azokat a körülményeket, amelyek mellett adatkérési, vizsgálati, jogérvényesítési felhívásokat és bírságértesítőket ad ki ([234]) (lásd még a (93) preambulumbekezdést és az (EU) 2016/680 irányelv szerinti megfelelőségi határozat (101)–(102) preambulumbekezdését).

(161) Legfrissebb éves jelentései szerint (2018–2019 ([235]), 2019–2020 ([236])), az információügyi biztos számos vizsgálatot folytatott és végrehajtási intézkedéseket hozott a bűnüldöző hatóságok által végzett adatkezeléssel kapcsolatban. Például a biztos vizsgálatot folytatott és 2019 októberében véleményt tett közzé az arcfelismerési technológia nyilvános helyeken, bűnüldözési céllal történő használatáról. A vizsgálat különösen az élő arcfelismerő funkciók dél-walesi rendőrség és a Fővárosi Rendőrség (MPS) általi használatára összpontosított. Az információügyi biztos megvizsgálta az MPS „bandamátrixát" is ([237]) és az adatvédelmi jogszabályok súlyos megsértését állapította meg, amely valószínűleg gyengíti a mátrixba és az adatok felhasználásának módjába vetett bizalmát. 2018 novemberében az információügyi biztos jogérvényesítési felhívást adott ki, és az MPS ezt követően megtette a szükséges lépéseket a biztonság és az

([226]) A 2018. évi adatvédelmi törvény 116. szakasza.
([227]) Lásd a nyomozati hatáskörökről szóló 2016. évi törvényt, és különösen a 8. rész 1. fejezetét.
([228]) A 2018. évi adatvédelmi törvény 13. mellékletének 2. pontja.
([229]) Az adatkezelő és az adatfeldolgozó (és bizonyos körülmények között bármely más személy) számára a szükséges információk megadásának elrendelése (a 2018. évi adatvédelmi törvény 142. szakasza).
([230]) Vizsgálat és ellenőrzés végzésének lehetővé tétele, amelyben elrendelhető az adatkezelő vagy az adatfeldolgozó számára, hogy engedélyezze a biztos számára a belépést meghatározott helyiségekbe, dokumentumok vagy berendezések megtekintését vagy vizsgálatát, a személyes adatokat az adatkezelő nevében feldolgozó személyek kihallgatását (a 2018. évi adatvédelmi törvény 146. szakasza).
([231]) A korrekciós hatáskör gyakorlásának engedélyezése, amely szerint megkövetelheti az adatkezelőktől/adatfeldolgozóktól meghatározott lépések megtételét, vagy azoktól való tartózkodást (a 2018. évi adatvédelmi törvény 149. szakasza).
([232]) A 2018. évi adatvédelmi törvény 154. szakasza.
([233]) A 2018. évi adatvédelmi törvény 155. szakasza.
([234]) Szabályozási cselekvési politika, lásd a 96. lábjegyzetet.
([235]) Az információügyi biztos 2018–19-as éves jelentése és pénzügyi kimutatásai (lásd a 101. lábjegyzetet).
([236]) Az információügyi biztos 2019-20-as éves jelentése és pénzügyi kimutatásai (lásd a 82. lábjegyzetet).
([237]) Adatbázis, amelyben rögzítették a feltételezett bandatagokkal és a bandához kapcsolható bűncselekmények áldozataival kapcsolatban szerzett információkat.

elszámoltathatóság növelése, valamint az adatok arányos felhasználásának biztosítása érdekében. A területen a legutóbbi jogérvényesítési intézkedésekre másik példa egy 325 000 GBP összegű bírság, amelyet a biztos 2018 májusában bocsátott ki a Crown Prosecution Service (királyi ügyészség) ellen, a rendőrségi kihallgatásokat tartalmazó titkosítatlan DVD-k elvesztése miatt. Az információügyi biztos tágabb témákban is folytatott vizsgálatokat, például 2020 első felében a mobiltelefonból kinyert adatok rendészeti célokra történő felhasználásáról és az áldozatok adatainak rendőrség általi kezeléséről. Ezenkívül a biztos jelenleg folytat vizsgálatot egy ügyben, amelynek tényállása szerint a bűnüldöző hatóságok hozzáférnek egy magánszektorbeli szervezet, a Clearview AI Inc. birtokában lévő adatokhoz ([238]).

(162) Az információügyi biztos (160) és (161) preambulumbekezdésben említett végrehajtási hatáskörein túl az adatvédelmi jogszabályok bizonyos megsértései bűncselekménynek minősülnek, ezért büntetőjogi szankciókkal sújthatók (a 2018. évi adatvédelmi törvény 196. szakasza). Ez vonatkozik például a személyes adatok adatkezelő hozzájárulása nélküli gyűjtésére, közlésére vagy megtartására, valamint más személy megbízása a személyes adatok adatkezelő hozzájárulása nélküli közlésével ([239]); az anonimizált személyes adatnak minősülő információk újbóli azonosítása a személyes adatok anonimizálásáért felelős adatkezelő hozzájárulása nélkül ([240]); a biztos szándékos akadályozására abban, hogy gyakorolja a személyes adatok nemzetközi kötelezettségekkel összhangban történő ellenőrzésével kapcsolatos hatáskörét ([241]), hamis állítások megtételére az adatkérési felhívásra adott válaszul, vagy információk megsemmisítésére az adatkérési és vizsgálati felhívások kapcsán ([242]).

3.2.3.2. Egyéb felügyeleti szervek a bűnüldözés területén

(163) Az információügyi biztoson kívül a bűnüldözés területén több felügyeleti szerv is működik, amelyeknek az adatvédelmi kérdésekre vonatkozó konkrét megbízása van. Idetartozik például a biometrikus anyagok megőrzéséért és felhasználásáért felelős biztos (a továbbiakban: biometriáért felelős biztos) ([243]) és a térfigyelő kamerák biztosa ([244]).

3.2.3.3. Parlamenti felügyelet a bűnüldözés területén

(164) A Belügyi Választott Bizottság (HASC) biztosítja a parlamenti felügyeletet a bűnüldözés területén. Ez a bizottság 11 képviselőből áll, akiket a három legnagyobb politikai párt képviselői közül választanak. A bizottság feladata a Belügyminisztérium és a kapcsolódó állami szervek – köztük a rendőrség és az NCA (amelyek munkáját a Bizottság külön megvizsgálhatja) – kiadásainak, adminisztrációjának és politikájának vizsgálata ([245]).

([238]) Lásd a biztos nyilatkozatát, amely a következő linken érhető el: 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]) A 2018. évi adatvédelmi törvény 170. szakasza.

([240]) A 2018. évi adatvédelmi törvény 171. szakasza.

([241]) A 2018. évi adatvédelmi törvény 119. szakaszának (6) bekezdése.

([242]) A 2019. április 1. és 2020. március 31. közötti időszakra eső pénzügyi évben a biztos vizsgálatai nyomán négy figyelmeztetést adtak és nyolc büntetőeljárást indítottak. Ezekkel az ügyekkel szemben az 1998. évi adatvédelmi törvény 55. szakasza, az információszabadságról szóló 2000. évi törvény 77. szakasza és a 2018. évi adatvédelmi törvény 170. szakasza alapján indult büntetőeljárás. Az ügyek 75 %-ában a vádlottak vádalkut kötöttek, ellenezve az elhúzódó tárgyalások szükségességét és a kapcsolódó költségeket. (Az információügyi biztos 2019/2020-as éves jelentése és pénzügyi kimutatásai, lásd a 87. lábjegyzetet, 40. oldal).

([243]) A biometriáért felelős biztost a szabadságjogok védelméről szóló 2012. évi törvény hozta létre (lásd: https://www.legislation.gov.uk/ukpga/2012/9/contents). Egyéb feladatai mellett a biometriáért felelős biztos dönt, hogy a rendőrség megőrizheti-e a letartóztatott, de nem a megőrzésre feljogosító bűncselekménnyel vádolt személyektől nyert DNS-profil iratokat és ujjlenyomatokat (az 1984. évi rendőrségi törvény 63G. szakasza). Ezenkívül a biometriáért felelős biztos általános felelőssége a DNS és az ujjlenyomatok megőrzésének és felhasználásának, valamint nemzetbiztonsági okokból történő megőrzésének folyamatos felülvizsgálata (a szabadságjogok védelméről szóló 2012. évi törvény 20. szakaszának (2) bekezdése). A biometriáért felelős biztost a Code for Public Appointments elnevezésű (az állami kinevezések kódexéről szóló) törvény szerint nevezik ki (a kódex a következő linken érhető el: https://www.gov.uk/government/publications/governance-code-for-public-appointments) és kinevezési feltételei egyértelművé teszik, hogy a belügyminiszter csak szűkkörűen meghatározott körülmények esetén mozdíthatja el hivatalából; idetartozik, ha kötelességei három hónapon át nem teljesíti, bűncselekmény miatt elítélik vagy kinevezésének feltételeit nem tartja be.

([244]) A térfigyelő kamerák biztosát a szabadságjogok védelméről szóló 2012. évi törvény hozta létre, feladata a megfigyelő kamerák gyakorlati kódexének való megfelelés ösztönzése; e kódex működésének felülvizsgálata; valamint tanácsadás a minisztereknek arról, hogy szükséges-e a kódex módosítása. A biztos kinevezése ugyanazon szabályok szerint történik, mint a biometriáért felelős biztosoké, és hasonló hatáskörök, források és elmozdítás elleni védelem illeti meg.

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

(165) A bizottság hatáskörének keretein belül kiválaszthatja vizsgálatának tárgyát, beleértve a konkrét eseteket is, amennyiben a kérdés nem áll elbírálás alatt. A bizottság írásbeli és szóbeli bizonyítékokat is kérhet az érintett csoportok és egyének széles körétől. Jelentéseket készít megállapításairól és ajánlásokat ad a kormánynak ([246]). A kormánytól elvárt a jelentés egyes ajánlásaira való reagálás, és 60 napon belül válaszolnia kell ([247]).

(166) A felügyelet területén a bizottság jelentést készített a Regulation of Investigatory Powers Act 2000 elnevezésű (a nyomozati hatáskörök szabályozásáról szóló 2000. évi) törvényről is ([248]), amely megállapította, hogy a nyomozati hatáskörök (Skócia) szabályozásáról szóló 2000. évi törvény nem alkalmas a céljára. Jelentésüket figyelembe vették a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény jelentős részeinek a nyomozati hatáskörökről szóló 2016. évi törvénnyel való felváltása során. A vizsgálatok teljes listája megtalálható a bizottság honlapján ([249]).

(167) A HASC feladatait Skóciában a Rendészeti Igazságügyi Albizottság, Észak-Írországban pedig az Igazságügyi Bizottság látja el ([250]).

3.2.4. *Jogorvoslat*

(168) A bűnüldöző hatóságok általi adatkezelés tekintetében jogorvoslati mechanizmusok a 2018. évi adatvédelmi törvény 3. része és a nyomozati hatáskörökről szóló 2016. évi törvény, valamint az 1998. évi emberi jogi törvény alapján állnak rendelkezésre.

(169) Ezek a mechanizmusok hatékony adminisztratív és bírósági jogorvoslati lehetőségeket biztosítanak az érintetteknek, lehetővé téve számukra különösen jogaik, többek között a személyes adatokhoz való hozzáférés joga, illetve az említett adatok helyesbíttetésére vagy töröltetésére vonatkozó joguk biztosítását.

(170) Először is, a 2018. évi adatvédelmi törvény 165. szakasza értelmében az érintettnek joga van panaszt benyújtani az információügyi biztoshoz, ha az érintett úgy ítéli meg, hogy a rá vonatkozó személyes adatokkal kapcsolatban megsértették a 2018. évi adatvédelmi törvény 3. részét ([251]). Az információügyi biztos hatáskörébe tartozik annak értékelése, hogy az adatkezelő és az adatfeldolgozó megfelel-e a 2018. évi adatvédelmi törvénynek, megkövetelheti tőlük, hogy meg nem felelés esetén tegyék meg a szükséges lépéseket, és bírságot szab ki.

([246]) A választott bizottságokra – beleértve a Belügyi Választott Bizottságot is – az alsóház eljárási szabályzata vonatkozik. Az eljárási szabályzat az alsóház által elfogadott, a parlament tevékenységét szabályozó szabályzat. A választott bizottságok feladatai széles körűek, az eljárási szabályzat 152. cikkének (1) bekezdése előírja, hogy a „választott bizottságokat az e szabályzat (2) pontjában meghatározott fő kormányzati szervek és a kapcsolódó állami szervek kiadásainak, adminisztrációjának és politikájának vizsgálatára kell kijelölni." Ez lehetővé teszi a Belügyi Választott Bizottság számára, hogy megvizsgálja a Belügyminisztérium által irányított politikákat, amelyek részét képezik a nyomozati hatáskörökre vonatkozó irányelvek (és a kapcsolódó jogszabályok). Ezenkívül az eljárási szabályzat 152. cikkének (4) bekezdése egyértelművé teszi, hogy a bizottságoknak különféle hatásköreik vannak, beleértve azt a lehetőséget, hogy személyeket kérjenek fel egy adott kérdésben tanúvallomás tételére vagy dokumentumok benyújtására és jelentések készítésére. A bizottság jelenlegi és korábbi vizsgálatai a következő linken érhetők el https://committees.parliament.uk/committee/83/home-affairs-committee/.

([247]) Az angliai és walesi Belügyi Választott Bizottság hatásköreit az alsóház eljárási szabályzata rögzíti, amely a következő linken érhető el: https://www.parliament.uk/business/publications/commons/standing-orders-public11/

([248]) Elérhető az alábbi linken: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm

([249]) Elérhető az alábbi linken: https://committees.parliament.uk/committee/83/home-affairs-committee

([250]) A skóciai rendőrség igazságügyi albizottságának szabályzata a következő linken található: https://www.parliament.scot/parliamentarybusiness/CurrentComm Communities/justice-committee.aspx, Észak-Írország Igazságügyi Bizottságának szabályzata a következő linken található: http://www.niassembly.gov.uk/assembly-business/standing-orders/

([251]) A biztos legutóbbi éves jelentése részletezi a beérkezett és lezárt panaszok jellegét. Különösen a „rendőrségi és bűnügyi nyilvántartás" miatt beérkezett panaszok száma a kapott panaszok teljes számának 6 %-át teszi ki (az előző pénzügyi évhez képest 1 %-os növekedéssel). Az éves jelentés azt is mutatja, hogy az érintettek hozzáférési kérelmeivel kapcsolatos panaszok képviselik a legnagyobb számot (a panaszok teljes számának 46 %-a, az előző pénzügyi évhez képest 8 %-os növekedés) (az információügyi biztos 2019–2020.évi éves jelentése, 55. oldal; lásd a 88. lábjegyzetet).

(171) Másodszor, a 2018. évi adatvédelmi törvény jogot biztosít az információügyi biztossal szembeni jogorvoslatra, ha nem kezeli megfelelően az érintett panaszát. Konkrétan, ha a biztos nem „halad” ([252]) az érintett által benyújtott panasz ügyével, a panaszost bírósági jogorvoslat illeti meg, mivel a First Tier Tribunal ([253]) előtt kérheti a biztos arra kötelezését, hogy tegye meg a megfelelő lépéseket a panasz elintézésére, vagy tájékoztassa a panaszost a panasz állásáról ([254]). Ezenkívül bárki, aki a biztostól az említett bármelyik felhívást (adatkérési, vizsgálati, jogérvényesítési felhívás vagy bírságértesítő) megkapja, fellebbezést nyújthat be a First Tier Tribunalhoz. Ha ez a bíróság úgy ítéli meg, hogy a biztos döntése nincs összhangban a jogszabályokkal, vagy az információügyi biztosnak másként kellett volna gyakorolnia mérlegelési jogkörét, akkor engedélyeznie kell a fellebbezést, vagy olyan másik felhívást vagy határozatot kell elfogadnia, amelyet az információügyi biztos elfogadhatott volna ([255]).

(172) Harmadszor: az egyének az adatkezelőkkel és az adatfeldolgozókkal szemben közvetlenül a bírósághoz fordulva is bírósági jogorvoslatot nyerhetnek. Különösen: a 2018. évi adatvédelmi törvény 167. szakasza értelmében az érintett kérelmet nyújthat be a bírósághoz az adatvédelmi jogszabályok szerinti jogának megsértése miatt, a bíróság pedig végzéssel kötelezheti az adatkezelőt, hogy fogadjon el lépéseket (vagy tartózkodjon lépések megtételétől) annak érdekében, hogy az adatkezelés megfeleljen a 2018. évi adatvédelmi törvénynek. Ezenkívül a 2018. évi adatvédelmi törvény 169. szakasza szerint minden olyan személy kártérítésre jogosult az adatkezelőtől vagy az adatfeldolgozótól, aki – az Egyesült Királyság általános adatvédelmi rendeletétől eltérő – adatvédelmi jogszabályok (ideértve a 2018. évi adatvédelmi törvény 3. részét) valamely követelményének megsértése miatt szenved kárt, kivéve, ha az adatkezelő vagy az adatfeldolgozó bizonyítja, hogy az adatkezelő vagy adatfeldolgozó semmilyen módon nem felelős a kárt okozó eseményért. A kártérítés kiterjed mind az anyagi veszteségre, mind a nem vagyoni kárra, például a sérelemre.

(173) Végül, aki úgy véli, hogy bármely hatóság megsértette jogait, beleértve a magánélethez és az adatvédelemhez való jogokat, az 1998. évi emberi jogi törvény alapján jogorvoslatot kérhet az Egyesült Királyság bíróságaitól ([256]), és a nemzeti jogorvoslatok kimerítése után a személy, nem kormányzati szervezet és egyének csoportjai jogorvoslatot nyerhetnek az Emberi Jogok Európai Bírósága előtt az Emberi Jogok Európai Egyezménye által garantált jogok megsértése miatt ([257]) (lásd a (111) preambulumbekezdésben).

3.2.4.1. A nyomozati hatáskörökről szóló 2016. évi törvény keretében rendelkezésre álló jogorvoslati mechanizmusok

(174) Az egyének az Investigatory Powers Tribunal előtt nyerhetnek jogorvoslatot a nyomozati hatáskörökről szóló 2016. évi törvény megsértése miatt. A nyomozati hatáskörökről szóló 2016. évi törvény keretében rendelkezésre álló jogorvoslati lehetőségeket a (263)–(269) below preambulumbekezdés ismerteti.

([252]) A 2018. évi adatvédelmi törvény 166. szakasza konkrétan az alábbi helyzetekre utal: a) a biztos nem tesz megfelelő intézkedéseket a panasz megválaszolására, b) a biztos nem ad a panaszosnak tájékoztatást a panasz állásáról vagy kimeneteléről a panasz biztos általi kézhezvételétől számított 3 hónapos időszak végéig, vagy c) ha a panasz biztos általi vizsgálata ebben az időszakban nem fejeződik be, a következő három hónapos időszak alatt nem ad tájékoztatást erről a panaszosnak.

([253]) A First Tier Tribunal a kormányzati szabályozó szervek által hozott határozatok elleni fellebbezések elintézésére illetékes bíróság. Az információügyi biztos döntése esetén az illetékes tanács az „Általános szabályozói tanács”, amelynek illetékessége az Egyesült Királyság egészére kiterjed.

([254]) A 2018. évi adatvédelmi törvény 166. szakasza. A biztos elleni a Közszolgálati Törvényszék előtt megnyert ügyekre példa az az ügy, amelyben a biztos nyugtázta az érintett panaszának kézhezvételét, de nem jelezte, hogy milyen lépéseket szándékozik megtenni, és ezért elrendelték, hogy erősítse meg 21 naptári napon belül, megvizsgálja-e a panaszokat, és ha igen, akkor azt követően legalább minden 21. naptári napon belül tájékoztassa a panaszost a vizsgálat előrehaladásáról (az ítéletet még nem tették közzé), és az az ügy, amelyben az Elsőfokú Törvényszék úgy vélte, hogy nem világos, hogy a biztos panaszosnak adott válasza megfelelő volt-e a panasz „kimeneteleként” (lásd: Susan Milne kontra információügyi biztos ügy (2020), a következő linken érhető el: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

([255]) A 2018. évi adatvédelmi törvény 162. és 163. szakasza.

([256]) Lásd például a Brown kontra Commissioner of Police of the Metropolis & Anor ügyet (2019 EWCA Civ 1724), amelyben az 1998. évi adatvédelmi törvény és az 1998. évi emberi jogi törvény alapján 9 000 GBP kártérítést ítéltek meg személyes adatok jogszerűtlen gyűjtése és azokkal való visszaélés miatt, és az R (Bridges kérelmére) kontra Chief Constable of South Wales ügyet (2020 EWCA Civ 1058), amennyiben a Court of Appeal jogellenesnek nyilvánította egy arcfelismerő rendszer walesi rendőrség általi kiépítését, mivel az az EJEE 8. cikkébe ütközött, és az adatkezelő által készített adatvédelmi hatásvizsgálat nem felelt meg a 2018. évi adatvédelmi törvénynek.

([257]) Az Emberi Jogok Európai Egyezményének 34. cikke előírja, hogy „A Bíróság kérelmeket vehet át bármely természetes személytől, nem-kormányzati szervezettől vagy személyek csoportjaitól, akik vagy amelyek azt állítják, hogy az Egyezményben vagy az ahhoz kapcsolódó jegyzőkönyvekben biztosított jogok valamely Magas Szerződő Fél részéről történt megsértésének áldozatai. A Magas Szerződő Felek kötelezettséget vállalnak arra, hogy semmilyen módon nem akadályozzák e jog hatékony gyakorlását”.

3.3. **Az egyesült királyságbeli közigazgatási szervek hozzáférése az adatokhoz és az adatok használata nemzetbiztonsági célokból**

(175) Az Egyesült Királyság jogrendjében a nemzetbiztonsági okokból az adatkezelők vagy adatfeldolgozók birtokában lévő elektronikus adatok gyűjtésére jogosult hírszerző ügynökség a megfelelőségi esetkör szempontjából releváns helyzetekben a Biztonsági Szolgálat ([258]) (MI5), a Titkosszolgálat ([259]) (SIS) és a Kormányzati Kommunikációs Központ ([260]) ([261]).

3.3.1. *Jogalapok, korlátok és biztosítékok*

(176) Az Egyesült Királyságban a hírszerző ügynökségek hatásköreit a nyomozati hatáskörökről szóló 2016. évi törvény és a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény rögzíti, amelyek a 2018. évi adatvédelmi törvénnyel együtt meghatározzák e hatáskörök tárgyi és személyi terjedelmét, illetve korlátokat és biztosítékokat írnak elő e hatáskörök gyakorlásához. Ezeket a hatásköröket, valamint a rájuk vonatkozó korlátozásokat és biztosítékokat a következő szakaszok részletesen értékelik.

3.3.1.1. A nemzetbiztonság keretében gyakorolt nyomozati hatáskörök

(177) A nyomozati hatáskörökről szóló 2016. évi törvény jogi keretet biztosít a nyomozati hatáskörök alkalmazásához, azaz hatáskört lehallgatásra, a kommunikációs adatokhoz való hozzáférésre és a berendezések zavarásának végrehajtására. A nyomozati hatáskörökről szóló 2016. évi törvény általános tilalmat vezet be és bűncselekménnyé teszi azokat a technikákat, amelyek jogszerű felhatalmazás nélkül hozzáférést tesznek lehetővé a kommunikáció tartalmához, hozzáférést a kommunikációs adatokhoz vagy a berendezéseket zavarják ([262]). Ez tükröződik abban a tényben is, hogy e nyomozati jogkörök csak akkor jogszerűek, ha azt parancs vagy engedély alapján hajtják végre ([263]).

(178) A nyomozati hatáskörökről szóló 2016. évi törvény részletes szabályokat állapít meg az egyes nyomozati hatáskörök terjedelmére és alkalmazására, valamint azok egyedi korlátaira és biztosítékaira. Különböző szabályok érvényesülnek a nyomozati hatáskör típusától (a kommunikáció lehallgatása, a kommunikációs

([258]) Az MI5 a belügyminiszter felügyelete alatt áll. A biztonsági szolgálatokról szóló 1989. évi törvény határozza meg az MI5 feladatait: a nemzetbiztonság védelme (ideértve a kémkedés, a terrorizmus és a szabotázs, a külföldi hatalmak képviselőinek tevékenységei, valamint a parlamenti demokrácia politikai, ipari vagy erőszakos intézkedésekkel történő megdöntése vagy gyengítése elleni védelmet), az Egyesült Királyság gazdasági jólétének védelme külső fenyegetések ellen, valamint a rendőrség és más bűnüldöző szervek tevékenységeinek támogatása a súlyos bűncselekmények megelőzése és felderítése terén.

([259]) A SIS a külügyminiszter felügyelete alatt áll, és funkcióit a hírszerzési szolgálatokról szóló 1994. évi törvény határozza meg. Feladata a Brit-szigeteken kívüli személyek cselekedeteivel vagy szándékaival kapcsolatos információk gyűjtése és továbbítása, valamint az említett személyek cselekedeteivel vagy szándékaival kapcsolatos egyéb feladatok ellátása. Ezek a funkciók csak a nemzetbiztonság, az Egyesült Királyság gazdasági jóléte vagy a súlyos bűncselekmények megelőzése vagy felderítése érdekében gyakorolhatók.

([260]) A GCHQ a külügyminiszter felügyelete alatt áll, és funkcióit a hírszerzési szolgálatokról szóló 1994. évi törvény határozza meg. Ezek a következők: a) az elektromágneses és egyéb kibocsátások, valamint az említett kibocsátást előidéző berendezések figyelemmel kísérése, hasznosítása vagy zavarása, az említett kibocsátásokból vagy berendezésekből, illetve a titkosított anyagokból származó vagy ezekhez kapcsolódó információk gyűjtése és továbbítása; b) nyelvi tanácsadás és segítségnyújtás, ideértve a műszaki kérdésekben és a rejtjelezésben használt terminológiát, valamint a fegyveres erők, a kormány vagy más megfelelőnek ítélt szervezetek vagy személyek számára az információk védelmével kapcsolatos egyéb kérdéseket. Ezeket a funkciókat csak a nemzetbiztonság érdekében, az Egyesült Királyság gazdasági jólétének érdekében, a Brit-szigeteken kívüli személyek cselekedeteivel vagy szándékaival összefüggésben, illetve a súlyos bűncselekmények megelőzésének vagy felderítésének támogatására lehet gyakorolni.

([261]) A nemzetbiztonság szempontjából fontos feladatokat ellátó egyéb állami szervek a Védelmi Hírszerzés (DI), a Nemzetbiztonsági Tanács és a Titkárság, a Közös Hírszerző Szervezet és a Hírszerzés Közös Bizottsága. Azonban sem a JIC, sem a JIO nem tudja kihasználni a nyomozati hatásköröket a nyomozati hatáskörökről szóló 2016. évi törvény keretében, míg a DI korlátozotton tudja hatásköreit használni.

([262]) A tilalom mind a nyilvános, mind a magán kommunikációs hálózatokra, valamint az állami postaszolgálatra vonatkozik, amennyiben a lehallgatást az Egyesült Királyságban végzik. A tilalom nem vonatkozik a magánhálózat adatkezelőjére, ha az adatkezelő kifejezett vagy hallgatólagos hozzájárulást kapott a lehallgatás végrehajtására (a nyomozati hatáskörökről szóló 2016. évi törvény 3. szakasza).

([263]) Bizonyos, korlátozott esetekben jogszerű lehallgatás parancs nélkül is lehetséges, azaz a küldő vagy a címzett hozzájárulásával történő lehallgatáskor (a nyomozati hatáskörökről szóló 2016. évi törvény 44. szakasza), korlátozott adminisztratív vagy végrehajtási célok esetén (a nyomozati hatáskörökről szóló törvény 45–48. szakasza), egyes különleges intézményekben (a nyomozati hatáskörökről szóló 2016. évi törvény 49–51. szakasza) és a tengerentúli kéréseknek megfelelően (a nyomozati hatáskörökről szóló 2016. évi törvény 52. szakasza).

adatok gyűjtése és megőrzése és a berendezés zavarása) ([264]), valamint attól függően, hogy a hatáskört egy meghatározott célpont tekintetében vagy tömegesen gyakorolják-e. A nyomozati hatáskörökről szóló 2016. évi törvény által előírt egyes intézkedések hatályát, biztosítékait és korlátozásait részletesen a lenti külön szakasz ismerteti.

(179) Emellett a nyomozati hatáskörökről szóló 2016. évi törvényt számos, a miniszter által kiadott, az Országgyűlés mindkét háza által jóváhagyott jogszabályi kódex egészíti ki ([265]) és az egész országban alkalmazható, útmutatót nyújtva e hatáskörök használatához ([266]). Míg az érintettek közvetlenül hivatkozhatnak jogaik gyakorlásához a nyomozati hatáskörökről szóló 2016. évi törvényben megállapított rendelkezésekre, a nyomozati hatáskörökről szóló 2016. évi törvény 7. mellékletének 5. pontja előírja, hogy a gyakorlati kódexek a polgári és büntetőeljárások során bizonyítékként elfogadhatók, és a bíróság, a törvényszék vagy a felügyeleti hatóság figyelembe veheti a kódexek be nem tartását a bírósági eljárásban a releváns kérdések meghatározásakor ([267]). Az Egyesült Királyság korábbi felügyeleti jogszabályainak, a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvénynek a jogszabályok minőségével kapcsolatos értékelése kapcsán az Emberi Jogok Európai Bíróságának nagytanácsa kifejezetten elismerte az Egyesült Királyság gyakorlati kódexeinek relevanciáját, és elfogadta, hogy rendelkezéseit figyelembe lehet venni a felügyeletet lehetővé tevő jogszabályok előreláthatóságának értékelésekor ([268]).

(180) Meg kell viszont jegyezni, hogy a célzott hatáskörök (célzott lehallgatás ([269]), kommunikációs adatok gyűjtése ([270]), kommunikációs adatok megőrzése ([271]) és a berendezések célzott zavarása ([272])) a nemzeti biztonsági ügynökségek és egyes bűnüldöző hatóságok számára elérhetők ([273]), míg tömeges hatásköröket (azaz a tömeges lehallgatást ([274]), a kommunikációs adatok tömeges gyűjtését ([275]), a berendezések tömeges zavarását ([276]) és a tömeges személyesadat-állományokat ([277])) csak a hírszerző ügynökségek vehetnek igénybe.

(181) Annak eldöntése során, hogy mely nyomozati jogkört kell használni, a hírszerző ügynökségnek eleget kell tennie a nyomozati hatáskörökről szóló 2016. évi törvény 2. szakasza (2) bekezdésének a) pontjában felsorolt, „a magánélet védelmével kapcsolatos általános kötelezettségeknek”, amelyek szükségességi és arányossági tesztet is tartalmaznak. Pontosabban, e rendelkezés értelmében a nyomozati hatáskört alkalmazni szándékozó hatóságnak meg kell

([264]) Ami például az ilyen intézkedések alkalmazási körét illeti, a 3. és a 4. részben (kommunikációs adatok megőrzése és megszerzése) az intézkedés terjedelme szigorúan kapcsolódik a „távközlési szolgáltatók” meghatározásához, amelyek felhasználóinak adatai képezik az intézkedés tárgyát. Másik példaként említhető a tömeges hatáskörök használata. Ebben az esetben e hatáskörök hatálya „a Brit-szigeteken kívül tartózkodó személyek által küldött vagy fogadott kommunikációra” korlátozódik.

([265]) A nyomozati hatáskörökről szóló 2016. évi törvény 7. melléklete meghatározza a kódexek alkalmazási körét, a kiadásuk során követendő eljárást, felülvizsgálatuk szabályait és a kódexek hatását.

([266]) A nyomozati hatáskörökről szóló 2016. évi törvény szerinti gyakorlati kódexek a következő linken érhetők el: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

([267]) A bíróságok a gyakorlati kódexeket használják a hatóságok magatartása jogszerűségének értékelésére. Lásd például: a Dias kontra Cleveland Police ügyet (2017 UKIPTrib15_586-CH), amelyben az Investigatory Powers Tribunal hivatkozott a kommunikációs adatok gyakorlati kódexének egyes szakaszaira, hogy megértse a „bűncselekmények megelőzésének vagy felderítésének vagy a rendellenességek megelőzésének” jogalapja fogalommeghatározását, amelyre a kommunikációs adatok gyűjtése kérelmezéséhez hivatkoztak. A kódexet belefoglalták az indokolásba annak megállapításához, hogy ezt a jogalapot helytelenül használták-e. A Bíróság arra a következtetésre jutott, hogy a vitatott magatartások jogellenesek voltak. A bíróságok értékelték a kódexekben rendelkezésre álló biztosítékok szintjét is, lásd például a Just for Law Kids kontra Secretary of State for the Home Department (2019 EWHC 1772 (Admin)) ügyet, amelyben a High Court megállapította, hogy az elsődleges és a másodlagos jogszabályok, valamint a belső útmutatók elegendő biztosítékot nyújtottak; vagy az R (National Council for Civil Liberties) kontra Secretary of State for the Home Department és társai ügyet (2019 EWHC 2057 (Admin)), amelyben megállapította, hogy a nyomozati hatáskörökről szóló 2016. évi törvény és a berendezések zavarásáról szóló gyakorlati kódex is elegendő rendelkezést tartalmazott a parancsok specifikusságának szükségességére vonatkozóan.

([268]) A Big Brother Watch ügyben, az Emberi Jogok Európai Bírósága megjegyezte, hogy „Az információügyi biztos kódexe nyilvános dokumentum, amelyet a Parlament mindkét háza jóváhagyott, és a kormány az interneten és nyomtatásban is közzétette, és amelyet mind a lehallgatási feladatokat ellátóknak, mind a bíróságoknak figyelembe kell venniük (lásd a fenti 93–94. pontot). Ennek következtében a Bíróság elfogadta, hogy rendelkezéseit figyelembe lehet venni a nyomozati hatáskörök szabályozásáról szóló törvény előreláthatóságának értékelésekor (lásd a fent idézett Kennedy-ügy 157. pontját). Ennek megfelelően a Bíróság elfogadta, hogy a nemzeti jog megfelelően „hozzáférhető” volt.” (lásd: Emberi Jogok Európai Bírósága (nagytanács), Big Brother Watch és társai kontra Egyesült Királyság, 58170/13., 62322/14. és 24960/15. sz. kérelem, 2021. május 25., 366. pont).

([269]) A nyomozati hatáskörökről szóló 2016. évi törvény 2. része.

([270]) A nyomozati hatáskörökről szóló 2016. évi törvény 3. része.

([271]) A nyomozati hatáskörökről szóló 2016. évi törvény 4. része.

([272]) A nyomozati hatáskörökről szóló 2016. évi törvény 5. része.

([273]) Azon bűnüldöző hatóságok listáját, amelyek a nyomozati hatáskörökről szóló 2016. évi törvény keretében célzott nyomozati hatásköröket alkalmazhatnak, lásd a (139) lábjegyzetben.

([274]) A nyomozati hatáskörökről szóló 2016. évi törvény 136. szakasza.

([275]) A nyomozati hatáskörökről szóló 2016. évi törvény 158. szakasza.

([276]) A nyomozati hatáskörökről szóló 2016. évi törvény 176. szakasza.

([277]) A nyomozati hatáskörökről szóló 2016. évi törvény 199. szakasza.

fontolnia, i. hogy a parancs, felhatalmazás vagy értesítés által elérni kívánt cél elérhető-e más, kevésbé beavatkozó jellegű eszközökkel; ii. hogy az információ különleges jellege miatt a parancs, felhatalmazás vagy felhívás alapján az információk gyűjtésével kapcsolatban alkalmazandó védelmi szint magasabb-e; iii. a távközlési rendszerek és a postai szolgáltatások integritásához és biztonságához fűződő közérdek, és iv. a magánélet védelméhez fűződő közérdek egyéb vonatkozásait ([278]).

(182) E kritériumok alkalmazási módját – és e hatáskörök használatának miniszter és a független igazságügyi biztosok általi engedélyezésének részeként megfelelésük értékelésének módját – a vonatkozó magatartási kódexek részletezik. Különösen bármely ilyen nyomozati hatáskör használatának mindig „arányban kell állnia az elérni kívánt céllal, [amely] magában foglalja a magánéletbe való beavatkozás súlyosságának (és a 2. szakasz (2) bekezdésében meghatározott egyéb szempontoknak) a tevékenység nyomozati, operatív vagy kapacitási szükségességével való kiegyensúlyozását". Ez különösen azt jelenti, hogy „reális esélyt kell kínálnia a várt haszon elérésére, és nem lehet aránytalan vagy önkényes", és „a magánéletbe való beavatkozást nem lehet arányosnak tekinteni, ha a kért információt észszerűen más, kevésbé beavatkozó jellegű eszközökkel is meg lehet szerezni" ([279]). Pontosabban, az arányosság elvének való megfelelést a következő kritériumok alapján kell értékelni: „i. a magánéletbe való javasolt beavatkozás mértéke az elérni kívánt célokhoz képest; ii. az alkalmazandó módszerek hogyan és miért okozzák a lehető legkevesebb beavatkozást a személy és mások számára; iii. a tevékenység a törvény megfelelő alkalmazása-e és az elérni kívánt cél elérésére észszerű mód-e, az összes észszerű alternatíva figyelembevételével; iv. adott esetben milyen egyéb módszereket nem hajtottak végre vagy alkalmaztak, de a javasolt nyomozati hatáskör igénybevétele nélkül elégtelennek ítélnek meg az operatív célok teljesítéséhez" ([280]).

(183) A gyakorlatban – amint azt az Egyesült Királyság hatóságai kifejtették – ez biztosítja, hogy egy hírszerző ügynökség először is meghatározza az operatív célt (ezáltal körülhatárolja az adatgyűjtést, pl. egy nemzetközi terrorizmusellenes cél egy adott földrajzi területen), másrészt pedig ezen operatív cél alapján meg kell vizsgálnia, hogy melyik technikai lehetőség (pl. célzott vagy tömeges lehallgatás, berendezés zavarása, kommunikációs adatok gyűjtése) a leginkább arányos (azaz a legkevésbé beavatkozó a magánéletbe [vö. a nyomozati hatáskörökről szóló törvény 2. szakaszának (2) bekezdésével]) és ezért engedélyezhető a rendelkezésre álló törvényi jogalapok valamelyike alapján.

(184) Érdemes megjegyezni, hogy a szükségesség és az arányosság mércéjére való támaszkodást az ENSZ magánélethez való joggal foglalkozó különleges előadója, Joseph Cannataci is megemlítette és üdvözölte, aki kijelentette a nyomozati hatáskörökről szóló 2016. évi törvény által létrehozott rendszerrel kapcsolatban, hogy „[ú]gy tűnik, hogy a hírszerző ügynökségeken és a bűnüldöző szerveken belül is érvényben lévő eljárások szisztematikusan megkövetelik a felügyeleti intézkedés vagy művelet szükségességének és arányosságának mérlegelését, mielőtt engedélyeztetésre ajánlanák, valamint annak ugyanazon alapon történő felülvizsgálatát ([281])". Megjegyezte azt is, hogy a bűnüldöző szervek és a nemzetbiztonsági ügynökségek képviselőivel folytatott találkozóján „[konszenzusos álláspontot látott] arról, hogy a magánélethez való jognak elsődleges szempontnak kell lennie a felügyeleti intézkedésekkel kapcsolatos döntések során. Mindannyian megértették és értékelték a szükségességet és az arányosságot mint figyelembe veendő sarkalatos elveket".

([278]) A kommunikáció lehallgatásának gyakorlati kódexe meghatározza, hogy az arányossági teszt további elemei az alábbiak: „i. a magánéletbe való javasolt beavatkozás mértéke az elérni kívánt célokhoz képest; ii. az alkalmazandó módszerek hogyan és miért okozzák a lehető legkevesebb beavatkozást a személy és mások számára; iii. a tevékenység a törvény megfelelő alkalmazása-e és az elérni kívánt cél elérésére észszerű mód-e, az összes észszerű alternatíva figyelembevételével; iv. adott esetben milyen egyéb módszereket nem hajtottak végre vagy alkalmaztak, de a javasolt nyomozati hatáskör igénybevétele nélkül elégtelennek ítélnek meg az operatív célok teljesítéséhez". A kommunikáció lehallgatásának gyakorlati kódexe, 4.16. pont, elérhető a következő linken: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

([279]) Lásd: A kommunikáció lehallgatásának gyakorlati kódexe, 4.12. és 4.15. pont, elérhető a következő linken: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

([280]) Lásd: A kommunikáció lehallgatásának gyakorlati kódexe, 4.16. pont.

([281]) A Nagy-Britannia és Észak-Írország Egyesült Királyságába irányuló missziójának küldetészáró nyilatkozata a magánélethez való joggal foglalkozó különleges előadó küldetésének befejezésekor, a következő linken érhető el: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, 1.a. pont.

(185) A (186)–(243) preambulumbekezdés részletezi a különböző parancsok kibocsátásának konkrét kritériumait, valamint a nyomozati hatáskörökről szóló 2016. évi törvény által az egyes nyomozati hatáskörökre vonatkozóan megállapított korlátozásokat és biztosítékokat.

3.3.1.1.1. Célzott lehallgatás és vizsgálat

(186) A célzott lehallgatás tekintetében három típusú parancs létezik: a célzott lehallgatási parancs ([282]), a célzott vizsgálati parancs és a kölcsönös segítségnyújtási parancs ([283]). A parancsok kiadásának feltételeit és a vonatkozó biztosítékokat a nyomozati hatáskörökről szóló 2016. évi törvény 2. részének 1. fejezete tartalmazza.

(187) A célzott lehallgatási parancs engedélyezi a parancsban leírt kommunikációk lehallgatását azok továbbítása során, valamint az e kommunikáció szempontjából releváns egyéb adatok gyűjtését ([284]), beleértve a másodlagos adatokat is ([285]). A célzott vizsgálati parancs felhatalmaz egy személyt a tömeges lehallgatási parancs alapján megszerzett lehallgatott tartalom vizsgálatára ([286]).

(188) A nyomozati hatáskörökről szóló 2016. évi törvény 2. része alapján bármilyen parancsot a miniszter adhat ki ([287]) egy igazságügyi biztos jóváhagyásával ([288]). A célzott parancs időtartamam minden esetben 6 hónapra korlátozódik ([289]) módosítására ([290]) és a megújítására ([291]) pedig külön szabályok vonatkoznak.

(189) A parancs kiadása előtt a miniszternek el kell végeznie a szükségesség és az arányosság értékelését ([292]). Konkrétan, a célzott lehallgatási és célzott vizsgálati parancsok esetében a miniszternek ellenőriznie kell, hogy az intézkedésre a következő okok valamelyike miatt van-e szükség: nemzetbiztonsági érdek; a súlyos bűncselekmények megelőzése vagy felderítése; vagy az Egyesült Királyság gazdasági jólétének érdekei ([293]), amennyiben ezek az érdekek a nemzetbiztonsági érdekek szempontjából is relevánsak ([294]). Másrészről kölcsönös segítségnyújtási parancs (lásd a (139) above preambulumbekezdést) csak akkor adható ki, ha a miniszter úgy ítéli meg, hogy fennállnak azokkal a körülményekkel egyenértékű körülmények, amelyekben a súlyos bűncselekmények megelőzése vagy felderítése érdekében parancsot adna ki ([295]).

(190) Ezenkívül a miniszternek fel kell mérnie, hogy az intézkedés arányos-e az elérni kívánt céllal ([296]). A kért intézkedések arányosságának értékelésénél figyelembe kell venni a nyomozati hatáskörökről szóló 2016. évi törvény 2. szakaszának (2) bekezdésében meghatározott, a magánélet védelmével kapcsolatos általános kötelezettségeket, nevezetesen annak felmérését, hogy amit a parancs, engedély vagy felhívás révén el akarnak érni, észszerűen más,

([282]) A nyomozati hatáskörökről szóló 2016. évi törvény 15. szakaszának (2) bekezdése.
([283]) A nyomozati hatáskörökről szóló 2016. évi törvény 15. szakaszának (4) bekezdése.
([284]) A nyomozati hatáskörökről szóló 2016. évi törvény 15. szakaszának (2) bekezdése.
([285]) A másodlagos adatok olyan adatok, amelyek logikailag kapcsolódnak a lehallgatott kommunikációhoz vagy azzal együtt járnak, logikailag elkülöníthetők attól, és külön nem tárnának fel semmit abból, ami észszerűen a kommunikáció értelmének tekinthető (ha van ilyen). A másodlagos adatokra néhány példa: az útválasztó vagy a tűzfalak konfigurációi, vagy az az időtartam, amikor egy útválasztó aktív volt a hálózaton, amikor a lehallgatott kommunikáció részét alkotta, azzal együtt járt vagy ahhoz logikailag kapcsolódott. További részletekért lásd a nyomozati hatáskörökről szóló 2016. évi törvény 16. szakaszában szereplő meghatározást és a kommunikáció lehallgatása gyakorlati kódexének 2.19. pontját, lásd a 278. lábjegyzetet.
([286]) Ezt a vizsgálatot a nyomozati hatáskörökről szóló 2016. évi törvény 152. szakaszának (4) bekezdése alóli kivételként hajtják végre, amely tiltja a Brit-szigeteken tartózkodó személyek kommunikációjának azonosítását. Lásd a (229) preambulumbekezdést.
([287]) A skót miniszter engedélyezi a parancsot, ha az súlyos skóciai bűncselekményhez kapcsolódik (lásd a nyomozati hatáskörökről szóló 2016. évi törvény 21. és 22. szakaszát), míg a miniszter kijelölhet egy magas rangú tisztet kölcsönös segítségnyújtási parancs kiadására, ha úgy tűnik, hogy a lehallgatás az Egyesült Királyságon kívül található személyt vagy helyiségeket érint (a nyomozati hatáskörökről szóló 2016. évi törvény 40. szakasza).
([288]) A nyomozati hatáskörökről szóló 2016. évi törvény 19. és 23. szakasza.
([289]) A nyomozati hatáskörökről szóló 2016. évi törvény 32. szakasza.
([290]) A nyomozati hatáskörökről szóló 2016. évi törvény 39. szakasza. Meghatározott személyek korlátozottan módosíthatják a parancsokat a nyomozati hatáskörökről szóló 2016. évi törvényben meghatározott feltételek szerint. A parancsot kiadó személy bármikor visszavonhatja a parancsot. Ezt akkor kell megtenniük, ha a parancsra semmilyen releváns okból nincs már szükség, vagy a parancs által engedélyezett magatartás már nem arányos az elérni kívánt céllal.
([291]) A nyomozati hatáskörökről szóló 2016. évi törvény 33. szakasza. A parancs megújításáról szóló határozatot egy igazságügyi biztosnak kell jóváhagynia.
([292]) A nyomozati hatáskörökről szóló 2016. évi törvény 19. szakasza.
([293]) Az „Egyesült Királyság gazdasági jólétének érdeke amennyiben ezek az érdekek a nemzetbiztonság szempontjából is relevánsak” fogalmáról az Emberi Jogok Európai Bíróságának nagytanácsa a Big Brother Watch és mások kontra Egyesült Királyság ügyben (lásd a fenti 268. lábjegyzetet), 371. pont, megállapította, hogy ez a fogalom kellően a nemzetbiztonságra összpontosított. Míg a Bíróság megállapítása ebben az ügyben e fogalomnak a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvényben való használatához kapcsolódott, ugyanezt a fogalmat a nyomozati hatáskörökről szóló 2016. évi törvény is használja.
([294]) A nyomozati hatáskörökről szóló 2016. évi törvény 20. szakaszának (2) bekezdése.
([295]) A nyomozati hatáskörökről szóló 2016. évi törvény 20. szakaszának (3) bekezdése.
([296]) A nyomozati hatáskörökről szóló 2016. évi törvény 19. szakasza (1) bekezdésének b) pontja, 19. szakasza (2) bekezdésének b) pontja és 19. szakasza (3) bekezdésének b) pontja.

kevésbé beavatkozó jellegű eszközökkel is el lehetne-e érni, és hogy az információ alapján a parancs alapján alkalmazandó védelem szintje magasabb-e ezen információk különleges jellege okán (lásd a (181) above preambulumbekezdést).

(191) Ennek érdekében a miniszternek figyelembe kell vennie a kérést benyújtó hatóság által benyújtott kérelem összes elemét, különös tekintettel a lehallgatandó személyekre és az intézkedés nyomozás szempontjából fennálló relevanciájára. Ezeket az elemeket a kommunikáció lehallgatásának gyakorlati kódexe tartalmazza, és ezeket meghatározott részletességgel kell leírni ([297]). Ezenkívül a nyomozati hatáskörökről szóló 2016. évi törvény 17. szakasza előírja, hogy a 2. fejezete alapján kiadott minden parancsnak meg kell neveznie vagy ismertetnie kell a lehallgatni kívánt személyt vagy személyek csoportját, szervezetet vagy helyiséget (a „célt"). Célzott lehallgatási parancs vagy célzott vizsgálati parancs esetén ezek személyek csoportjára, több személyre vagy szervezetre vagy több helyiségcsoportra is vonatkozhatnak (más néven „tematikus parancs") ([298]). Ezekben az esetekben a parancsnak ismertetnie kell a személyek csoportjának közös célját vagy tevékenységét vagy a műveletet/vizsgálatokat, és meg kell neveznie vagy le kell írnia annyi személyt/szervezetet vagy helyiséget, ami észszerűen megvalósítható ([299]). Végül a nyomozati hatáskörökről szóló 2016. évi törvény 2. része alapján kibocsátott összes parancsnak meg kell határoznia azokat a címeket, számokat, készülékeket, tényezőket vagy tényezőkombinációkat, amelyeket a kommunikáció azonosításához használni kell ([300]). E tekintetben a kommunikáció lehallgatásának gyakorlati kódexe meghatározza, hogy célzott lehallgatási és célzott vizsgálati parancs esetén „a parancsnak meg kell határoznia (vagy le kell írnia) azokat a tényezőket vagy tényezők kombinációját, amelyeket a kommunikáció azonosításához használni kell. Amennyiben a kommunikációt például telefonszám alapján kell azonosítani, a számot teljes egészében fel kell tüntetni. De amennyiben nagyon összetett vagy folyamatosan változó internetes választókat kell a kommunikáció azonosításához használni, ezeket a választókat a lehető legteljesebb mértékben le kell írni" ([301]).

(192) Fontos biztosíték ebben az összefüggésben az, hogy a miniszter által a parancs kiadásához elvégzett értékelést független igazságügyi biztosnak kell jóváhagynia ([302]), aki különösen azt ellenőrzi, hogy a parancs kiadásáról szóló határozat megfelel-e a szükségesség és az arányosság elvének ([303]) (az igazságügyi biztosok jogállásáról és szerepéről lásd a (251)–(256) below preambulumbekezdést). A nyomozati hatáskörökről szóló 2016. évi törvény azt is pontosítja, hogy az említett ellenőrzés során az igazságügyi biztosnak ugyanazokat az elveket kell alkalmaznia, mint amelyeket a bíróság a bírósági felülvizsgálat iránti kérelem esetében alkalmazna ([304]). Ez biztosítja, hogy minden esetben és az adatokhoz való hozzáférés előtt egy független testület módszeresen ellenőrzi a szükségesség és az arányosság elvének való megfelelést.

(193) A nyomozati hatáskörökről szóló 2016. évi törvény rendelkezik néhány korlátozott és szűk körű kivételről, amikor a lehallgatás parancs nélkül elvégezhető. A korlátozott eseteket a törvény részletezi ([305]), és – a küldő/címzett „hozzájárulásán alapuló" eset kivételével – a nemzetbiztonsági ügynökségektől eltérő személyek (magánszemélyek vagy állami szervek) hajtják végre. Ezenkívül az említett típusú lehallgatásokat más célokból végzik, mint a „hírszerzési információk" gyűjtését ([306]), és néhányuk esetében nagyon valószínűtlen, hogy az adatgyűjtésre egy „adattovábbítási" forgatókönyvvel összefüggésben kerülhet sor (például egy pszichiátriai kórházban vagy börtönben

([297]) A kért információk tartalmazzák az előzményeket részletesen (a személyek/szervezetek/helyiségek leírása, a lehallgatandó kommunikáció leírása) és azt, hogy ezeknek az információknak a gyűjtése milyen előnyökkel jár a nyomozás számára, valamint az engedélyezni kívánt magatartás leírását. Abban az esetben, ha a személyeket/szervezetet/telephelyet nem lehet leírni, magyarázatot kell adni arra, hogy ez miért nem volt lehetséges, vagy miért csak általános leírás készült (a kommunikáció lehallgatásának gyakorlati kódexe, 5.32. és 5.34. pont, lásd a 278. lábjegyzetet).

([298]) A nyomozati hatáskörökről szóló 2016. évi törvény 17. szakaszának (2) bekezdése. Lásd még: A kommunikáció lehallgatásának gyakorlati kódexe, 5.11. és azt követő bekezdések, lásd a 278. lábjegyzetet.

([299]) A nyomozati hatáskörökről szóló 2016. évi törvény 31. szakaszának (4) és (5) bekezdése.

([300]) A nyomozati hatáskörökről szóló 2016. évi törvény 31. szakaszának (8) bekezdése.

([301]) A kommunikáció lehallgatásának gyakorlati kódexe, 5.37. és 5.38. pont, lásd a 278. lábjegyzetet.

([302]) Az igazságügyi biztos jóváhagyása nem szükséges, ha a miniszter úgy ítéli meg, hogy sürgősen ki kell adni a parancsot (a nyomozati hatáskörökről szóló törvény 19. cikkének (1) bekezdése). Az igazságügyi biztost azonban rövid időn belül tájékoztatni kell, és döntenie kell, hogy jóváhagyja-e a parancsot. Ha nem hagyja jóvá, a parancs hatályát veszti (a nyomozati hatáskörökről szóló 2016. évi törvény 24. és 25. szakasza).

([303]) A nyomozati hatáskörökről szóló 2016. évi törvény 23. szakaszának (1) bekezdése.

([304]) A nyomozati hatáskörökről szóló 2016. évi törvény 23. szakaszának (2) bekezdése.

([305]) Lásd a nyomozati hatáskörökről szóló 2016. évi törvény 44–51. szakaszát és a kommunikációs adatok tömeges beszerzésének gyakorlati kódexének 12. szakaszát (lásd a 278. lábjegyzetet).

([306]) Ez a helyzet például akkor, amikor a börtönben vagy a pszichiátriai kórházban van lehallgatásra (az őrizetbe vett személy vagy egy páciens magatartásának ellenőrzése céljából), vagy egy postai vagy távközlési szolgáltató részéről például visszaélést megvalósító tartalom észlelésére szükség.

végzett lehallgatás esetén). Figyelembe véve annak a (nemzetbiztonsági ügynökségektől eltérő) szervnek a jellegét, amelyre ezek a különleges esetek vonatkoznak, a 2018. évi adatvédelmi törvény 2. részében és az Egyesült Királyság általános adatvédelmi rendeletében biztosított összes biztosíték érvényesül, beleértve az információügyi biztos általi felügyeletet és a rendelkezésre álló jogorvoslati mechanizmusokat. Ezenkívül a 2018. évi adatvédelmi törvény által biztosított biztosítékok mellett bizonyos esetekben a nyomozati hatáskörökről szóló 2016. évi törvény előírja a nyomozási biztos hivatala általi utólagos felügyeletet ([307]) is.

(194) Lehallgatás végzésekor további korlátozásokat és biztosítékokat kell alkalmazni a lehallgatott személy(ek) sajátos jogállására figyelemmel ([308]). Például az ügyvédi titoktartási kötelezettség alá esők lehallgatása csak kivételes és kényszerítő körülmények fennállása esetén engedélyezett, a parancsot kiadó személynek figyelembe kell vennie az ügyvédi titoktartási kötelezettséghez fűződő közérdeket, és hogy az ilyen anyagok kezelésére, megőrzésére és közlésére külön követelmények vonatkoznak ([309]).

(195) Ezenkívül a nyomozati hatáskörökről szóló 2016. évi törvény a biztonsággal, a megőrzéssel és a közléssel kapcsolatos konkrét biztosítékokat ír elő, amelyeket a miniszternek figyelembe kell vennie a célzott parancs kiadása előtt ([310]). A nyomozati hatáskörökről szóló 2016. évi törvény 53. szakaszának (5) bekezdése előírja különösen, hogy a parancs alapján összegyűjtött anyagok bármelyikéről készült minden másolatot biztonságos módon kell tárolni és meg kell semmisíteni, amint annak megőrzésére már nincs releváns ok, míg a nyomozati hatáskörökről szóló 2016. évi törvény 53. szakaszának (2) bekezdése előírja, hogy azoknak a személyeknek a számát, akik számára az anyagot nyilvánosságra hozzák, valamint az anyag közlésének, hozzáférhetővé tételének vagy másolásának terjedelmét a törvényi célokhoz szükséges minimumra kell korlátozni.

(196) Végül ha a célzott lehallgatási parancs vagy kölcsönös segítségnyújtási parancs alapján lehallgatott anyagot harmadik országnak kell átadni („tengerentúli közlések"), a nyomozati hatáskörökről szóló 2016. évi törvény előírja, hogy a miniszternek biztosítania kell a megfelelő intézkedések meghozatalát annak biztosítására, hogy a biztonság, a megőrzés és a közlés terén hasonló biztosítékok létezzenek az adott harmadik országban ([311]). Emellett a 2018. évi adatvédelmi törvény 109. szakaszának (2) bekezdése előírja, hogy a hírszerző ügynökségek személyes adatokat az Egyesült Királyságon kívüli területre csak akkor továbbíthatnak, ha az adattovábbítás az adatkezelő törvényi funkcióinak vagy más, a biztonsági szolgálatokról szóló 1989. évi törvény 2. szakasza (2) bekezdésének a) pontjában vagy a hírszerző ügynökségekről szóló 1994. évi törvény 2. szakasza (2) bekezdésének a) pontjában és 4. szakasza (2) bekezdésének a) pontjában előírt más céloknak megfelelően végzett, szükséges és arányos intézkedés ([312]). Fontos, hogy ezek a követelmények azokban az esetekben is érvényesülnek, amikor a 2018. évi adatvédelmi törvény 110. szakasza szerinti nemzetbiztonsági kivételre hivatkoznak, mivel a 2018. évi adatvédelmi törvény 110. szakasza nem sorolja fel a 2018. évi adatvédelmi törvény 109. szakaszát azon rendelkezések között, amelyek alkalmazása mellőzhető, ha a nemzetbiztonság védelme érdekében bizonyos rendelkezések alóli kivételre van szükség.

3.3.1.1.2. Kommunikációs adatok célzott gyűjtése és megőrzése

(197) A nyomozati hatáskörökről szóló 2016. évi törvény lehetővé teszi a miniszter számára, hogy a távközlési szolgáltatóktól megkövetelje a kommunikációs adatok megőrzését számos hatóság – ideértve a bűnüldöző és hírszerző ügynökségeket is – célzott hozzáférése céljából. A nyomozati hatáskörökről szóló 2016. évi törvény 4. része a kommunikációs adatok megőrzéséről rendelkezik, míg a 3. rész a kommunikációs adatok (TCD) célzott gyűjtéséről. A nyomozati hatáskörökről szóló 2016. évi törvény 3. és 4. része meghatároz ezen hatáskörök felhasználására egyedi korlátozásokat is, és külön biztosítékokat ír elő.

([307]) A contrario lásd a nyomozati hatáskörökről szóló törvény 229. szakaszának (4) bekezdését.

([308]) A nyomozati hatáskörökről szóló 2016. évi törvény 26–29. szakasza korlátozásokat vezet be a célzott lehallgatási és vizsgálati parancsok gyűjtésére vonatkozóan a parlamenti (az Egyesült Királyság bármelyik parlamentje) képviselő által küldött vagy neki szánt kommunikáció lehallgatásával, az ügyvédi titoktartási kötelezettség alá eső tételek, valamint olyan kommunikáció lehallgatásával kapcsolatban, amelyekről a lehallgató hatóság úgy véli, hogy bizalmas újságírói anyagokat tartalmazó kommunikáció lesz, és amennyiben a parancs célja az újságírói információk forrásának azonosítása vagy megerősítése.

([309]) A nyomozati hatáskörökről szóló 2016. évi törvény 26. szakasza.

([310]) A nyomozati hatáskörökről szóló 2016. évi törvény 19. szakaszának (1) bekezdése.

([311]) A nyomozati hatáskörökről szóló 2016. évi törvény 54. szakasza. Az anyagok külföldi hatóságokkal való közlésével kapcsolatos biztosítékokat a gyakorlati kódexek tovább részletezik: lásd különösen a kommunikáció lehallgatásának gyakorlati kódexének 9.26. és azt követő pontjai, valamint annak 9.87. pontja, és a berendezések zavarásáról szóló gyakorlati kódex 9.33. és azt követő pontjai, valamint annak 9.41. pontja (lásd a 278. lábjegyzetet).

([312]) Ezek a célok a következők: a Biztonsági Szolgálat esetében a súlyos bűncselekménye megelőzése vagy felderítések vagy bármely büntetőeljárás (a biztonsági szolgálatokról szóló 1989. évi törvény 2. szakasza (2) bekezdésének a) pontja), a Titkosszolgálat esetében a nemzetbiztonsági érdekek, a súlyos bűncselekmények megelőzése vagy felderítése, vagy bármilyen büntetőeljárás (a hírszerző ügynökségekről szóló 1994. évi törvény 2. szakasza (2) bekezdésének a) pontja), a Kormányzati Kommunikációs Központ esetében pedig bármely büntetőeljárás (a hírszerző ügynökségekről szóló 1994. évi törvény 4. szakasza (2) bekezdésének a) pontja). Lásd a 2018. évi adatvédelmi törvény indokolását, amely a következő linken érhető el: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

(198) A „kommunikációs adatok” kifejezés magában foglalja a kommunikáció alanyait, idejét, helyét és módját, de a tartalmát, vagyis az elmondottakat vagy abban írtakat nem. A lehallgatástól eltérően a kommunikációs adatok gyűjtése és megőrzése nem a kommunikáció tartalmának gyűjtésére, hanem olyan információk gyűjtésére irányul, mint például a telefonos szolgáltatás előfizetője vagy tételes számla. Ez magában foglalhatja a kommunikáció idejét és időtartamát, a kezdeményező és a fogadó számát vagy e-mail-címét, valamint időnként azoknak az eszközöknek a helyét, amelyekről a távközlés történt ([313]).

(199) Meg kell jegyezni, hogy a kommunikációs adatok megőrzése és gyűjtése általában nem uniós érintettek e határozat alapján az Egyesült Királyságba továbbított személyes adataira fog irányulni. A kommunikációs adatok megőrzésére vagy közlésére vonatkozó kötelezettség a nyomozati hatáskörökről szóló 2016. évi törvény 3. és 4. része szerint azokra az adatokra terjed ki, amelyeket az Egyesült Királyság telekommunikációs szolgáltatói közvetlenül a távközlési szolgáltatás felhasználóitól gyűjtenek ([314]). Ez a fajta „ügyfélalapú” feldolgozás általában nem jár e határozat alapján adattovábbítással, vagyis uniós adatkezelőtől/adatfeldolgozótól egyesült királyságbeli adatkezelőhöz/adatfeldolgozóhoz történő adattovábbítással.

(200) A teljesség kedvéért azonban a következő preambulumbekezdésekben elemzésre kerülnek az említett gyűjtési és megőrzési rendszereket szabályozó feltételek és biztosítékok.

(201) Kiindulásként meg kell jegyezni, hogy a kommunikációs adatok megőrzése és célzott gyűjtése mind a nemzetbiztonsági ügynökségek, mind az egyes bűnüldöző hatóságok számára elérhető ([315]). A kommunikációs adatok megőrzésének és/vagy gyűjtésének megkövetelésének feltételei az intézkedés igénylésének okától, nevezetesen a nemzetbiztonsági vagy bűnüldözési céltól függően eltérőek lehetnek.

(202) Különösen, míg az új rendszer bevezette a független testület *előzetes* engedélyének általános követelményt, amely minden esetben alkalmazandó, amikor a kommunikációs adatokat megőrzik és/vagy gyűjtik (bűnüldözési vagy nemzetbiztonsági célból), az Európai Bíróság Tele2/Watson ügyben hozott ítéletét ([316]) követően különleges biztosítékokat vezettek be arra az esetre, amikor az intézkedést bűnüldözési célokra kérik. Különösen, az engedélyt minden esetben a nyomozati hatáskörök biztosának kell előzetesen megadnia, ha a kommunikációs adatok megőrzését vagy gyűjtését bűnüldözési célból kérik. Nem mindig ez a helyzet, amennyiben az intézkedést nemzetbiztonsági célból kérik, mivel az alábbiakban leírtak szerint bizonyos esetekben ilyen típusú intézkedéseket más „engedélyező személyek” engedélyezhetnek. Emellett az új rendszer a „súlyos bűncselekményekre” emelte azt a küszöböt, amelynek esetében megengedhető a kommunikációs adatok megőrzése és gyűjtése ([317]).

([313]) A kommunikációs adatokat a nyomozati hatáskörökről szóló 2016. évi törvény 261. szakaszának (5) bekezdése határozza meg. A kommunikációs adatok feloszthatók „eseményadatokra” (minden olyan adat, amely azonosítja vagy leírja az eseményt, függetlenül attól, hogy a helyszínre utal-e vagy sem, egy távközlési rendszerben vagy annak segítségével, amennyiben az esemény meghatározott tevékenység meghatározott időpontban egy vagy több jogalany általi folytatása) és a „jogalany adataira” (minden olyan adat, amely a) i. egy jogalanyra, ii. egy távközlési szolgáltatás és egy jogalany kapcsolatára, vagy iii. a távközlési rendszer bármely része és a jogalany kapcsolatára vonatkozik, b) olyan adatokból áll vagy olyan adatokat tartalmaz, amelyek azonosítják vagy leírják a jogalanyt (akár utalva a jogalany helyére, akár nem), és c) nem eseményadatok).

([314]) Ez a kommunikációs adatoknak a nyomozati hatáskörökről szóló 2016. évi törvény 261. szakaszának (5) bekezdésében szereplő meghatározásából következik, miszerint a kommunikációs adatokat egy távközlési szolgáltató birtokolja vagy szerzi be, és vagy egy távközlési szolgáltatás felhasználójára vonatkoznak, és e szolgáltatás nyújtásával kapcsolatosak, vagy egy kommunikáció részét képezit, ahhoz csatolták vagy logikailag kapcsolódik (lásd még a kommunikációs adatok gyakorlati kódexét, elérhető a következő linken) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, (2.22–2.33. pont). Ezenkívül a távközlési szolgáltatónak a nyomozati hatáskörökről szóló 2016. évi törvény 261. szakaszának (10) bekezdésében szereplő meghatározása megköveteli, hogy a távközlési szolgáltató olyan személy legyen, aki telekommunikációs szolgáltatást kínál vagy nyújt az Egyesült Királyságban tartózkodó személyeknek, vagy olyan telekommunikációs rendszert irányít vagy biztosít, amely (teljes egészében vagy részben) az Egyesült Királyságban található vagy onnan irányítják. Ezek a meghatározások egyértelművé teszik, hogy a nyomozati hatáskörökről szóló 2016. évi törvény alapján nem róhatók kötelezettségek azokra a távközlési szolgáltatókra, amelyeknek nincsenek berendezései az Egyesült Királyságban vagy nem az Egyesült Királyságból irányítottak, és akik nem kínálnak vagy nyújtanak szolgáltatásokat az Egyesült Királyságban tartózkodó személyeknek (lásd még a kommunikációs adatok gyakorlati kódexének 2.1. pontját). Ha uniós előfizetők (függetlenül attól, hogy az EU-ban vagy az Egyesült Királyságban tartózkodnak-e) igénybe veszik a szolgáltatásokat az Egyesült Királyságban, a szolgáltatás nyújtásával kapcsolatos bármely kommunikációt közvetlenül az Egyesült Királyság szolgáltatója gyűjti össze, és nem az EU-ból kerül továbbításra.

([315]) Az érintett hatóságokat a nyomozati hatáskörökről szóló 2016. évi törvény 4. jegyzéke tartalmazza, és magukban foglalják a rendőrségeket, a hírszerző ügynökséget, néhány minisztériumot és kormányzati szervet, a Nemzeti Bűnügyi Ügynökséget, a királynő bevételi és vámügyi hivatalát, a Verseny- és Piacfelügyeleti Hatóságot, az információügyi biztost, a mentőket, tűzoltókat és mentő szolgálatokat, valamint például az egészségügyi és élelmiszer-biztonsági hatóságokat.

([316]) A C-203/15. és C-698/15. sz., Tele2/Watson egyesített ügyekben hozott ítélet, ECLI:EU:C:2016:970.

([317]) A kommunikációs adatok megszerzése vonatkozásában lásd a 61.7. pont b) alpontját, és a kommunikációs adatok megőrzése tekintetében pedig a 87.10. pontot.

i. *Kommunikációs adatok gyűjtésének engedélyezése*

(203) A nyomozati hatáskörökről szóló 2016. évi törvény 3. része szerint az érintett hatóságok jogosultak kommunikációs adatok távközlési szolgáltatótól vagy olyan személytől való gyűjtésére, aki képes ilyen adatokat megszerezni és közölni. Az engedély nem teheti lehetővé a közlemények tartalmának lehallgatását ([318]) és egy hónap elteltével hatályát veszti ([319]), a további engedély alapján történő megújítás lehetőségével ([320]). Kommunikációs adatok gyűjtéséhez a nyomozati hatáskörök biztosának (nyomozási biztos) engedélye szükséges ([321]) (a nyomozási biztos státusáról és hatásköréről lásd a (250)–(251) below preambulumbekezdést). Ez a helyzet minden olyan esetben, amikor a kommunikációs adatok gyűjtését az érintett rendvédelmi hatóság kéri. A nyomozati hatáskörökről szóló 2016. évi törvény 61. szakasza szerint azonban amikor az adatokat az Egyesült Királyság nemzetbiztonsága vagy – amennyiben ez releváns a nemzetbiztonság szempontjából – gazdasági jóléte érdekében gyűjtik, vagy ha a kérelmet hírszerző ügynökség tagja nyújtja be a 61. cikk (7) bekezdésének b) pontja alapján ([322]), az adatok gyűjtése ehelyett történhet ([323]) a nyomozási biztos vagy egy kijelölt vezető tiszt engedélyével ([324]). A kijelölt tisztviselőnek függetlennek kell lennie az érintett vizsgálattól vagy művelettől, és ismernie kell az emberi jogi elveket és a jogszabályokat, különös tekintettel a szükségességre és az arányosságra vonatkozókra ([325]). A kijelölt tisztviselő által hozott határozatot a nyomozási biztos utólag felügyeli (a nyomozási biztos utólagos felügyeleti funkciójáról részletesen lásd a (254) below preambulumbekezdést).

(204) A kommunikációs adatok gyűjtésének engedélyezése az intézkedés szükségességének és arányosságának értékelésén alapul. Pontosabban az intézkedés szükségességét a jogszabályokban felsorolt okokra figyelemmel értékelik ([326]). Figyelembe véve ezen intézkedés célzott jellegét, annak szükségesnek kell lennie egy konkrét nyomozáshoz vagy művelethez is ([327]). Az intézkedések szükségességének értékelésére vonatkozó további követelményeket a kommunikációs adatok gyakorlati kódexe határozza meg ([328]). Ez a kódex különösen azt írja elő, hogy a megkereső hatóság által benyújtott kérelemnek három minimumelemet kell meghatároznia a kérelem szükségességének igazolására: i. a vizsgált esemény, például egy bűncselekmény vagy egy kiszolgáltatott eltűnt személy tartózkodási helye; ii. az a személy, akinek az adatait kérik, például gyanúsított, tanú vagy eltűnt személy, és hogy miként kapcsolódnak az eseményhez; és iii. a kért kommunikációs adatok, például telefonszám vagy IP-cím, és hogy ezek az adatok miként kapcsolódnak a személyhez és az eseményhez ([329]).

(205) Ezenkívül a kommunikációs adatok gyűjtésének arányosban kell állnia az elérni kívánt célokkal ([330]). A kommunikációs adatokra vonatkozó magatartási kódex egyértelművé teszi, hogy az említett értékelés elvégzése során az engedélyező személynek egyensúlyba kell hoznia az „egyén jogaiba és szabadságaiba való beavatkozás mértékét és az illetékes hatóság által közérdekből végzett nyomozás vagy művelet konkrét előnyét”, és hogy egy

([318]) A nyomozati hatáskörökről szóló 2016. évi törvény 60A. szakaszának (6) bekezdése.

([319]) Ez az időtartam három napra rövidül, ha az engedélyt sürgős okokból adják meg (a nyomozati hatáskörökről szóló 2016. évi törvény 65. szakasza (3) bekezdésének A. pontja).

([320]) A nyomozati hatáskörökről szóló 2016. évi törvény 65. szakasza szerint a megújított engedély a jelenlegi engedély lejártától számított egy hónapig érvényes. Az engedélyt megadó személy bármikor visszavonhatja az engedélyt, ha úgy ítéli meg, hogy a követelmények már nem teljesülnek.

([321]) A nyomozati hatáskörökről szóló 2016. évi törvény 60A. szakaszának (1) bekezdése. Az Office for Communications Data Authorisations (OCDA – Kommunikációs Adatengedélyezési Hivatal) ezt a funkciót a nyomozási biztos nevében látja el (lásd: a kommunikációs adatokra vonatkozó gyakorlati kódex, 5.6. pont).

([322]) A nyomozati hatáskörökről szóló 2016. évi törvény 61. szakasza (7) bekezdésének b) pontja szerinti kérelmet „egy bűncselekménnyel kapcsolatos megfelelő célból” nyújtják be, vagyis a nyomozati hatáskörökről szóló 2016. évi törvény 61. szakasza (7) bekezdésének A. pontja szerint: „Ha a kommunikációs adatok részben vagy egészben eseményadatok, a súlyos bűncselekmények megelőzésének vagy felderítésének céljából; minden más esetben a bűnözés megelőzésének vagy felderítésének vagy a rendbontás megelőzésének céljából”.

([323]) A kommunikációs adatokkal kapcsolatos gyakorlati kódex meghatározza, hogy „Ha a nemzetbiztonsággal kapcsolatos kérelmet akár a 60A., akár a 61. szakasz alapján lehet benyújtani, az egyes hatóságok döntenek, hogy az adott esetben melyik engedélyezési mód a legmegfelelőbb. Azoknak a hatóságoknak, amelyek a kijelölt vezető tiszt útvonalat kívánják használni, egyértelmű iránymutatásokkal kell rendelkezniük arra vonatkozóan, hogy ez az engedélyezési út mikor megfelelő”(a kommunikációs adatok gyakorlati kódexének 5.19. pontja, elérhető a következő linken: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

([324]) A nyomozati hatáskörökről szóló 2016. évi törvény 70. szakaszának (3) bekezdése határozza meg a „kijelölt tisztviselő” fogalmát, amely az érintett hatóságtól függően változik (a nyomozati hatáskörökről szóló 2016. évi törvény 4. mellékletében meghatározottak szerint).

([325]) A kijelölt vezető tisztviselő függetlenségére vonatkozó további részleteket a kommunikációs adatokra vonatkozó gyakorlati kódex 4.12–4.17. pontja írja elő, lásd a 323. lábjegyzetet).

([326]) Az indokok a következők lehetnek: i. nemzetbiztonsági érdekében; ii. a bűnözés megelőzése vagy felderítése, vagy rendbontás megelőzése (az „eseményadatok” esetében csak súlyos bűncselekmények esetén); iii. az Egyesült Királyság gazdasági jóléte érdekében, amennyiben ezek az érdekek a nemzetbiztonsági érdekek szempontjából is relevánsak; iv. a közbiztonság érdekében; v. halál vagy sérülés, vagy egy személy testi vagy lelki egészsége bármilyen károsodásának megelőzése, vagy testi vagy lelki egészség sérülésének vagy károsodásának enyhítése céljából; vi. az állítólagos bírói tévedések kivizsgálásának elősegítése, vagy vii. egy halott vagy olyan személy azonosítása, aki egy bizonyos betegség miatt nem képes azonosítani magát (a nyomozati hatáskörökről szóló 2016. évi törvény 61. szakaszának (7) bekezdése).

([327]) A nyomozati hatáskörökről szóló 2016. évi törvény 60A. szakasza (1) bekezdésének b) pontja.

([328]) A kommunikációs adatok gyakorlati kódexének 3.3. és azt követő szakaszai, lásd a 323. lábjegyzetet.

([329]) A kommunikációs adatok gyakorlati kódexének 3.13. pontja, lásd a 323. lábjegyzetet.

([330]) A nyomozati hatáskörökről szóló 2016. évi törvény 60. szakasza (1) bekezdésének c) pontja.

adott eset összes szempontjának figyelembevételével „az egyén jogaiba való beavatkozás továbbra sem feltétlenül indokolt, ha egy másik egyén vagy egyének csoportjának jogaira gyakorolt kedvezőtlen hatás túl súlyos". Ezenkívül az intézkedés arányosságának konkrét értékelése érdekében a Kódex számos olyan elemet sorol fel, amelyeknek szerepelnie kell a megkereső hatóság által benyújtott kérelemben ([331]). Ezenkívül különös figyelmet kell fordítani a kommunikációs adatok típusára („jogalanyra" vagy „eseményekre" vonatkozó adatok ([332])), és előnyben kell részesíteni a kevésbé beavatkozó adatkategória használatát ([333]). A kommunikációs adatok gyakorlati kódexe konkrét utasításokat is tartalmaz az egyes szakmákban dolgozók (például orvosok, ügyvédek, újságírók, parlamenti képviselők vagy vallásminiszterek) kommunikációs adatait érintő engedélyekre vonatkozóan ([334]), amelyekre további biztosítékok vonatkoznak ([335]).

ii. *Felhívás a kommunikációs adatok megőrzésére*

(206) A nyomozati hatáskörökről szóló 2016. évi törvény 4. része meghatározza a kommunikációs adatok megőrzésének szabályait, és különösen azokat a kritériumokat, amelyek lehetővé teszik a miniszter számára, hogy megőrzési felhívást adjon ki ([336]). A nyomozati hatáskörökről szóló törvény által bevezetett biztosítékok akkor is azonosak, ha az adatokat bűnüldözési célból vagy a nemzetbiztonság érdekében őrzik.

(207) Az említett megőrzési felhívások kiadásának célja annak biztosítása, hogy a távközlési szolgáltatók legfeljebb 12 hónapig megőrizzék azokat a releváns kommunikációs adatokat, amelyeket egyébként törölnének, ha azok már nem szükségesek üzleti célokra ([337]). A megőrzött adatoknak a szükséges ideig rendelkezésre kell állniuk, amennyiben később a hatóságnak szüksége lenne azok beszerzésére a nyomozati hatáskörökről szóló 2016. évi törvény 3. részében megadott és a (203)–(205) preambulumbekezdésben ismertetett kommunikációs adatok célzott gyűjtésére vonatkozó engedély alapján.

(208) A bizonyos adatok megőrzésének előírására vonatkozó hatáskör gyakorlására számos korlátozás és biztosíték vonatkozik. A miniszter csak akkor adhat ki megőrzési felhívást egy vagy több szolgáltatónak ([338]), ha úgy ítéli meg, hogy az adatok megőrzésének követelménye jogszabályi okok valamelyikéhez szükséges ([339]) és arányos az elérni kívánt célokkal ([340]). Amint azt maga a nyomozati

([331]) Ezeknek az információknak magukban kell foglalniuk az alábbiakat: i. annak felvázolása, hogy az adatok gyűjtése milyen előnyökkel jár a nyomozás vagy a művelet vonatkozásában; ii. a kért időszakok relevanciájának magyarázata, beleértve azt is, hogy ezek az időszakok arányosak-e a vizsgált eseménnyel; iii. annak magyarázata, hogy a beavatkozás szintje miért indokolt, ha figyelembe vesszük az adatok által a vizsgálat vonatkozásában nyújtott előnyöket (ennek az indokolásnak ki kell terjednie annak mérlegelésére, hogy végezhető-e kevesebb beavatkozással járó nyomozati cselekmény a cél elérése érdekében); iv. az egyén jogainak (különösen a magánélethez való jog és adott esetben a véleménynyilvánítás szabadsága) mérlegelése, valamint e jogok és a nyomozás előnyei egyensúlyának mérlegelése; v. annak részletei, hogy milyen járulékos beavatkozás történhet, és hogyan befolyásolják a kért időszakok a járulékos beavatkozást (a kommunikációs adatokra vonatkozó gyakorlati kódex 3.22–3.26. szakasza, lásd a 323. lábjegyzetet).

([332]) Lásd a 313 lábjegyzetet.

([333]) Ha tolakodóbb kommunikációs adatokat (azaz eseményadatokat) kérnek, a kódex előírja, hogy helyesebb először a jogalany adatainak gyűjtése vagy az események közvetlen adatainak gyűjtése korlátozott, sürgős esetkörben (a kommunikációs adatokra vonatkozó gyakorlati kódex, 6.10–6.14. pont, lásd a 323. lábjegyzetet).

([334]) A kommunikációs adatok gyakorlati kódexe, 8.8–8.44. pont, lásd a 323. lábjegyzetet.

([335]) A gyakorlati kódex meghatározza, hogy „az engedélyező személynek különös gonddal kell eljárnia az említett kérelmek elbírálásakor, beleértve annak további megfontolását, hogy lehetnek-e nem szándékolt következményei az említett kérelmeknek, és hogy a közérdeket legmegfelelőbben a kérelem szolgálja-e" (A kommunikációs adatok gyakorlati kódexe, 8.8. pont). Ezenkívül nyilvántartást kell vezetni az említett típusú kérelmekről, és a következő ellenőrzéskor ezeket a kérelmeket meg kell jelölni a nyomozási biztos számára (a kommunikációs adatok gyakorlati kódexe, 8.10. pont, lásd a 323. lábjegyzetet).

([336]) A nyomozati hatáskörökről szóló 2016. évi törvény 87–89. szakasza.

([337]) A nyomozati hatáskörökről szóló 2016. évi törvény 90. szakasza értelmében az a távközlési szolgáltató, amely megőrzési felhívást kap, felülvizsgálatot kérhet az azt kiadó minisztertől.

([338]) A nyomozati hatáskörökről szóló 2016. évi törvény 87. cikke (2) bekezdésének a) pontja alapján a megőrzési felhívás vonatkozhat „egy adott üzemeltetőre vagy bármely leírásnak megfelelő üzemeltetőre".

([339]) Az okok a következők: i. a nemzetbiztonság érdekei; ii. a bűncselekménnyel kapcsolatos vonatkozó cél (a nyomozati hatáskörökről szóló 2016. évi törvény 87.10A. szakaszában meghatározottak szerint); iii. az Egyesült Királyság gazdasági jólétének érdekei, amennyiben ezek az érdekek a nemzetbiztonsági érdekek szempontjából is relevánsak; iv. a közbiztonság érdekei; v. halál vagy sérülés, vagy egy személy testi vagy lelki egészsége bármilyen károsodásának megelőzése, vagy testi vagy lelki egészség sérülésének vagy károsodásának enyhítése céljából; vagy vi. az állítólagos bírói tévedések kivizsgálásának támogatása (a nyomozati hatáskörökről szóló törvény 87. szakasza).

([340]) A nyomozati hatáskörökről szóló 2016. évi törvény 87. szakasza. Ezenkívül a vonatkozó gyakorlati kódex szerint a megőrzési felhívás arányosságának értékelése érdekében a nyomozati hatáskörökről szóló 2016. évi törvény 2. szakaszának (2) bekezdésében előírt kritériumok alkalmazandók, nevezetesen annak a követelménynek az értékelése, hogy amit a felhívással el kívánnak elérni, kevésbé beavatkozó jellegű eszközökkel észszerűen elérhető-e. A kommunikációs adatok gyűjtése arányosságának értékeléséhez hasonlóan a kommunikációs adatok gyakorlati kódexe is egyértelművé teszi, hogy ez az értékelés magában foglalja az „egyén magánéletének tiszteletben tartásához való jogába való beavatkozás mértéke és a nyomozás konkrét haszna egyensúlyának megteremtését (a kommunikációs adatok gyakorlati kódexének 16.3. pontja, lásd a 323. lábjegyzetet).

hatáskörökről szóló 2016. évi törvény is pontosítja ([341]), a megőrzési felhívás kiadása előtt a miniszternek figyelembe kell vennie az alábbiakat: a hirdetmény várható előnyei ([342]); a távközlési szolgáltatás ismertetése; a megőrzendő adatok hely szerinti korlátozásának helyessége vagy a távközlési szolgáltatásokat nyújtó személyek leírása alapján ([343]); a hírközléssel érintett bármely távközlési szolgáltatás várható felhasználóinak száma (ha ismert) ([344]); a felhívásnak való megfelelés műszaki megvalósíthatósága; a felhívás betartásának valószínű költségei és a közlemény bármilyen más hatása a távközlési szolgáltatóra (vagy megjelölt üzemeltetőkre), amelyre az vonatkozik ([345]). Amint azt a kommunikációs adatokkal kapcsolatos gyakorlati kódex 17. fejezete részletezi, minden megőrzési felhívásnak meg kell határoznia minden megtartandó adattípust, és azt, hogy az adott adattípus hogyan felel meg a megőrzéshez szükséges teszteken.

(209) A miniszter megőrzési felhívás kiadására vonatkozó határozatát minden esetben (nemzetbiztonságra vagy bűnüldözés célra hivatkozáskor is) független igazságügyi biztosnak kell jóváhagynia az úgynevezett „duplán ellenőrzött eljárás" alapján, akinek különösen azt kell ellenőriznie, hogy az érintett kommunikációs adatok megőrzésére vonatkozó felhívás egy vagy több jogszabályi okból szükséges-e ([346]).

3.3.1.1.3. A berendezés zavarása

(210) A berendezések zavarása olyan technikák összessége, amelyeket különféle adatok gyűjtésére használnak berendezésekből ([347]), amelybe beletartoznak a számítógépek, táblagépek és okostelefonok, valamint kábelek, vezetékek és tárolóeszközök ([348]). A berendezés zavarása lehetővé teszi a kommunikáció és a berendezés adatai tartalmának gyűjtését ([349]).

(211) A nyomozati hatáskörökről szóló 2016. évi törvény 13. szakaszának (1) bekezdésével összhangban a berendezések zavarásának hírszerző ügynökség általi használatához engedély szükséges a nyomozati hatáskörökről szóló 2016. évi törvény által létrehozott „duplán ellenőrzött" eljárás szerinti engedély alapján, feltéve, hogy fennáll „kapcsolódás a Brit-szigetekkel" ([350]). Az Egyesült Királyság hatóságainak magyarázata szerint azokban a helyzetekben, amikor az adatokat az Európai Unióból az Egyesült Királyságba továbbítják e határozat hatálya alatt, mindig fennáll

([341]) Lásd a nyomozati hatáskörökről szóló 2016. évi törvény 88. szakaszát.

([342]) Az előnyök lehetnek fennállóak vagy előre láthatóak, és olyan törvényi célok vonatkozásában kell fennállniuk, amelyekre adatok megtarthatók (a kommunikációs adatokra vonatkozó gyakorlati kódexének 17.17. pontja, lásd a 323. lábjegyzetet).

([343]) Ezeknek a megfontolásoknak része annak eldöntése, hogy a megőrzési felhívás teljes földrajzi terjedelme szükséges és arányos-e, valamint hogy szükséges és arányos-e a személyek valamilyen konkrét leírásának beillesztése vagy kizárása (a kommunikációs adatok gyakorlati kódexének 17.17. pontja, lásd a 323. lábjegyzetet).

([344]) Ez segíti a minisztert az ügyfeleket érő beavatkozás mértékének, de a megőrzendő adatok várható előnyeinek mérlegelésében is (a kommunikációs adatokra vonatkozó gyakorlati kódexének 17.17. pont, lásd a 323. lábjegyzetet).

([345]) A nyomozati hatáskörökről szóló 2016. évi törvény 88. szakasza.

([346]) A nyomozati hatáskörökről szóló 2016. évi törvény 89. szakasza.

([347]) A nyomozati hatáskörökről szóló 2016. évi törvény 135. szakaszának (1) bekezdése és 198. szakaszának (1) bekezdése értelmében a „berendezés" magában foglalja az elektromágneses, akusztikus vagy egyéb sugárzást kibocsátó berendezéseket és minden olyan eszközt, amely alkalmas az említett berendezésekkel való kapcsolatra.

([348]) Gyakorlati kódex a berendezések zavarásáról, elérhető a következő linken: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, 2.2. pont.

([349]) A berendezés adatait a nyomozati hatáskörökről szóló 2016. évi törvény 100. szakasza olyan rendszeradatként határozza meg, amely a) a kommunikációt tartalmazza, annak részét képezi, ahhoz csatolva van vagy logikailag kapcsolódik (akár a küldő révén, akár más módon), vagy bármely más információelem; b) logikusan elkülöníthető a kommunikáció vagy az információ többi részétől, és c) külön nem tárnának fel semmit abból, ami észszerűen a kommunikáció vagy információ értelmének tekinthető (ha van ilyen).

([350]) Ahhoz, hogy a parancsra vonatkozó követelmény kötelező legyen, a nyomozati hatáskörökről szóló 2016. évi törvény 13. szakaszának (1) bekezdése előírja azt is, hogy a hírszerző ügynökség magatartása egy vagy több bűncselekménynek minősüljön a Computer Misuse Act 1990 elnevezésű (a számítógépes visszaélésekről szóló 1990. évi) törvény 1–3. szakasza szerint, ami az esetek túlnyomó többségére igaz lenne, lásd a Berendezések zavarásáról szóló gyakorlati kódex 3.32. és 3.6–3.9. pontját). A nyomozati hatáskörökről szóló 2016. évi törvény 13. szakaszának (2) bekezdése szerint „a kapcsolódás a Brit-szigetekkel" akkor áll fenn, ha a) bármely magatartás a Brit-szigeteken valósulna meg (függetlenül a berendezés helyétől, b) a hírszerző ügynökség úgy véli, hogy bármely berendezés, amelyet ténylegesen vagy lehetségesen zavarnak, annak során valamikor a Brit-szigeteken lenne vagy lehetne, vagy c) a zavarás célja: i. olyan kommunikáció megszerzése, amelynek küldője vagy címzettje a hírszerző ügynökség feltételezése szerint a Brit-szigeteken tartózkodik; vagy ii. a hírszerző ügynökség feltételezése szerint a Brit-szigeteken tartózkodó személyre vonatkozó magáninformáció, vagy iii. olyan berendezés adat, amely az i. vagy ii. albekezdés hatálya alá tartozó kommunikáció vagy magáninformáció részét képezi vagy ahhoz kapcsolódik.

kapcsolódás a „Brit-szigetekkel”, és ezért a berendezések említett adatokra kiterjedő bármilyen zavarására érvényes a nyomozati hatáskörökről szóló 2016. évi törvény 13. szakasz (1) bekezdésében szereplő parancs követelménye ([351]).

(212) A célzott berendezészavarási parancsokra vonatkozó szabályokat a nyomozati hatáskörökről szóló 2016. évi törvény 5. része tartalmazza. A célzott lehallgatáshoz hasonlóan a célzott berendezészavarásnak egy meghatározott „célhoz” kell kapcsolódnia, amelyet a parancsban fel kell tüntetni ([352]). A „cél” azonosításának részletei az ügytől és a zavarni kívánt berendezés típusától függenek. Különösen a nyomozati hatáskörökről szóló törvény 115. szakaszának (3) bekezdése határozza meg azokat az elemeket, amelyeket a parancsnak tartalmaznia kell (pl. a személy vagy szervezet neve, a helyszín leírása), például attól függően, hogy a zavarás olyan berendezésre vonatkozik-e, amely egy adott személy, szervezet vagy személyek csoportja tulajdonában vagy birtokában van, meghatározott helyen található és így tovább. ([353]). Azok a célok, amelyekre célzott berendezészavarási parancs kiadható, attól függenek, hogy milyen hatóság kérelmezi azt ([354]).

(213) A célzott lehallgatáshoz hasonlóan a kibocsátó hatóságnak meg kell vizsgálnia, hogy az intézkedés szükséges-e egy meghatározott cél eléréséhez, és hogy arányos-e az elérni kívánt céllal ([355]). Ezenkívül azt is mérlegelnie kell, hogy léteznek-e biztosítékok a biztonság, a megőrzés és közlés, valamint a „tengerentúli közlés” vonatkozásában ([356]) (lásd a (196) preambulumbekezdést).

(214) A parancsot egy igazságügyi biztosnak kell jóváhagynia, a sürgős eseteket kivéve ([357]). Ez utóbbi esetben az igazságügyi biztost tájékoztatni kell a parancs kiadásáról, és azt három munkanapon belül jóvá kell hagynia. Abban az esetben, ha az igazságügyi biztos elutasítja annak jóváhagyását, a parancs hatályát veszti és nem újítható meg ([358]). Ezenkívül az igazságügyi biztosnak hatásköre van arra, hogy megkövetelje a parancs alapján gyűjtött adatok törlését ([359]). Az a tény, hogy a parancsot sürgősséggel adták ki, nem befolyásolja az utólagos felügyeletet (lásd a (244)–(255) preambulumbekezdést) vagy az egyének jogorvoslati lehetőségeit (lásd a (260)–(270) preambulumbekezdést). A magánszemélyek a szokásos módon panaszt tehetnek az információügyi biztosnál, vagy bármely állítólagos magatartással szemben igényt terjeszthetnek a nyomozati hatáskörrel foglalkozó bírósághoz. Az igazságügyi biztos a parancs jóváhagyásáról való döntéskor minden esetben alkalmazza a célzott lehallgatás iránti kérelmekre a szükségességi és arányossági tesztet ([360]) (lásd a (192) above preambulumbekezdést).

([351]) A teljesség kedvéért meg kell jegyezni, hogy még egy olyan helyzetben is, amelyben nincs „kapcsolódás a Brit-szigetekhez”, és a berendezések zavarásának használata ezért nem tartozik a nyomozati hatáskörökről szóló 2016. évi törvény 13. szakaszának (1) bekezdésében előírt kötelező parancs követelményének hatálya alá, az olyan tevékenység folytatását tervező hírszerző ügynökségnek, amelyre tömeges berendezészavarási parancsot kaphat, a szabályzat alapján be kell szereznie ezt az engedélyt (lásd: a berendezések zavarásáról szóló gyakorlati kódex, 3.24. pontja). Még ha a nyomozati hatáskörökről szóló 2016. évi törvény szerinti berendezészavarási parancsot jogszabály nem írja elő és azt a szabályzat alapján sem szerzik be, a hírszerző ügynökség tevékenységeire számos feltétel és korlátozás vonatkozik a hírszerző ügynökségekről szóló 1994. évi törvény 7. szakasza szerint. Ez magában foglalja különösen a miniszteri engedély követelményét, akinek meg kell győződnie arról, hogy egy intézkedés sem lépi túl a hírszerző ügynökség funkcióinak megfelelő ellátásához szükséges mértéket.

([352]) A nyomozati hatáskörökről szóló 2016. évi törvény 115. szakasza szabályozza a parancs tartalmát, meghatározva, hogy tartalmaznia kell a „célpontot” képező személyek, szervezetek, helyszín vagy személyek csoportja nevét vagy leírását, a nyomozás jellegének leírását és azoknak a tevékenységeknek a leírását, amelyekhez a berendezést használják. Ismertetnie kell a berendezés típusát és azt a magatartást is, amelyre a parancs címzettje jogosult.

([353]) Lásd még a berendezések zavarásáról szóló gyakorlati kódex 5.7. pontját, lásd a 348. lábjegyzetet.

([354]) A nemzetbiztonsági ügynökségek nemzetbiztonsági célokból, súlyos bűncselekmények felderítése érdekében és/vagy az Egyesült Királyság gazdasági jóléte érdekében nyújthatnak be kérelmet a berendezések zavarására vonatkozóan, amennyiben ezek az érdekek relevánsak a nemzetbiztonsági érdekek vonatkozásában is (a nyomozati hatáskörökről szóló 2016. évi törvény 102–103. szakasza). Az ügynökségtől függően a berendezészavarási parancsot bűnüldözési célból lehet kérni, ha ez súlyos bűncselekmény felderítéséhez vagy megelőzéséhez, vagy a halál, bármely személy testi vagy lelki egészsége sérüléséhez vagy károsodásának megelőzéséhez vagy enyhítéséhez, vagy bármely személy testi vagy lelki egészsége sérülésének vagy károsodásának enyhítéséhez szükséges (lásd a nyomozati hatáskörökről szóló 2016. évi törvény 106. szakaszának (1) és (3) bekezdését).

([355]) A nyomozati hatáskörökről szóló 2016. évi törvény 102. szakaszának (1) bekezdése.

([356]) A nyomozati hatáskörökről szóló 2016. évi törvény 129–131. szakasza.

([357]) A nyomozati hatáskörökről szóló 2016. évi törvény 109. szakasza.

([358]) A nyomozati hatáskörökről szóló 2016. évi törvény 109. szakaszának (4) bekezdése.

([359]) A nyomozati hatáskörökről szóló 2016. évi törvény 110. szakasza (3) bekezdésének b) pontja. A berendezések zavarásának gyakorlati kódexe 5.67. pontjának értelmében a sürgősséget az határozza meg, hogy észszerűen beszerezhető-e az igazságügyi biztos jóváhagyása a parancs kiadásához az operatív vagy nyomozati igény kielégítésére rendelkezésre álló idő alatt. A sürgős parancsoknak a következő kategóriák egyikéhez vagy mindkettőhöz kell kapcsolódnia: i. közvetlen életveszély vagy súlyos kár bekövetkezése fenyeget, például, ha egy embert elraboltak, és úgy ítélik meg, hogy életét közvetlen veszély fenyegeti; vagy ii. a hírszerzési információk gyűjtésének vagy a nyomozati lehetőség elvégzésének ideje korlátozott – például egy A osztályú kábítószer-szállítmányt hamarosan be fognak szállítani az Egyesült Királyságba, és a bűnüldöző szervek a súlyos bűncselekmények elkövetői letartóztatásához kívánnak alapot szerezni. Lásd a 348. lábjegyzetet.

([360]) A nyomozati hatáskörökről szóló 2016. évi törvény 108. szakasza.

(215) Végül a célzott lehallgatásra alkalmazandó különleges biztosítékok a berendezések zavarására is vonatkoznak, a parancs időtartamát, megújítását és módosítását, valamint a parlamenti képviselők, az ügyvédi titoktartási kötelezettség alá eső tételek és az újságírói anyagok lehallgatását illetően (további részletekért lásd a (193) preambulumbekezdést).

3.3.1.1.4. Tömeges hatáskör gyakorlása

(216) A tömeges hatásköröket a nyomozati hatáskörökről szóló 2016. évi törvény 6. része szabályozza. Ezenkívül a gyakorlati kódex további részleteket tartalmaz a tömeges hatáskörök használatáról. Noha az Egyesült Királyság jogszabályaiban nincs meghatározva a „tömeges hatáskör", a nyomozati hatáskörökről szóló 2016. évi törvény összefüggésében ez a kormány által különféle eszközökkel megszerzett nagy mennyiségű adat összegyűjtése és megőrzése (azaz a tömeges lehallgatás hatásköre, tömeges adatszerzés, berendezések tömeges zavarása és tömeges személyesadat-állományok), amelyekhez később a hatóságok hozzáférhetnek. Ezt a leírást a „tömeges hatáskörnek" nem minősülő hatáskörökkel való szembeállítással pontosítjuk: nem egyenlő a korlátozások és biztosítékok nélküli, úgynevezett „tömeges megfigyeléssel". Épp ellenkezőleg, az alábbiakban kifejtettek szerint, korlátozásokat és biztosítékokat tartalmaz, amelyek célja annak biztosítása, hogy az adatokhoz való hozzáférés ne válogatás nélkül vagy indokolatlanul történjen ([361]). A tömeges hatáskörök különösen csak akkor használhatók fel, ha a kapcsolat megállapítást nyer a nemzeti hírszerző ügynökség által használni kívánt technikai intézkedés és azon operatív cél között, amelyre az említett intézkedést kérték.

(217) Ezenkívül a tömeges hatáskörök csak a hírszerző ügynökségeknek állnak rendelkezésre, és mindig a miniszter által kiadott és igazságügyi biztos által jóváhagyott parancs alapján. Az információgyűjtés eszközének megválasztásakor figyelembe kell venni, hogy a kérdéses cél elérhető-e „kevésbé beavatkozó jellegű eszközökkel" ([362]). Ez a megközelítés a jogszabály keretrendszeréből következik, amely az arányosság elvére épül, és ezért elsőbbséget élvez a tömeges gyűjtés előtt.

3.3.1.1.4.1. Tömeges lehallgatás és a berendezések tömeges zavarása

(218) A tömeges lehallgatás rendszerét a nyomozati hatáskörökről szóló 2016. évi törvény 6. részének 1. fejezete tartalmazza, míg ugyanezen rész 3. fejezete a berendezések tömeges zavarását szabályozza. Ezek a rendszerek lényegében megegyeznek, ezért az e parancsokra irányadó feltételek és kiegészítő biztosítékok elemzése együtt történik.

i. *A parancs kiadásának feltételei és kritériumai*

(219) A tömeges lehallgatási parancs csak a Brit-szigeteken kívüli magánszemélyek által küldött vagy fogadott kommunikáció lehallgatására ([363]), úgynevezett „tengerentúli kommunikációra" ([364]), valamint egyéb releváns

([361]) Lord David Anderson, a terrorizmusról szóló jogszabályok független felülvizsgálója által a nyomozati hatáskörökről szóló 2016. évi törvény jóváhagyása előtt bemutatott, a tömeges hatáskörről szóló jelentés szerint *„egyértelműnek kell lennie, hogy az adatok tömeges gyűjtése és megőrzése nem egyenlő az úgynevezett »tömeges megfigyeléssel«. Bármely, nevére érdemes jogrendszer korlátozásokat és biztosítékokat tartalmaz, amelyek célja pontosan annak biztosítása, hogy a különleges adatok (…) tárolóihoz való hozzáférést ne válogatás nélkül vagy indokolatlanul biztosítsák. Ilyen korlátozások és biztosítékok mindenképpen léteznek a törvényjavaslatban"*. Lord David Anderson, Jelentés a tömeges hatáskörök felülvizsgálatáról, 2016. augusztus, 1.9. pont (kiemelés hozzáadva), elérhető a következő linken: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF

([362]) A nyomozati hatáskörökről szóló 2016. évi törvény 2,2. szakasza. Lásd például a Kommunikációs adatok tömeges gyűjtése gyakorlati kódexének 4.11. pontját, amely a következő linken érhető el: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf

([363]) A „Brit-szigetek": az Egyesült Királyság, a Csatorna-szigetek és a Man-sziget, és meghatározása az Interpretation Act 1978 elnevezésű (1978. évi értelmezési) törvény 1. mellékletében található, amely a következő linken érhető el https://www.legislation.gov.uk/ukpga/1978/30/schedule/1

([364]) A nyomozati hatáskörökről szóló 2016. évi törvény 136. szakasza szerint a „tengerentúli kommunikáció" a következőket jelenti: i. a Brit-szigeteken kívüli magánszemélyek által küldött kommunikáció, vagy ii. a Brit-szigeteken kívüli magánszemélyek által küldött kommunikáció. Ez a rendszer – amint azt az Egyesült Királyság hatóságai megerősítették – két olyan személy közötti kommunikációt is magában foglalja, amik mindketten a Brit-szigeteken kívül tartózkodnak. Az Emberi Jogok Európai Bíróságának nagytanácsa a Big Brother Watch és társai kontra Egyesült Királyság ügy (lásd a fenti 279. lábjegyzetet) 376. pontjában a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény alapján tömeges lehallgatással rögzíthető kommunikáció hasonló (a „külső kommunikáció"-ra hivatkozással történő) korlátozása vonatkozásában megállapította, hogy az kellően körülhatárolt és előre látható volt.

adatokra és a lehallgatott anyag vizsgálatra történő későbbi kiválasztására ([365]) korlátozódik. A tömeges berendezészavarási parancs ([366]) felhatalmazza a címzettet, hogy biztonságosan zavarjon bármilyen berendezést a tengerentúl kommunikáció (ideértve a beszédet, zenét, hangokat, vizuális képeket vagy bármilyen leírást tartalmazó adatokat), a berendezés adatai (a postai szolgáltatás működését lehetővé tevő vagy megkönnyítő adatok); távközlési rendszer; távközlési szolgáltatás) vagy bármilyen más információ ([367]) gyűjtése céljából.

(220) A miniszter tömeges parancsot csak a hírszerző ügynökség vezetőjének kérelme alapján adhat ki ([368]). A tömeges lehallgatást vagy a berendezések tömeges zavarását engedélyező parancsot csak akkor lehet kiadni, ha ez a nemzetbiztonság érdekében és a súlyos bűncselekmények megelőzésének vagy felderítésének további céljára, vagy adott esetben az Egyesült Királyság gazdasági jólétének érdekében szükséges, ha ez nemzetbiztonsági szempontból releváns ([369]). Ezenkívül a nyomozati hatáskörökről szóló 2016. évi törvény 142. szakaszának (7) bekezdése előírja, hogy a tömeges lehallgatási parancsot részletesebben meg kell határozni a „nemzetbiztonsági érdekekre", „az Egyesült Királyság gazdasági jólétére" és a „súlyos bűncselekmények megelőzésére és az ellenük való küzdelemre" történő egyszerű hivatkozásnál, hanem kapcsolatot kell teremteni a kért intézkedés és egy vagy több operatív cél között, amelyet fel kell tüntetni a parancsban.

(221) Az operatív cél megválasztása többlépcsős folyamat eredménye. A 142. szakasz (4) bekezdése előírja, hogy a parancsban meghatározott operatív célokat a hírszerző ügynökség vezetői által vezetett listában kell meghatározni, az általuk operatív célnak tekintett azon célokként, amelyek érdekében a lehallgatott tartalom vagy tömeges lehallgatással nyert másodlagos adatok vizsgálatra kiválasztása indokolt lehet. Az operatív célok felsorolását a miniszternek kell jóváhagynia. A miniszter csak akkor adhatja meg a jóváhagyást, ha meggyőződik arról, hogy az operatív célt a parancs engedélyezésének általános indokainál (nemzetbiztonság vagy nemzetbiztonság és gazdasági jólét vagy a súlyos bűncselekmények megelőzése) részletesebben meghatározták ([370]). A miniszternek minden releváns három hónapos időszak végén át kell adnia az operatív célok listájának másolatát a parlamenti ISC-nek. Végül a miniszterelnöknek évente legalább egyszer felül kell vizsgálnia az operatív célok listáját ([371]). Ahogyan azt a Legfelsőbb Bíróság megjegyezte, „ezeket nem szabad jelentéktelen biztosítékként lebecsülni, mivel az elszámoltathatóság módjainak bonyolult szövetét alkotják, amely magában foglalja a Parlamentet és a kormánytagokat is a legmagasabb szinten" ([372]).

(222) Az említett operatív célok korlátozzák a lehallgatási anyag vizsgálati szakaszra kiválasztásának terjedelmét is. A tömeges engedély alapján összegyűjtött bármely anyag vizsgálatra való kiválasztását az operatív cél(ok)ra figyelemmel kell indokolni. Amint azt az Egyesült Királyság hatóságai kifejtették, ez azt jelenti, hogy a miniszternek már a parancs kiadásának szakaszában értékelnie kell a vizsgálat gyakorlati elrendezését, elegendő részletet megadva a nyomozati hatáskörökről szóló 2016. évi törvény 152. és 193. szakasza szerinti törvényi kötelezettségek teljesítéséhez ([373]). A miniszternek az említett elrendezéssel kapcsolatban adott részletes tájékoztatásnak tartalmaznia kell például az arra vonatkozó információkat (ha vannak), hogy a szűrési szabályok miként változhatnak a parancs hatálya alatt ([374]). A folyamattal és a szűrési és vizsgálati szakaszokban alkalmazott biztosítékokkal kapcsolatos további részletek a (229) below preambulumbekezdésben találhatók.

([365]) A nyomozati hatáskörökről szóló 2016. évi törvény 136. szakaszának (4) bekezdése. Az Egyesült Királyság kormányától kapott magyarázatok szerint a tömeges lehallgatás felhasználható például az Egyesült Királyság nemzetbiztonságát érintő, eddig ismeretlen fenyegetések azonosítására, a lehallgatott anyagok szűrésével és elemzésével hírszerzési értékű kommunikáció azonosítása érdekében (Az Egyesült Királyság magyarázata, H szakasz: Nemzetbiztonság, 27–28. o., lásd a 29. lábjegyzetet). Amint azt az Egyesült Királyság hatóságai kifejtették, ilyen eszközök felhasználhatók az érdeklődésre számot tartó témák közötti kapcsolatok létrehozására, valamint olyan egyének tevékenysége nyomainak felkutatására, akik esetleg még nem ismertek, de akik egy vizsgálat során felbukkannak, valamint olyan tevékenységi minták azonosítására, amelyek veszélyt jelenthetnek az Egyesült Királyságra.

([366]) A nyomozati hatáskörökről szóló 2016. évi törvény 13. szakaszának (1) bekezdésével összhangban a hírszerző ügynökség által a berendezések zavarásának felhasználásához a nyomozati hatáskörökről szóló 2016. évi törvény szerint engedély szükséges, feltéve, hogy fennáll a „kapcsolódás a Brit-szigetekhez", lásd a (211) preambulumbekezdést.

([367]) A nyomozati hatáskörökről szóló 2016. évi törvény 176. szakasza. A berendezések tömeges zavarására vonatkozó parancs nem engedélyezhet olyan magatartást, amely (amennyiben nem jogszerű felhatalmazással történik) jogellenes lehallgatást valósít meg (kivéve a tárolt kommunikációval kapcsolatos lehallgatást). Az Egyesült Királyság magyarázata szerint a gyűjtött információkra szükség lehet az érdeklődésre számot tartó érintettek azonosításához, és ezek általában kellően nagyszabású műveletek lesznek (az Egyesült Királyság magyarázata, H. szakasz: Nemzetbiztonság, 28. o., lásd a 29. lábjegyzetet.

([368]) A nyomozati hatáskörökről szóló 2016. évi törvény 138. szakaszának (1) bekezdése és 178. szakaszának (1) bekezdése.

([369]) A nyomozati hatáskörökről szóló 2016. évi törvény 138. szakaszának (2) bekezdése és 178. szakaszának (2) bekezdése.

([370]) Az Egyesült Királyság hatóságainak magyarázata szerint például egy operatív cél az intézkedés hatályát egy adott földrajzi területen fennálló fenyegetésre korlátozhatja.

([371]) A nyomozati hatáskörökről szóló 2016. évi törvény 142. szakaszának (4)–(10) bekezdése.

([372]) High Court of Justice, Liberty-ügy (2019 EWHC 2057 (Admin)), 167. pont.

([373]) A nyomozati hatáskörökről szóló 2016. évi törvény 152. és 193. szakasza előírja a következőket: a) a vizsgálatra történő kiválasztást csak a parancsban meghatározott operatív célokból hajtják végre, b) a vizsgálatra való kiválasztás minden körülmények között szükséges és arányos, és c) a vizsgálatra történő kiválasztás nem sérti azon anyag kiválasztásának és azon közlemények azonosításának tilalmát, amelyeket akkoriban ismerten a Brit-szigeteken tartózkodó személyek küldtek vagy nekik szántak.

([374]) Lásd: A kommunikáció lehallgatásának gyakorlati kódexe, 6.6. pont, lásd a 278. lábjegyzetet.

(223) Tömeges hatáskör csak akkor engedélyezhető, ha az arányos az elérni kívánt céllal ([375]). A lehallgatás gyakorlati kódexében meghatározottak szerint az arányosság minden értékelése magában foglalja „a magánéletbe való beavatkozás súlyossága (és a 2. szakasz (2) bekezdésében meghatározott egyéb szempontok) és a tevékenység nyomozati, operatív vagy kapacitási szükségessége egyensúlyának megteremtését. Az engedélyezett magatartásnak reális kilátást kell kínálnia a várt haszon elérésére, és nem lehet aránytalan vagy önkényes" ([376]). Amint már említést nyert, ez a gyakorlatban azt jelenti, hogy az arányossági teszt az elérni kívánt célok („operatív cél(ok)") és a rendelkezésre álló technikai lehetőségek (pl. célzott vagy tömeges lehallgatás, berendezés interferencia, kommunikációs adatok) egyensúlyának megteremtése, a legkevésbé beavatkozó jellegű eszközöket előnyben részesítve (lásd a (181) és (182) above preambulumbekezdést). Ha több intézkedés felel meg a célnak, akkor a kevésbé beavatkozó jellegű eszközöket kell előnyben részesíteni.

(224) A kért intézkedés arányosságának értékelése során további biztosítékot nyújt az a tény, hogy a miniszternek meg kell kapnia az értékelés megfelelő elvégzéséhez szükséges információkat. A lehallgatás gyakorlati kódexe és a berendezések zavarásáról szóló gyakorlati kódex előírja különösen, hogy az illetékes hatóság által benyújtott kérelemben fel kell tüntetni az alkalmazás előzményeit, a lehallgatandó kommunikáció leírását és azon távközlési szolgáltatókat, akiknek a segítségére szükség van, az engedélyezendő magatartás, az operatív célok leírását és annak magyarázatát, hogy miért szükséges és arányos a magatartás ([377]).

(225) Végül és kiemelten, a miniszternek a parancs kiadásáról szóló döntését független igazságügyi biztosnak kell jóváhagynia, aki felméri a javasolt intézkedés szükségességének és arányosságának értékelését, ugyanazokat az elveket alkalmazva, amelyeket a bíróság a bírósági felülvizsgálat alkalmával ([378]). Konkrétabban, az igazságügyi biztos felülvizsgálja a miniszter következtetéseit arra vonatkozóan, hogy szükséges-e a határozat, és hogy a magatartás arányos-e a nyomozati hatáskörökről szóló 2016. évi törvény 2. szakaszának 2. pontjában meghatározott elvekre (a magánélet védelmével kapcsolatos általános kötelezettségekre) figyelemmel. Az igazságügyi biztos megvizsgálja a miniszter következtetéseit arra vonatkozóan is, hogy a parancsban meghatározott operatív célok mindegyike olyan-e, amelyhez a vizsgálat szükséges, vagy szükséges lehet. Ha az igazságügyi biztos elutasítja a parancs kiadásáról szóló határozat jóváhagyását, a miniszter: i. elfogadja a határozatot, és ezért nem adja ki a parancsot; vagy ii. határozathozatal céljából továbbítja az ügyet a nyomozati hatáskörök biztosához (kivéve, ha a nyomozati hatáskörök biztosa hozta meg az eredeti döntést) ([379]).

ii. *További biztosítékok*

(226) A nyomozati hatáskörökről szóló 2016. évi törvény további korlátokat vezetett be a tömeges parancsok időtartamára, megújítására és módosítására. A parancs időtartama legfeljebb hat hónap, és a megújítási vagy módosítási döntéseket (kivéve a kisebb módosításokat) az igazságügyi biztosnak is jóvá kell hagynia ([380]). A lehallgatás gyakorlati kódexe és a berendezés zavarásáról szóló gyakorlati kódex meghatározta, hogy a parancs operatív céljainak megváltoztatása a parancs jelentős módosításának tekinthető ([381]).

([375]) A nyomozati hatáskörökről szóló 2016. évi törvény 138. szakasza (1) bekezdésének b) és c) pontja 178. szakaszának b) és c) pontja.

([376]) A kommunikáció lehallgatásának gyakorlati kódexe, 4.10. pont, lásd a 278. lábjegyzetet.

([377]) A kommunikáció lehallgatásának gyakorlati kódexe, 6.20. pont, lásd a 278. lábjegyzetet, és a berendezés zavarásáról szóló gyakorlati kódex 6.13. szakasza, lásd a 348. lábjegyzetet.

([378]) A nyomozati hatáskörökről szóló 2016. évi törvény 138. szakasza (1) bekezdésének g) pontja és 178. szakasza (1) bekezdésének f) pontja. Az Emberi Jogok Európai Bírósága a tömeges lehallgatás keretében történő visszaélések ellen egy független testület előzetes engedélyét fontos garanciának minősítette. Emberi Jogok Európai Bírósága (nagytanács), Big Brother Watch és társai kontra Egyesült Királyság ügy (lásd a fenti 269. lábjegyzetet), 351. és 352. pont. Fontos szem előtt tartani, hogy ez az ítélet a korábbi jogi keretre (a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény) vonatkozott, amely nem tartalmazta a nyomozati hatáskörökről szóló 2016. évi törvény által bevezetett biztosítékok egy részét (ideértve a független igazságügyi biztos előzetes engedélyét is).

([379]) A nyomozati hatáskörökről szóló 2016. évi törvény 159. szakaszának (3) és (4) bekezdése.

([380]) A nyomozati hatáskörökről szóló 2016. évi törvény 143–146. szakasz és 184–188. szakasza. Sürgős módosítás esetén a miniszter jóváhagyás nélkül elvégezheti a módosítást, de erről értesítenie kell a biztost, majd a biztosnak döntenie kell a módosítás jóváhagyásáról vagy elutasításáról (a nyomozati hatáskörökről szóló 2016. évi törvény 147. szakasza). A parancsot vissza kell vonni, ha a parancs már nem szükséges vagy arányos, vagy ha a lehallgatott tartalom, metaadatok vagy az engedély alapján megszerzett egyéb adatok vizsgálata már nem szükséges a parancsban meghatározott operatív célok egyikének sem (a nyomozati hatáskörökről szóló 2016. évi törvény 148. szakasza és 189. szakasza).

([381]) A kommunikáció lehallgatásának gyakorlati kódexe, 6.44–6.47. pont, lásd a 278. lábjegyzetet és a berendezések zavarásáról szóló gyakorlati kódex 6.48. szakasza, lásd a 348. lábjegyzetet.

(227) A célzott lehallgatásra előírtakhoz hasonlóan a nyomozati hatáskörökről szóló 2016. évi törvény 6. része előírja, hogy a miniszternek gondoskodnia kell arról, hogy hatályban legyenek azok az intézkedések, amelyek biztosítékot nyújtanak a parancs alapján megszerzett anyag megőrzésére és közlésére ([382]), valamint a tengerentúli közlésre ([383]). A nyomozati hatáskörökről szóló 2016. évi törvény 150. szakaszának (5) bekezdése és 191. szakaszának (5) bekezdése előírja különösen, hogy az engedély alapján összegyűjtött anyagok bármelyikéről készült minden másolatot biztonságos módon kell tárolni, és meg kell semmisíteni, amint már megőrzésére nincsenek releváns okok, míg a 150. szakasz (2) bekezdése és a 191. szakasz (2) bekezdése előírja, hogy azoknak a személyeknek a számát, akikkel az anyagot közlik, valamint az anyag közlésének, hozzáférhetővé tételének vagy másolásának mértékét a törvényi célokból szükséges minimumra kell korlátozni ([384]).

(228) Végül ha a tömeges lehallgatással vagy tömeges berendezészavarással lehallgatott anyagot továbbítani kell egy harmadik országnak („tengerentúli közlés"), a nyomozati hatáskörökről szóló 2016. évi törvény előírja, hogy a miniszternek gondoskodnia kell az azt biztosító megfelelő intézkedésekről, hogy a biztonság, a megőrzés és a közlés terén hasonló biztosítékok létezzenek ebben a harmadik országban ([385]). Emellett a 2018. évi adatvédelmi törvény 109. szakasza külön követelményeket tartalmaz a személyes adatok hírszerző ügynökség által harmadik országokba vagy nemzetközi szervezetekhez történő továbbítására, és nem engedélyezi adatok továbbítását az Egyesült Királyságon kívüli országba vagy területre vagy egy nemzetközi szervezethez, kivéve, ha az adattovábbítás az adatkezelő törvényi funkcióinak vagy más, a biztonsági szolgálatokról szóló 1989. évi törvény 2. szakasza (2) bekezdésének a) pontjában vagy a hírszerző ügynökségekről szóló 1994. évi törvény 2. szakasza (2) bekezdésének a) pontjában és 4. szakasza (2) bekezdésének a) pontjában előírt más céloknak megfelelően szükséges és arányos ([386]). Fontos, hogy ezek a követelmények azokban az esetekben is érvényesülnek, amikor a 2018. évi adatvédelmi törvény 110. szakasza szerinti nemzetbiztonsági kivételre hivatkoznak, mivel a 2018. évi adatvédelmi törvény 110. szakasza nem sorolja fel a 2018. évi adatvédelmi törvény 109. szakaszát azon rendelkezések között, amelyek alkalmazása mellőzhető, ha a nemzetbiztonság védelme érdekében bizonyos rendelkezések alóli kivételre van szükség.

(229) Miután a parancsot jóváhagyták és a tömeges adatgyűjtés megtörtént, az adatokat a vizsgálat előtt válogatják. A kiválasztási és vizsgálati fázisban az elemzőnek egy további arányossági tesztet kell végeznie, amely a megbízásban szereplő operatív célok (és az esetlegesen létező szűrési szabályok) alapján meghatározza a kiválasztás kritériumait. A nyomozati hatáskörökről szóló törvény 152. és 193. szakasza előírja, hogy a miniszter a parancs kiadásakor gondoskodik arról, hogy azt garantáló intézkedések legyenek érvényben, hogy az anyag kiválasztása csak a meghatározott operatív célokra történhessen, és hogy ez minden körülmények között szükséges és arányos legyen. Ebben a tekintetben az Egyesült Királyság hatóságai pontosították, hogy a tömegesen lehallgatott anyagot elsősorban automatizált szűréssel válogatják le azzal a céllal, hogy kiszűrik azokat az adatokat, amelyek valószínűleg nemzetbiztonsági szempontból érdektelenek. A szűrők időről időre változnak (az internetes forgalmi minták, típusok és protokollok változásával), és a technológiától és az operatív körülményektől függenek. Ezt a fázist követően adatok csak akkor választhatók ki vizsgálatra, ha azok a parancsban meghatározott operatív célok szempontjából relevánsak ([387]). A nyomozati hatáskörökről szóló 2016. évi törvény által az összegyűjtött anyag vizsgálatához nyújtott biztosítékok minden típusú adatra vonatkoznak (mind a lehallgatott tartalomra, mind a másodlagos adatokra) ([388]). A nyomozati hatáskörökről szóló 2016. évi törvény 152. és 193. szakasza is általános tilalmat ír elő a Brit-szigeteken tartózkodó személyek által küldött vagy nekik szánt beszélgetésekre utaló anyagok vizsgálatra kiválasztására. Ha a hatóságok meg kívánják vizsgálni az említett anyagokat, kérelmet nyújtanak be a miniszter által kiállított és egy igazságügyi biztos által jóváhagyott, a nyomozati hatáskörökről szóló 2016. évi törvény 2. és 4. része szerinti célzott vizsgálati parancs iránt ([389]). Ha valaki a jogszabályokban meghatározott követelményekbe ütközően ([390]) szándékosan választ ki lehallgatott tartalmat vizsgálatra, bűncselekményt követ el ([391]).

([382]) A nyomozati hatáskörökről szóló 2016. évi törvény 156. szakasza.
([383]) A nyomozati hatáskörökről szóló 2016. évi törvény 150. és 191. szakasza.
([384]) Az Emberi Jogok Európai Bíróságának nagytanácsa a Big Brother Watch és mások kontra Egyesült Királyság ügyben (lásd a fenti 268 lábjegyzetet) fenntartotta a megőrzésre, hozzáférésre és nyilvánosságra hozatalra vonatkozó további biztosítékok rendszerét, amelyet a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény biztosított, lásd a 392–394. és a 402–405. bekezdést. A nyomozati hatáskörökről szóló 2016. évi törvény a biztosítékok hasonló rendszerét írja elő.
([385]) A nyomozati hatáskörökről szóló 2016. évi törvény 151. és 192. szakasza.
([386]) E célokról részletesebben lásd a 312 lábjegyzetet.
([387]) A kommunikáció lehallgatására vonatkozó kódexek e tekintetben meghatározzák, hogy „Ezek a feldolgozó rendszerek olyan kommunikációs kapcsolatokból vagy jelekből származó adatokat kezelnek, amelyeket a lehallgató hatóság lehallgatásra kiválasztott. Ezután bizonyos mértékű szűrést alkalmaznak az említett kapcsolatok és jelek forgalmára, amelynek célja a potenciálisan hírszerzési értéket képviselő kommunikációtípusok kiválasztása, elvetve ugyanakkor azokat, amelyek hírszerzési értéke a legkevésbé valószínű. Ennek a feldolgozó rendszerek között esetlegesen eltérő szűrésnek az eredményeként az említett kapcsolatokon és jeleken keresztül zajlott kommunikáció jelentős részét automatikusan elvetik. Ezután további összetett keresésekre kerülhet sor, amelyek kiszűrik a legnagyobb valószínűséggel hírszerzés értéket hordozó és az ügynökség törvényi funkcióihoz kapcsolódó kommunikációt. Ezeket a kommunikációkat ezután kiválaszthatják a parancsban meghatározott egy vagy több operatív célból történő vizsgálatra, amennyiben a szükségesség és az arányosság feltételei teljesülnek. Csak a ki nem szűrt elemek választhatók ki felhatalmazott személyek általi vizsgálatra" (A kommunikáció lehallgatására vonatkozó gyakorlati kódexek, 6.6. pont, lásd a 278. lábjegyzetet).
([388]) Lásd a nyomozati hatáskörökről szóló 2016. évi törvény 152. szakasza (1) bekezdésének a) és b) pontját, amelyek szerint mindkét adattípus (mind a lehallgatott tartalom, mind a másodlagos adatok) esetében a vizsgálat csak a meghatározott célból végezhető, és annak minden körülmények között szükségesnek és arányosnak kell lennie.
([389]) Nincs szükség ilyen típusú parancsra, ha a Brit-szigeteken tartózkodó egyénekre vonatkozó adatok „másodlagos adatok" (a nyomozati hatáskörökről szóló 2016. évi törvény 152. szakasza (1) bekezdésének c) pontja).
([390]) A nyomozati hatáskörökről szóló 2016. évi törvény 152. és 193. szakasza.
([391]) A nyomozati hatáskörökről szóló 2016. évi törvény 155. és 196. szakasza.

(230) Az elemző által a kiválasztott anyagon elvégzett értékelést a nyomozási biztos utólag felügyeli, aki értékeli a nyomozati hatáskörökről szóló 2016. évi törvényben a vizsgálati szakaszra meghatározott különleges biztosítékok betartását ([392]) (lásd még a (229) preambulumbekezdést). A nyomozási biztosnak folyamatosan figyelemmel kell kísérnie a hatóságok által a nyomozati hatáskörökről szóló 2016. évi törvényben említett nyomozati hatáskörök gyakorlását (ideértve az ellenőrzés, felügyelet és vizsgálat útján történő figyelemmel kísérést is) ([393]). Ebben a tekintetben a lehallgatás gyakorlati kódexe és a berendezések zavarásáról szóló gyakorlati kódex egyértelművé teszi, hogy az ügynökségnek nyilvántartást kell vezetnie későbbi vizsgálatok és ellenőrzések céljára, és ezekben a nyilvántartásokban fel kell tüntetni, hogy miért szükséges és arányos az anyaghoz a felhatalmazott személyeknek hozzáférni, a vonatkozó operatív célokkal együtt ([394]). Például a 2018. évi éves jelentésben a Nyomozati Hatáskörök Biztosának Hivatala (nyomozási biztos hivatala) ([395]) arra a következtetésre jutott, hogy az elemző által bizonyos tömegesen összegyűjtött anyagok vizsgálatához rögzített indokolások megfeleltek az előírt arányossági mércének, elegendő részletességgel megadva a „lekérdezések" okait az elérendő célokkal kapcsolatban ([396]). A nyomozási biztos hivatala 2019-es jelentésében a tömeges hatáskörökkel kapcsolatban egyértelműen kijelentette, hogy szándékában áll folytatni a tömeges lehallgatások ellenőrzését, ideértve a kiválasztási és a keresési szempontok részletes vizsgálatát ([397]). Emellett a továbbiakban is alaposan, esetenként ellenőrzi a (tömeges vagy célzott) berendezészavarási tevékenység megválasztását, mind a parancs iránti kérelmek duplán ellenőrzött eljárás szerinti elbírálása, mind az ellenőrzések során" ([398]). Ezt a további nyomon követést kellően figyelembe fogják venni a (281)–(284) preambulumbekezdésben említett, az e határozattal kapcsolatos bizottsági nyomon követés során.

3.3.1.1.4.2. Távközlési adatok tömeges gyűjtése

(231) A nyomozati hatáskörökről szóló 2016. évi törvény 6. részének 2. fejezete szabályozza a tömeges adatgyűjtési parancsokat, amelyek felhatalmazzák a címzettet arra, hogy a távközlési szolgáltatótól megkövetelje az üzemeltető birtokában lévő bármely kommunikációs adat közlését vagy gyűjtését. Ezek a parancsok felhatalmazzák a megkereső hatóságot az adatok vizsgálat további szakaszára történő kiválasztására. A kommunikációs adatok célzott megőrzéséhez és gyűjtéséhez hasonlóan (lásd a (199) preambulumbekezdést) a kommunikációs adatok tömeges gyűjtése általában nem érinti az e határozat alapján az Egyesült Királyságba továbbított uniós érintettek személyes adatait. A kommunikációs adatok közlésének kötelezettsége a nyomozati hatáskörökről szóló 2016. évi törvény 6. részének 2. fejezete szerint azokra az adatokra terjed ki, amelyeket az Egyesült Királyság telekommunikációs szolgáltatói gyűjtenek közvetlenül a távközlési szolgáltatás felhasználóitól ([399]). Ez a fajta „ügyfélalapú" feldolgozás általában nem jár e határozat alapján adattovábbítással, vagyis uniós adatkezelőtől/adatfeldolgozótól egyesült királyságbeli adatkezelőhöz/adatfeldolgozóhoz történő adattovábbítással.

(232) A teljesség kedvéért azonban a tömeges kommunikációs adatok gyűjtését szabályozó feltételeket és biztosítékokat az alábbiakban ismertetjük.

([392]) A nyomozati hatáskörökről szóló 2016. évi törvény 152. és 193. szakasza.

([393]) A nyomozati hatáskörökről szóló 2016. évi törvény 229. szakasza.

([394]) A kommunikáció lehallgatásának gyakorlati kódexe, 6.74. pont, lásd a 278. lábjegyzetet, és a berendezések zavarásáról szóló gyakorlati kódex, 6.78. pont, lásd a 348. lábjegyzetet.

([395]) A nyomozási biztos hivatala a nyomozati hatáskörökről szóló 2016. évi törvény 238. szakasza alapján jött létre, hogy a nyomozási biztost ellássa a feladatai ellátásához szükséges személyzettel, helyszínnel, berendezésekkel és egyéb létesítményekkel és szolgáltatásokkal (lásd a (251) preambulumbekezdést).

([396]) A nyomozási biztos hivatalának 2018. évi éves jelentése meghatározta, hogy a Kormányzati Kommunikációs Központ elemzői által rögzített indoklások „megfelelnek az előírt követelményeknek, és az elemzők kellő részletességgel figyelembe veszik a tömeges adatok lekérdezésének arányosságát". A nyomozati hatáskörök biztosának 2018. évi éves jelentése, 6.22. pont, lásd a 464. lábjegyzetet.

([397]) A nyomozati hatáskörök biztosának 2019. évi éves jelentése, 7.6. pont, lásd a 463. lábjegyzetet.

([398]) A nyomozati hatáskörök biztosának 2019. évi éves jelentése, 10.22. pont, lásd a 463. lábjegyzetet.

([399]) Ez a kommunikációs adatoknak a nyomozati hatáskörökről szóló 2016. évi törvény 261. szakaszának (5) bekezdésében szereplő meghatározásából következik, amely szerint a kommunikációs adatokat egy távközlési szolgáltató birtokolja vagy gyűjti, és vagy egy távközlési szolgáltatás felhasználójáról szól, és ennek a szolgáltatásnak a nyújtására vonatkozik vagy egy kommunikáció részeként, ahhoz csatolva vagy logikailag kapcsolódva (lásd még a Kommunikációs adatok tömeges gyűjtéséről szóló gyakorlati kódexet, amely a következő linken érhető el): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf 2.15–2.22. pont). Ezenkívül a távközlési szolgáltatónak a nyomozati hatáskörökről szóló 2016. évi törvény 261. szakaszának (10) bekezdésében szereplő meghatározása megköveteli, hogy a távközlési szolgáltató olyan személy legyen, aki telekommunikációs szolgáltatást kínál vagy nyújt az Egyesült Királyságban tartózkodó személyeknek, vagy olyan telekommunikációs rendszert irányít vagy biztosít, amely (teljes egészében vagy részben) az Egyesült Királyságban található vagy onnan irányítják. Ezek a meghatározások egyértelművé teszik, hogy a nyomozati hatáskörökről szóló 2016. évi törvény alapján nem róhatók kötelezettségek azokra a távközlési szolgáltatókra, akiknek a berendezései nincsenek az Egyesült Királyságban vagy nem az Egyesült Királyság ellenőrzése alatt állnak, és akik nem kínálnak vagy nyújtanak szolgáltatásokat az Egyesült Királyságban tartózkodó személyeknek (lásd még: A kommunikáció tömeges beszerzésének gyakorlati kódexe) Adatok, 2.2. pont). Ha uniós előfizetők (függetlenül attól, hogy az EU-ban vagy az Egyesült Királyságban tartózkodnak-e) igénybe veszik a szolgáltatásokat az Egyesült Királyságban, a szolgáltatás nyújtásával kapcsolatos bármely kommunikációt közvetlenül az Egyesült Királyság szolgáltatója gyűjti össze, és nem az EU-ból kerül továbbításra.

(233) A nyomozati hatáskörökről szóló 2016. évi törvény váltja fel a tömeges hírközlési adatok gyűjtésére vonatkozó azon jogszabályokat, amelyeket az EUB a Privacy International ügyben hozott ítéletében tárgyalt. Az abban az ügyben tárgyalt jogszabályt hatályon kívül helyezték, és az új rendszer konkrét feltételeket és biztosítékokat ír elő, amelyek alapján az említett intézkedés engedélyezhető.

(234) Különösen eltérően a korábbi rendszertől, amelynek értelmében a miniszternek teljes mérlegelési jogköre volt az intézkedés engedélyezésére ([400]), a nyomozati hatáskörökről szóló 2016. évi törvény megköveteli, hogy a miniszter csak akkor adjon ki parancsot, ha az intézkedés szükséges és arányos. Ez a gyakorlatban azt jelenti, hogy összefüggésnek kell lennie az adatokhoz való hozzáférés és az elérni kívánt cél között ([401]). Pontosabban, a miniszternek értékelnie kell a kapcsolat fennállását a kért intézkedés és a parancsban (lásd a (219) preambulum-bekezdést) feltüntetett egy vagy több „operatív cél" között az arányosság értékelése tekintetében, a vonatkozó gyakorlati kódex előírja, hogy „a miniszternek figyelembe kell vennie, hogy a parancs által elérni kívánt cél elérhető-e más, kevésbé beavatkozó jellegű eszközökkel (a törvény 2. szakasza (2) bekezdésének a) pontja). Például a szükséges információk gyűjtése kevésbé tolakodó hatáskörrel, például a kommunikációs adatok célzott gyűjtésével" ([402]).

(235) Az említett értékelés elvégzéséhez a miniszter azokra az információkra támaszkodik, amelyeket a hírszerzési vezetők ([403]) kötelesek benyújtani kérelmükben, például azok az indokok, amelyek miatt az intézkedést valamely jogszabályi alapon szükségesnek tartják, és annak oka, amiért az elérni kívánt célokat más, kevésbé beavatkozó jellegű eszközökkel észszerűen nem lehetne elérni ([404]). Ezenkívül az operatív célok korlátozzák azt a hatókört, amelyre a parancs alapján megszerzett adatok megvizsgálhatók ([405]). Amint azt a vonatkozó gyakorlati szabályzat előírja, az operatív céloknak egyértelmű követelményt kell tartalmazniuk, és elegendően részletesnek kell lenniük ahhoz, hogy a miniszter meggyőződhessen arról, hogy a gyűjtött adatokat csak konkrét okokból lehet megvizsgálásra kiválasztani ([406]). Valójában a miniszternek meg kell győződnie arról, hogy a parancs engedélyezése előtt vannak-e külön rendelkezések annak biztosítására, hogy a valamely operatív és törvényi célra szükségesnek minősülő anyagot válasszanak ki vizsgálat, és annak minden körülmények között arányosnak és szükségesnek kell lennie. Ez a külön követelmény, amelyet a nyomozati hatáskörökről szóló 2016. évi törvény 158. és 172. szakasza tükröz ([407]) a kiválasztás során alkalmazott kritériumok szükségességének és arányosságának előzetes értékelését illetően, a nyomozati hatáskörökről szóló 2016. évi törvény által bevezetett rendszer másik fontos újdonságát képezi a korábban hatályos rendszerhez képest.

(236) A nyomozati hatáskörökről szóló 2016. évi törvény bevezette a miniszter kötelességét is annak biztosítására, hogy a kommunikációs adatok tömeges gyűjtésére vonatkozó parancs kiadása előtt meghatározott korlátozások legyenek érvényben az összegyűjtött személyes adatok biztonságára, megőrzésére és közléséra vonatkozóan ([408]). Tengerentúli közlés esetén a (227) preambulumbekezdésben a tömeges lehallgatásra és berendezések tömeges zavarására leírt biztosítékokat ebben az összefüggésben is alkalmazni kell ([409]). A jogszabályok további korlátokat rögzítenek a tömeges parancsok időtartamára ([410]), megújítására ([411]) és módosítására ([412]) vonatkozóan.

(237) Fontos, hogy a többi tömeges hatáskörhöz hasonlóan a parancs kiadása előtt a miniszternek meg kell szereznie egy igazságügyi biztos jóváhagyását ([413]). Ez a nyomozati hatáskörökről szóló 2016. évi törvény által bevezetett rendszer kulcsfontosságú jellemzője.

([400]) Az 1984-es telekommunikációs törvény 94. szakaszának (1) bekezdése előírta, hogy a miniszter kiadhat „általános jellegű utasításokat, amelyeket a miniszter a nemzetbiztonság érdekében szükségesnek vagy célszerűnek tekint (…)" (lásd a 451. lábjegyzetet).

([401]) Lásd: Privacy International ügy, 78. pont

([402]) Lásd: A kommunikációs adatok tömeges gyűjtésének gyakorlati szabályzata, 4.11. pont (lásd a 399. lábjegyzetet).

([403]) Tömeges adatgyűjtési parancsot csak a hírszerző ügynökségek vezetői kérhetnek, akik az alábbiak: i. a Biztonsági Szolgálat főigazgatója; ii. a Titkosszolgálat vezetője; vagy iii. a Kormányzati Kommunikációs Központ igazgatója (lásd a nyomozati hatáskörökről szóló 2016. évi törvény 158. és 263. szakaszát).

([404]) A kommunikációs adatok tömeges gyűjtésének gyakorlati szabályzata, 4.5. pont (lásd a 399. lábjegyzetet).

([405]) A nyomozati hatáskörökről szóló 2016. évi törvény 161. szakasza szerint a parancsban meghatározott operatív céloknak szerepelniük kell a hírszerző ügynökségek vezetőinek által vezetett listán (a továbbiakban: az operatív célok listája), olyan okként, amely a tömeges adatgyűjtési paranccsal nyert kommunikációs adatok vizsgálatra kiválasztásához operatív célnak minősül.

([406]) A kommunikációs adatok tömeges gyűjtésének gyakorlati szabályzata, 6.6. pont (lásd a 399. lábjegyzetet).

([407]) A nyomozati hatáskörökről szóló 2016. évi törvény 172. szakasza előírja, hogy külön biztosítékokat kell bevezetni a tömegesen gyűjtött kommunikáció vizsgálatához szükséges szűrési és kiválasztási szakaszra. Ezenkívül az e biztosítékok megsértésével történő szándékos vizsgálat egyben bűncselekmény is (lásd a nyomozati hatáskörökről szóló 2016. évi törvény 173. szakaszát).

([408]) A nyomozati hatáskörökről szóló 2016. évi törvény 171. szakasza.

([409]) A nyomozati hatáskörökről szóló 2016. évi törvény 171. szakaszának (9) bekezdése.

([410]) A nyomozati hatáskörökről szóló 2016. évi törvény 162. szakasza.

([411]) A nyomozati hatáskörökről szóló 2016. évi törvény 163. szakasza.

([412]) A nyomozati hatáskörökről szóló 2016. évi törvény 164–166. szakasza.

([413]) A nyomozati hatáskörökről szóló 2016. évi törvény 159. szakasza.

(238) A nyomozási biztos a tömegesen gyűjtött anyagok (kommunikációs adatok) vizsgálati eljárását utólag felügyeli (lásd a (254) below preambulumbekezdést). E tekintetben a nyomozati hatáskörökről szóló 2016. évi törvény bevezette azt a követelményt, hogy a vizsgálatot végző hírszerző elemzőnek az adatok vizsgálatra kiválasztása előtt fel kell jegyeznie, hogy miért szükséges és arányos a javasolt vizsgálat egy meghatározott operatív cél érdekében ([414]). A nyomozási biztos hivatala 2019. évi éves jelentésében a Kormányzati Kommunikációs Központ és az MI5 gyakorlata kapcsán kiderült, hogy „a tömeges kommunikációs adatok kritikus szerepe a Kormányzati Kommunikációs Központban végzett tevékenységek körében jól megfogalmazódott az általunk ellenőrzött esetmunkában. Figyelembe vettük a kért adatok jellegét és a feltüntetett hírszerzési követelményeket, és meggyőződtünk arról, hogy a dokumentáció bizonyította, hogy megközelítésük szükséges és arányos volt" ([415]). Az MI5 által rögzített indokolások jó színvonalúak voltak, és kielégítették a szükségesség és az arányosság elvét" ([416]).

3.3.1.1.4.3. Tömeges személyesadat-állományok megőrzése és vizsgálata

(239) A tömeges személyesadat-állományokra vonatkozó parancs ([417]) felhatalmazza a hírszerző ügynökségeket olyan adatállományok megőrzésére és megvizsgálására, amelyek számos személyre vonatkozó személyes adatokat tartalmaznak. Az Egyesült Királyság hatóságainak magyarázata szerint az említett adatállományok elemzése „az egyetlen módja annak, hogy az UKIC előrelépjen a nyomozásban és azonosítsa a terroristákat igen csekély hírszerzési nyom alapján, vagy amikor a kommunikációjukat szándékosan leplezik" ([418]). Két típusú parancs létezik: „csoportos tömeges személyesadat-állományokra vonatkozó parancs" ([419]), amely egy bizonyos adatállomány-kategóriára vonatkozik, azaz olyan tartalmú és javasolt felhasználású adatállományokra, amelyek hasonló megfontolásokat vetnek fel például a beavatkozás mértéke és érzékenysége, valamint az adatok felhasználásának arányossága tekintetében, lehetővé téve ezért a miniszter számára az adott osztályon belüli összes adat egyszerre történő gyűjtése szükségességének és arányosságának megfontolását. Például egy csoportos tömeges személyesadat-állomány kiterjedhet a hasonló útvonalakra vonatkozó utazási adatállományokra ([420]). „Konkrét tömeges személyesadat-állományokra vonatkozó parancsok" ([421]) viszont egy meghatározott adatállományra vonatkoznak, például olyan új vagy szokatlan típusú adatállományra, amely nem tartozik a tömeges személyesadat-állományok meglévő csoportjába, vagy egy olyan adatállományra, amely a személyes adatok meghatározott típusaira vonatkozik ([422]) és ezért további biztosítékokat igényel ([423]). A nyomozati hatáskörökről szóló 2016. évi törvény tömeges személyesadat-állományokra vonatkozó rendelkezései csak akkor teszik lehetővé az említett adatállományok vizsgálatát és megőrzését, amennyiben ez szükséges és arányos ([424]), valamint megfelel a magánélet védelmével kapcsolatos általános kötelezettségeknek ([425]).

(240) A tömeges személyesadat-állományra vonatkozó parancs kiadásának hatásköre a „duplán ellenőrzött" eljárás alá tartozik: az intézkedés szükségességének és arányosságának értékelését először a miniszter, majd az igazságügyi biztos végzi ([426]). a miniszter köteles mérlegelni a kért parancs típusát és terjedelmét, az érintett adatok kategóriáját és azon egyedi tömeges személyes adatállományok számát, amelyek valószínűleg az adott típusú parancs alá tartoznak ([427]). Ezenkívül, amint azt a hírszerző ügynökségek tömeges személyesadat-állományai megőrzésének és használatának gyakorlati kódexe meghatározza, részletes nyilvántartásokat kell vezetni, és azokat a nyomozási biztos ellenőrizheti ([428]). A tömeges személyesadat-állományok nyomozati hatáskörökről szóló 2016. évi törvény szabta kereteken kívül történő megőrzése és vizsgálata bűncselekménynek minősül ([429]).

([414]) A nyomozási biztos hivatalának 2019. évi éves jelentése, 8.6. pont, lásd a 463. lábjegyzetet.
([415]) A nyomozási biztos hivatalának 2019. évi éves jelentése, 10.4. pont, lásd a 463. lábjegyzetet.
([416]) A nyomozási biztos hivatalának 2019. évi éves jelentése, 8.37. pont, lásd a 463. lábjegyzetet.
([417]) A nyomozati hatáskörökről szóló 2016. évi törvény 200. szakasza.
([418]) Az Egyesült Királyság magyarázata a megfelelőségi megbeszélésekre, H. szakasz: Nemzetbiztonság, 34. oldal, lásd a 29. lábjegyzetet.
([419]) A nyomozati hatáskörökről szóló 2016. évi törvény 204. szakasza.
([420]) A hírszerző ügynökségek tömeges személyesadat-állományai megőrzésének és használatának gyakorlati kódexe, 4.7. pont, elérhető a következő linken: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf
([421]) A nyomozati hatáskörökről szóló 2016. évi törvény 205. szakasza.
([422]) Ilyenek például a különleges személyes adatok, lásd a nyomozati hatáskörökről szóló 2016. évi törvény 202. szakaszát és A hírszerző ügynökség tömeges személyesadat-állományai megőrzésének és használatának gyakorlati kódexét, 4.21. és 4.12. pont, lásd a 469. lábjegyzetet.
([423]) A miniszternek külön, azaz egy adott adatkészlet tekintetében kell megvizsgálnia egy adott tömeges személyesadat-állományra vonatkozó parancs iránti kérelmet. A hírszerző ügynökségnek a nyomozati hatáskörökről szóló törvény 205. szakasza előírja, hogy egy adott tömeges személyesadat-állományra vonatkozó parancsra irányuló kérelmében adjon részletes magyarázatot a szóban forgó anyag jellegéről és terjedelméről, valamint sorolja fel azokat az „operatív célokat", amelyekre az érintett hírszerző ügynökség meg kívánja vizsgálni a tömeges személyesadat-állományt (amennyiben a hírszerző ügynökség megőrzés helyett inkább megőrzési és vizsgálati parancsot kér). A csoportos tömeges személyesadat-állományra vonatkozó parancs kiadásakor a miniszter ehelyett az adatállományok teljes kategóriáját egyszerre vizsgálja.
([424]) A nyomozati hatáskörökről szóló 2016. évi törvény 204. és 205. szakasza.
([425]) A nyomozati hatáskörökről szóló 2016. évi törvény 2. szakasza.
([426]) A nyomozati hatáskörökről szóló 2016. évi törvény 204. és 205. szakasza.
([427]) A hírszerző ügynökségek tömeges személyesadat-állományai megőrzésének és használatának gyakorlati kódexe, 5.2. pont, lásd a 420. lábjegyzetet.
([428]) A hírszerző ügynökségek tömeges személyesadat-állományai megőrzésének és használatának gyakorlati kódexe, 8.1–8.15. pont, lásd a 420. lábjegyzetet.
([429]) Az Egyesült Királyság magyarázata a megfelelőségi megbeszélésekre, H. szakasz: Nemzetbiztonság, 34. oldal, lásd a 29. lábjegyzetet.

3.3.2. *Az összegyűjtött információk további felhasználása*

(241) A 2018. évi adatvédelmi törvény 4. része szerint kezelt személyes adatokat tilos olyan módon kezelni, amely összeegyeztethetetlen azokkal a célokkal, amelyekre azokat gyűjtik ([430]). A 2018. évi adatvédelmi törvény előírja, hogy az adatkezelő az adatokat más attól eltérő célból is kezelheti, mint amelyre az adatokat gyűjtötték, amennyiben az összeegyeztethető az eredeti céllal, és feltéve, hogy az adatkezelőt törvény hatalmazza fel az adatok kezelésére, és az adatkezelés szükséges és arányos ([431]). Sőt, a biztonsági szolgálatokról szóló 1989. évi törvény és a hírszerző ügynökségekről szóló 1994. évi törvény meghatározza, hogy a hírszerző ügynökségek vezetőinek kötelességük biztosítani, hogy semmilyen információt ne gyűjtsenek vagy közöljenek, kivéve, ha az az ügynökségi feladatok megfelelő ellátásához vagy a vonatkozó rendelkezésekben felsorolt egyéb korlátozott és egyedi célokra szükséges ([432]).

(242) Ezenkívül a 2018. évi adatvédelmi törvény 109. szakasza konkrét követelményeket határoz meg a hírszerző ügynökségek által személyes adatok harmadik országoknak vagy nemzetközi szervezeteknek történő nemzetközi továbbítására vonatkozóan. E rendelkezés szerint a személyes adatok továbbítása nem engedélyezett az Egyesült Királyságon kívüli országba vagy területre vagy egy nemzetközi szervezethez, kivéve, ha az adattovábbítás az adatkezelő törvényi funkcióinak vagy más, a biztonsági szolgálatokról szóló 1989. évi törvény 2. szakasza (2) bekezdésének a) pontjában vagy a hírszerző ügynökségekről szóló 1994. évi törvény 2. szakasza (2) bekezdésének a) pontjában és 4. szakasza (2) bekezdésének a) pontjában előírt más céloknak megfelelően szükséges és arányos ([433]). Fontos, hogy ezek a követelmények azokban az esetekben is érvényesülnek, amikor a 2018. évi adatvédelmi törvény 110. szakasza szerinti nemzetbiztonsági kivételre hivatkoznak, mivel a 2018. évi adatvédelmi törvény 110. szakasza nem sorolja fel a 2018. évi adatvédelmi törvény 109. szakaszát azon rendelkezések között, amelyek alkalmazása mellőzhető, ha a nemzetbiztonság védelme érdekében bizonyos rendelkezések alóli kivételre van szükség.

(243) Sőt, amint azt az információügyi biztos hangsúlyozta a hírszerző szolgálatok általi adatkezelésre vonatkozó útmutatójában, a 2018. évi adatvédelmi törvény 4. részében biztosított biztosítékok mellett a hírszerző ügynökségre vonatkoznak az egyéb jogalkotási intézkedésekben előírt biztosítékok, amikor adatokat osztanak meg egy harmadik országbeli hírszerző szervvel, a személyes adatok jogszerű és felelősségteljes gyűjtése, megosztása és kezelése biztosításának érdekében ([434]). Például a nyomozati hatáskörökről szóló 2016. évi törvény további biztosítékokat határoz meg a célzott lehallgatás ([435]), a berendezés célzott zavarása ([436]), a tömeges lehallgatás ([437]), a kommunikációs adatok tömeges gyűjtése ([438]) és berendezések tömeges zavarása ([439]) útján gyűjtött anyagok harmadik országba történő továbbításával (úgynevezett „tengerentúli közlések") kapcsolatban. A parancsot kiadó hatóságnak különösen gondoskodnia kell arról, hogy érvényben legyenek azt biztosító intézkedések, hogy az adatokat fogadó harmadik ország a nyomozati hatáskörökről szóló 2016. évi törvényben meghatározott engedélyezett célokhoz szükséges lehető legalacsonyabbra korlátozza az anyagot megtekintők számát, a közlés terjedelmét és az anyagról készült másolatok számát ([440]).

3.3.3. *Felügyelet*

(244) A kormány nemzetbiztonsági célú hozzáférését számos különféle szerv felügyeli. Az információügyi biztosa személyes adatok kezelését a 2018. évi adatvédelmi törvényre figyelemmel felügyeli (a biztos függetlenségéről, kinevezési szerepéről és hatásköreiről bővebben lásd a (85)–(98) preambulumbekezdést), míg a nyomozati hatáskörök felhasználásának független és bírósági felügyeletét a nyomozati hatáskörökről szóló 2016. évi törvény

([430]) A 2018. évi adatvédelmi törvény 87. szakaszának (1) bekezdése.

([431]) A 2018. évi adatvédelmi törvény 87. szakaszának (3) bekezdése. Míg az adatkezelők a 2018. évi adatvédelmi törvény 110. szakasza alapján mentesülhetnek ez alól az elv alól, amennyiben ez a kivétel a nemzetbiztonság megőrzéséhez szükséges, az említett kivételt eseti alapon kell értékelni, és csak annyiban lehet arra hivatkozni, amennyiben egy adott rendelkezés alkalmazása hátrányos következményekkel járna a nemzetbiztonság szempontjából (lásd a (132) preambulumbekezdést). Az Egyesült Királyság hírszerző ügynökségei nemzetbiztonsági tanúsítványai (a következő linken érhetők el: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) nem terjednek ki a 2018. évi adatvédelmi törvény 87. szakaszának (3) bekezdésére. Ezenkívül, mivel minden más célú adatkezelést törvényben kell engedélyezni, a hírszerző ügynökségnek egyértelmű jogalapokkal kell rendelkezniük a további feldolgozáshoz.

([432]) E célokról részletesebben lásd a 312 lábjegyzetet.

([433]) Lásd a 312. lábjegyzetet.

([434]) ICO Intelligence Service, 2013-as tanulmány (lásd a 161. lábjegyzetet).

([435]) A nyomozati hatáskörökről szóló 2016. évi törvény 54. szakasza.

([436]) A nyomozati hatáskörökről szóló 2016. évi törvény 130. szakasza.

([437]) A nyomozati hatáskörökről szóló 2016. évi törvény 151. szakasza.

([438]) A nyomozati hatáskörökről szóló 2016. évi törvény 171. szakaszának (9) bekezdése.

([439]) A nyomozati hatáskörökről szóló 2016. évi törvény 192. szakasza.

([440]) A megállapodásoknak intézkedéseket kell tartalmazniuk annak biztosítására, hogy az anyag összes másolatát biztonságos módon tárolják az őrzés teljes ideje alatt. A parancs alapján megszerzett anyagot és az anyagból készült minden másolatot meg kell semmisíteni, amint annak megőrzésére már nincs releváns ok (lásd a nyomozati hatáskörökről szóló 2016. évi törvény 150. szakaszának (2) bekezdését, 150. szakaszának (5) bekezdését és 151. szakaszának (2) bekezdését). Érdemes megjegyezni, hogy a korábbi jogi keretben (a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény) biztosított hasonló biztosítékokat az Emberi Jogok Európai Bírósága a tömeges lehallgatással nyert anyag külföldi államokkal vagy nemzetközi szervezetekkel történő megosztására vonatkozó követelményeknek megfelelőnek találta (Európai Emberi Jogok Bírósága (nagytanács), Big Brother Watch és társai kontra Egyesült Királyság (lásd a fenti 279. lábjegyzetet), 362. és 399. pont.

szerint a nyomozási biztos biztosítja. A nyomozási biztos felügyeli a nyomozati hatáskörökről szóló 2016. évi törvény szerinti nyomozati hatáskörök bűnüldöző és a nemzetbiztonsági hatóságok általi felhasználását. A politikai felügyeletet a parlament hírszerző ügynökségekkel foglalkozó bizottsága garantálja.

3.3.3.1. Az adatvédelmi törvény 4. része szerinti felügyelet

(245) A személyes adatok hírszerző ügynökségek általi, a 2018. évi adatvédelmi törvény 4. része alapján végzett kezelését az információügyi biztos felügyeli ([441]).

(246) Az információügyi biztos általános feladatait a személyes adatok hírszerző ügynökségek általi, a 2018. évi adatvédelmi törvény 4. része szerinti kezelésével kapcsolatban a 2018. évi adatvédelmi törvény 13. melléklete állapítja meg. A feladatok a teljesség igénye nélkül magukban foglalják a 2018. évi adatvédelmi törvény 4. részének nyomon követését és végrehajtását, a közvélemény tudatosságának növelését, a Parlamentnek, a kormánynak és más intézményeknek történő tanácsadást a jogalkotási és közigazgatási intézkedések terén, az adatkezelők és adatfeldolgozók kötelezettségei tudatosításának előmozdítását, az érintettek tájékoztatását az érintett jogainak gyakorlásáról és vizsgálatok lefolytatását.

(247) A biztos – mint a 2018. évi adatvédelmi törvény 3. része esetében is – hatáskörrel rendelkezik arra, hogy értesítse az adatkezelőket az állítólagos jogsértésekről, és figyelmeztetéseket adjon ki, hogy egy adatkezelés valószínűleg a szabályokba ütközik, és a jogsértés megállapításakor megrovást ad. Kiadhat jogérvényesítési felhívást és bírságértesítőt is a törvény bizonyos rendelkezéseinek megsértése esetén ([442]). Ugyanakkor a 2018. évi adatvédelmi törvény más részeitől eltérően a biztos nem adhat ki vizsgálati felhívást nemzetbiztonsági szervnek ([443]).

(248) Ezenkívül a 2018. évi adatvédelmi törvény 110. szakasza kivételt tesz a biztos bizonyos hatásköreinek használata alól, amennyiben erre a nemzetbiztonság védelme érdekében van szükség. Idetartozik a biztos arra vonatkozó hatásköre, hogy az adatvédelmi törvény alapján (bármilyen típusú) felhívást adjon ki (adatkérési, vizsgálati, jogérvényesítési felhívás és bírságértesítők), a nemzetközi kötelezettségeknek megfelelő ellenőrzések elvégzésének hatásköre, a belépési és ellenőrzési jogkörök, valamint a bűncselekményekre vonatkozó szabályok ([444]). Amint azt a (126) preambulumbekezdés kifejti, ezek a kivételek csak szükség esetén és arányosan, eseti alapon érvényesülnek.

(249) A biztos és az Egyesült Királyság hírszerző ügynökségei egyetértési megállapodást írtak alá ([445]), amely létrehozza az együttműködés kereteit számos kérdésben, ideértve az adatvédelmi bejelentéseket és az érintettek panaszainak kezelését. Különösen előírja, hogy panasz kézhezvételekor a biztos értékeli, hogy a nemzetbiztonsági kivételek alkalmazása megfelelően történt-e. A biztos által az egyedi panaszok vizsgálata során feltett kérdésekre az érintett hírszerző ügynökségnek 20 munkanapon belül válaszolnia kell, megfelelő biztonságos csatornákon keresztül, amennyiben minősített adatokat tartalmaz. 2018 áprilisától a mai napig a biztos 21 panaszt kapott magánszemélyektől a hírszerző ügynökségekkel kapcsolatban. Minden panaszt értékeltek, és az eredményről tájékoztatták az érintettet ([446]).

([441]) A 2018. évi adatvédelmi törvény 116. szakasza.

([442]) A 2018. évi adatvédelmi törvény 13. mellékletének 2. pontja értelmében végrehajtási és bírságértesítőket az adatkezelőnek vagy az adatfeldolgozónak lehet kiadni a következők megsértése miatt: a 2018. évi adatvédelmi törvény 4. része 2. fejezete (az adatkezelés alapelvei), amely a 2018. évi adatvédelmi törvény 4. részének az érintetteknek jogot biztosító rendelkezése, a személyes adatok megsértésének a biztosnak történő bejelentésének követelménye a 2018. évi adatvédelmi törvény 108. szakasza alapján, valamint a személyes adatok harmadik országoknak, az egyezményen kívüli országoknak és a nemzetközi szervezeteknek történő továbbításának a 2018. évi adatvédelmi törvény 109. szakaszában foglalt elvei (a jogérvényesítési felhívásról és bírságértesítőről részletesebben lásd a fenti (92) preambulumbekezdést.

([443]) A 2018. évi adatvédelmi törvény 147. szakaszának (6) bekezdése szerint az információügyi biztos nem adhat ki vizsgálati felhívást a 2000. évi információszabadságról szóló törvény 23. szakaszának (3) bekezdésében meghatározott szervnek. Ezek közé tartozik a biztonsági szolgálat (MI5), a titkosszolgálat (MI6) és a Kormányzati Kommunikációs Központ.

([444]) A kivétel körébe vonható rendelkezések a következők: a 108. szakasz (személyes adatok megsértésének bejelentése a biztosnak), 119. szakasz (ellenőrzés a nemzetközi kötelezettségeknek megfelelően); a 142–154. szakasz és 15. melléklet (a biztos felhívásai, belépési és ellenőrzési jogkörök); és a 170–173. szakasz (személyes adatokkal kapcsolatos bűncselekmények). Emellett a hírszerző ügynökség által végzett adatkezelés mellett a 13. melléklet (a biztos egyéb általános feladatai) 1. pontjának a) és g) alpontjában, valamint a 2. pontjában szereplő adatkezeléssel kapcsolatban.

([445]) Az Információügyi Bizottság Irodája és az Egyesült Királyság Hírszerző Közössége közötti egyetértési megállapodás, lásd a 165. lábjegyzetet.

([446]) Ezen esetek közül hétben a biztos azt tanácsolta a panaszosnak, hogy aggályaival forduljon az adatkezelőhöz (ez az eset áll fenn, amikor egy magánszemély aggályait a biztosnál veti fel, de előbb az adatkezelőhöz kellett volna fordulnia), az egyik ilyen esetekben a biztos általános tanácsokkal látta el az adatkezelőt (ezt akkor veszik igénybe, ha az adatkezelő intézkedései nem tűnnek jogsértőnek, de a gyakorlatok javításával megelőzhető a biztosnál aggályok felvetése), és a másik 13 esetben az adatkezelőtől nem volt szükség semmilyen intézkedésre (ezt akkor veszik igénybe, ha az egyén által felvetett aggályok valóban a 2018. évi adatvédelmi törvény hatálya alá tartoznak, mert személyes adatok kezelésére vonatkoznak, de az adatkezelő az általa szolgáltatott információk alapján a jelek szerint nem sértette meg a jogszabályokat).

3.3.3.2. A nyomozati hatáskörök felhasználásának nyomozati hatáskörökről szóló 2016. évi törvény szerinti felügyelete

(250) A nyomozati hatáskörökről szóló 2016. évi törvény 8. része alapján a nyomozati hatáskörök felhasználásának felügyeletét a nyomozati hatáskörök biztosa (nyomozási biztos) gyakorolja. A nyomozási biztost más igazságügyi biztosok segítik, akiket gyűjtőnéven igazságügyi biztosnak neveznek ([447]). A nyomozati hatáskörökről szóló 2016. évi törvény meghatározza azokat a garanciákat, amelyek védik az igazságügyi biztosok függetlenségét. Az igazságügyi biztosok kötelesek hivatalban lévő vagy volt magas rangú bírák (azaz a legmagasabb szintű bíróságoknál kellett hivatalt betölteniük) ([448]) és az igazságszolgáltatás minden tagjához hasonlóan a kormánytól független jogállást élveznek ([449]). A nyomozati hatáskörökről szóló 2016. évi törvény 227. szakasza értelmében a miniszterelnök jelöli ki a nyomozási biztost és annyi igazságügyi biztost, amennyit szükségesnek tart. Valamennyi biztos, függetlenül attól, hogy a bírói kar jelenlegi vagy korábbi tagja, csak az Anglia és Wales, Skócia és Észak-Írország három főbírája (Chief Justice) és a Lord Chancellor együttes ajánlása alapján nevezhetők ki ([450]). A miniszternek biztosítania kell a nyomozási biztos számára személyzetet, elhelyezést, berendezéseket és egyéb létesítményeket és szolgáltatásokat ([451]). A biztosok megbízatása három évre szól, és újból kinevezhetők ([452]). A függetlenség további garanciájaként az igazságügyi biztosokat csak szigorú, magas mércét előíró feltételek mellett lehet felmenteni: a miniszterelnök által, a nyomozati hatáskörökről szóló 2016. évi törvény 228. szakaszának (5) bekezdésében tételesen felsorolt kivételes körülmények között (például csőd vagy szabadságvesztés esetén), vagy a Parlament mindkét háza által elfogadott felmentést jóváhagyó határozattal ([453]).

(251) A nyomozási biztost és az igazságügyi biztosokat a nyomozati hatáskörök biztosának irodája (nyomozási biztos hivatala) támogatja szerepkörében. A nyomozási biztos hivatalának munkatársai közé tartozik egy ellenőrcsoport, házon belüli jogi és műszaki szakértők, valamint egy technológiai tanácsadó testület szakértői tanácsadás céljából. Mint az egyes igazságügyi biztosok esetében, a nyomozási biztos hivatalának függetlensége is védelmet élvez. A nyomozási biztos hivatala a Belügyminisztériumtól „független testület", azaz a Belügyminisztériumtól kap támogatást, de feladatait függetlenül látja el ([454]).

(252) Az igazságügyi biztosok fő feladatait a nyomozati hatáskörökről szóló 2016. évi törvény 229. szakasza tartalmazza ([455]). Az igazságügyi biztosok különösen széles körű előzetes jóváhagyási hatáskörrel rendelkeznek, amely részét képezi az Egyesült Királyság jogi keretébe a nyomozati hatáskörökről szóló 2016. évi törvénnyel bevezetett biztosítékoknak. A célzott lehallgatásra, a berendezés zavarására, a tömeges személyesadat-állományokra, a kommunikációs adatok tömeges gyűjtésére, valamint a kommunikációs adatok megőrzésére vonatkozó figyelmeztetéseket az igazságügyi biztosoknak jóvá kell hagyniuk ([456]). A nyomozási biztosnak mindig előzetesen engedélyeznie kell a kommunikációs adatok bűnüldözési célú gyűjtését is ([457]). Ha egy biztos megtagadja parancs jóváhagyását, a miniszter fellebbezhet a nyomozati hatáskörök biztosához, akinek döntése végleges.

([447]) A nyomozati hatáskörökről szóló 2016. évi törvény 227. szakaszának (7) és (8) bekezdésével összhangban a nyomozati hatáskörök biztosa igazságügyi biztos, a nyomozati hatáskörök biztosa és a többi igazságügyi biztos gyűjtőnéven igazságügyi biztos. Jelenleg 15 igazságügyi biztos van.

([448]) A Constitutional Reform Act 2005 elnevezésű, a 2005. évi alkotmányos reformról szóló törvény 3. része 60. szakaszának (2) bekezdése szerint a „magas rangú bíró" a következő bíróságok bármelyikének bíráját jelenti: i. a Legfelsőbb Bíróság; ii. az angliai és walesi Court of Appeal; iii. az angliai és walesi High Court; iv. a Court of Session; v. az észak-írországi Court of Appeal; vi. az észak-írországi High Court; vagy a Lord of Appeal in Ordinary.

([449]) Az igazságszolgáltatás függetlensége hagyományon alapul, és az 1701. évi Act of Settlement elnevezésű (örökösödési) törvény óta széles körben elismert.

([450]) A nyomozati hatáskörökről szóló 2016. évi törvény 227. szakaszának (3) bekezdése. Az igazságügyi biztosokat a nyomozati hatáskörök biztosának is ajánlást kell tennie, a nyomozati hatáskörökről szóló 2016. évi törvény 227. szakasza (4) bekezdésének e) pontja.

([451]) A nyomozati hatáskörökről szóló 2016. évi törvény 238. szakasza.

([452]) A nyomozati hatáskörökről szóló 2016. évi törvény 227. szakaszának (2) bekezdése.

([453]) A felmentési eljárás megegyezik az Egyesült Királyság többi bírája esetében érvényesülő felmentési eljárással (lásd például a Senior Courts 1981 elnevezésű törvény 11. szakaszának (3) bekezdését és az alkotmányos reformról szóló 2005. évi törvény 33. szakaszát, amelyek szintén a Parlament mindkét házának jóváhagyását követő határozatot írnak elő). A mai napig egyetlen igazságügyi biztost sem mentettek fel hivatalából.

([454]) A független testület olyan szervezet vagy ügynökség, amely finanszírozást kap egy kormánytól, de képes függetlenül eljárni (a független testület meghatározását és további információkat lásd a Kabinetiroda köztestületek besorolására vonatkozó kézikönyvében, amely elérhető a következő linken: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf és az alsóház közigazgatási választott bizottságának 2014–2015-ös ülésszakáról szóló első jelentésben, amely a következő linken érhető el: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf).

([455]) A nyomozati hatáskörökről szóló 2016. évi törvény 229. szakasza szerint az igazságügyi biztosnak kiterjedt felügyeleti hatáskörei vannak a hírszerző ügynökségek által gyűjtött adatok megőrzése és közlése vonatkozásában.

([456]) A miniszter parancs kiadására vonatkozó határozatának jóváhagyásáról a döntés magukra az igazságügyi biztosokra tartozó kérdés. Ha egy biztos megtagadja parancs jóváhagyását, a miniszter fellebbezhet a nyomozati hatáskörök biztosához, akinek döntése végleges.

([457]) A nyomozási biztos engedélyét minden esetben kérik, amennyiben bűnüldözési célból gyűjtenek kommunikációs adatokat (a nyomozati hatáskörökről szóló 2016. évi törvény 60A. szakasza). Amennyiben a kommunikációs adatokat nemzetbiztonsági célból gyűjtik, az engedélyt a nyomozási biztos vagy helyette az illetékes hatóság kijelölt vezető tisztviselője adhatja meg (lásd a nyomozati hatáskörökről szóló 2016. évi törvény 61. és 61A. szakaszát és a fenti (203) preambulumbekezdést).

(253) Az ENSZ magánélethez való joggal foglalkozó különleges előadója határozottan üdvözölte az igazságügyi biztosok intézményének a nyomozati hatáskörökről szóló 2016. évi törvénnyel történt létrehozását, mivel „a megfigyelésre vonatkozó érzékeny vagy tolakodóbb kéréseket mind egy kabinetminiszternek, mind a nyomozati hatáskörök biztos irodájának engedélyeznie kell". Hangsúlyozta különösen, hogy „a bírósági felülvizsgálat ezen eleme [a nyomozási biztos szerepén keresztül] egy gyakorlott ellenőrökből és technológiai szakértőkből álló, erőforrásokkal jobban felszerelt csapat segítségével a nyomozati hatáskörökről szóló törvény által bevezetett egyik legjelentősebb új biztosíték", amely felváltotta a felügyeleti hatóságok korábbi széttagolt rendszerét, és kiegészíti a Parlament Hírszerzési és Biztonsági Bizottságának és az Investigatory Powers Tribunal szerepkörét" ([458]).

(254) Ezenkívül a nyomozási biztosnak van hatásköre a nyomozati hatáskörök felhasználása utólagos felügyeletének elvégzésére ([459]) a nyomozati hatáskörökről szóló 2016. évi törvény alapján, ideértve az ellenőrzés, vizsgálat és nyomozás útján végzett felügyeletet, valamint van a vonatkozó jogszabályokban meghatározott néhány más hatásköre és funkciója ([460]). Az említett utólagos felügyelet eredményét a jelentés tartalmazza, amelyet a nyomozási biztosnak évente el kell készítenie és be kell terjesztenie a miniszterelnöknek ([461]), és ezt közzé kell tenni és a Parlament elé is be kell terjeszteni ([462]). A jelentés tartalmazza a releváns statisztikákat és információkat a nyomozati hatáskörök hírszerző ügynökségek és bűnüldöző hatóságok általi felhasználásáról, valamint az ügyvédi titoktartási kötelezettség alá eső anyagokkal, a bizalmas újságírói anyagokkal és az újságírói információk forrásaival kapcsolatos biztosítékok alkalmazásáról, a tömeges parancsok kapcsán alkalmazott szabályokról és operatív célokról. Végül a nyomozási biztos hivatala éves jelentésben meg van határozva, hogy mely területekre vonatkozóan kaptak ajánlásokat a hatóságok, és miként kezelték azokat ([463]).

(255) A nyomozati hatáskörökről szóló 2016. évi törvény 231. szakaszával összhangban, ha a nyomozási biztos tudomást szerez a hatóságok által a nyomozati hatáskörük felhasználása során elkövetett bármely releváns hibáról, tájékoztatnia kell az érintett személyt, ha úgy ítéli meg, hogy a hiba súlyos, és a személy tájékoztatása közérdek ([464]). A nyomozati hatáskörökről szóló 2016. évi törvény 231. szakasza meghatározza különösen, hogy a személyek hibáról történő tájékoztatásakor a nyomozási biztosnak tájékoztatást kell adnia az Investigatory Powers Tribunalhoz való fordulás jogáról, és meg kell adnia azokat az adatokat, amelyeket a biztos szükségesnek tart e jogok gyakorlásához, és a közléshez közérdek fűződik ([465]).

([458]) A Nagy-Britannia és Észak-Írország Egyesült Királyságába irányuló missziójának küldetészáró nyilatkozata a magánélethez való joggal foglalkozó különleges előadó küldetésének befejezésekor (lásd a 281. lábjegyzetet).

([459]) A nyomozati hatáskörökről szóló 2016. évi törvény 229. szakasza. Az igazságügyi biztosok nyomozati és tájékoztatási feladatait a nyomozati hatáskörökről szóló 2016. évi törvény 235. szakasza tartalmazza.

([460]) Ez magában foglalja a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény szerinti felügyeleti intézkedéseket, a 1997. évi rendőrségi törvény 3. részében foglalt feladatok ellátását (a vagyoni jellegű cselekmények engedélyezését), valamint a miniszter hírszerző ügynökségekről szóló 1994. évi törvény 5–7. szakasza szerinti feladatainak ellátását (parancs a vezeték nélküli távírás zavarására, belépésre és vagyoni jellegű intézkedésre (a nyomozati hatáskörökről szóló 2016. évi törvény 229. szakasza).

([461]) A nyomozati hatáskörökről szóló 2016. évi törvény 230. szakasza. A nyomozási biztos saját kezdeményezésére beszámolhat a miniszterelnöknek a feladataival kapcsolatos bármely kérdésről. A nyomozási biztosnak kérésre a miniszterelnöknek is jelentést kell tennie, és a miniszterelnök utasíthatja a nyomozási biztost a hírszerző ügynökségek bármely funkciójának felülvizsgálatára.

([462]) Egyes részeket ki lehet zárni, ha azok közlése a nemzetbiztonságba ütközne.

([463]) Például a nyomozási biztos hivatalának 2019. évi éves jelentésében (6.38. pont) megemlítik, hogy az MI5-nek azt ajánlották, hogy módosítsa a tömeges személyesadat-állományok megőrzési szabályzatát, mivel olyan megközelítést kellett volna alkalmaznia, amely figyelembe veszi a megőrzés arányosságát a tömeges személyesadat-állományok összes mezőjére és minden egyes őrzött tömeges személyesadat-állományra. 2018 végén a nyomozási biztos hivatala nem volt elégedett azzal, ahogy ezt az ajánlást követték, és a 2019-es jelentés kifejtette, hogy az MI5 most új eljárást vezet be ennek a követelménynek a teljesítésére. A 2019-es éves jelentés (8.22. pont) megemlíti azt is, hogy a Kormányzati Kommunikációs Központ számos ajánlást kapott a tömeges adatokra vonatkozó lekérdezéseik arányosságának nyilvántartásával kapcsolatban. A jelentés megerősíti, hogy ezen a területen 2018 végén javítások történtek. A nyomozati hatáskörök biztosának 2019. évi éves jelentése, elérhető a következő linken: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf Továbbá, a hatóságál minden egyes, a nyomozási biztos hivatala által végzett ellenőrzést egy jelentés zár, amelyet a hatóságnak átadnak, és amely tartalmazza az ellenőrzés során felmerülő ajánlásokat. A nyomozási biztos hivatala ezután minden későbbi ellenőrzést a legutóbbi esetleges korábbi ajánlások felülvizsgálatával kezd, és az új ellenőrzési jelentésben feltünteti, hogy a korábbi ajánlásokkal foglalkoztak-e, vagy azokat tovább kell-e vinni.

([464]) A hiba akkor tekinthető „súlyosnak", ha a biztos úgy ítéli meg, hogy az jelentős sérelmet vagy kárt okozott az érintett személynek (a nyomozati hatáskörökről szóló 2016. évi törvény 231. szakaszának (2) bekezdése). 2018-ban 22 hibáról számoltak be, amelyek közül nyolcat súlyosnak ítéltek meg, és tájékoztatást adtak az érintett személy számára. Lásd a nyomozati hatáskörök biztosának 2018. évi éves jelentése C. mellékletét (lásd: https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). 2019-ben 14 hibát tekintettek súlyosnak. Lásd a nyomozati hatáskörök biztosának 2019. évi éves jelentését, C. melléklet, lásd a 463. lábjegyzetet.

([465]) A nyomozati hatáskörökről szóló 2016. évi törvény 231. szakasza előírja, hogy amikor egy személyt hibáról tájékoztatnak, a nyomozási biztosnak olyan részletadatokat kell megadnia, amelyeket a biztos szükségesnek tart e jogok gyakorlása érdekében, különös tekintettel arra, hogy a részletek közlése mennyiben ellentétes a közérdekkel, vagy sérti a súlyos bűncselekmények megelőzését vagy felderítését, az Egyesült Királyság gazdasági jólétét vagy a hírszerző ügynökségek bármelyike feladatainak folyamatos ellátását.

3.3.3.3. A hírszerző ügynökségek parlamenti felügyelete

(256) A Hírszerzési és Biztonsági Bizottság (ISC) által végzett parlamenti felügyelet jogszabályi alapja a Justice and Security Act 2013 elnevezésű, 2013. évi igazságügyi és biztonsági törvényben szerepel ([466]). A törvény az ISC-t az Egyesült Királyság Parlamentjének bizottságaként hozza létre. 2013 óta az ISC nagyobb hatásköröket kapott, ideértve a biztonsági szolgálatok operatív tevékenységeinek felügyeletét is. A 2013. évi igazságügyi és biztonsági törvény 2. szakasza értelmében az ISC feladata a nemzetbiztonsági ügynökségek kiadásainak, adminisztrációjának, politikájának és működésének felügyelete. A 2013. évi igazságügyi és biztonsági törvény meghatározza, hogy az ISC operatív kérdésekben vizsgálatokat folytathat le, ha azok nem folyamatban lévő műveletekhez kapcsolódnak ([467]). A miniszterelnök és az ISC között megkötött egyetértési megállapodás ([468]) részletesen meghatározza azokat az elemeket, amelyeket figyelembe kell venni annak mérlegelésekor, hogy egy tevékenység nem része-e valamely folyamatban lévő műveletnek ([469]). Az ISC-t felkérheti a miniszterelnök is a folyamatban lévő műveletek kivizsgálására, és felülvizsgálhatja az ügynökségek által önkéntesen szolgáltatott információkat.

(257) A 2013. évi igazságügyi és biztonsági törvény 1. melléklete értelmében az ISC felkérheti a három hírszerző ügynökség bármelyikének vezetőjét adatok kiadására. Az ügynökségnek hozzáférhetővé kell tennie ezeket az adatokat, kivéve, ha a miniszter megvétózza ezt ([470]). Az Egyesült Királyság hatóságainak magyarázata szerint a gyakorlatban nagyon kevés információt tartanak vissza az ISC-től ([471]).

(258) Az ISC tagjai a Parlament bármely házának képviselői, akiket a miniszterelnök nevez ki az ellenzék vezetőjével folytatott konzultációt követően ([472]). Az ISC-nek éves jelentést kell készítenie a Parlamentnek feladatai ellátásáról, valamint egyéb, általa megfelelőnek tartott jelentéseket ([473]). Ezenkívül az ISC jogosult háromhavonta azon operatív célok listájának kézhezvételére, amelyeket az tömegesen gyűjtött anyagok vizsgálatához használnak ([474]). A miniszterelnök megküldi az ISC-vel a nyomozati hatáskör biztosa vizsgálatai, ellenőrzései vagy auditjai jelentéseinek másolatát, ha a jelentések tárgya releváns a bizottság törvényi hatásköre szempontjából ([475]). Végül a bizottság felkérheti a nyomozási biztost vizsgálat végzésére, és a biztosnak tájékoztatnia kell az ISC-t arról a döntésről, hogy az említett vizsgálatot elvégzi-e ([476]).

(259) Az ISC hozzájárult a nyomozati hatáskörökről szóló 2016. évi törvény tervezetéhez is, amely számos olyan módosítást eredményezett, amelyeket most a nyomozati hatáskörökről szóló 2016. évi törvény tükröz ([477]). Az ISC különösen az adatvédelem garanciáinak erősítését javasolta egy olyan adatvédelmi biztosíték bevezetésével, amely a

([466]) Amint azt az Egyesült Királyság hatóságai kifejtették, az igazságügyi és biztonsági törvény kibővítette az ISC hatáskörét, és szerepet kapott a három ügynökségen túl a hírszerzési közösség felügyeletében, és lehetővé tette az ügynökségek operatív tevékenységeinek visszamenőleges felügyeletét jelentős nemzeti érdekű kérdésekben.

([467]) Lásd a 2013. évi igazságügyi és biztonsági törvény 2. szakaszát.

([468]) A miniszterelnök és az ISC közötti egyetértési megállapodás, amely a következő linken érhető el: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf

([469]) A miniszterelnök és az ISC közötti egyetértési megállapodás, 14. pont, lásd a 468. lábjegyzetet.

([470]) A miniszter csak két okból vétózhatja meg az információk közlését: az információ különleges adat és nemzetbiztonsági érdekből nem szabad az ISC elé tárni; vagy olyan jellegű információról van szó, hogy ha a minisztert arra kérnék fel, hogy mutassa be azt az alsóház egyik minisztériumi választott bizottsága előtt, a miniszter úgy ítélné meg (nem kizárólag a nemzetbiztonsági okokból), hogy ez nem lenne helyénvaló (a 2013. évi igazságügyi és biztonsági törvény 1. melléklete 4. pontjának (2) bekezdése).

([471]) Az Egyesült Királyság magyarázata a megfelelőségi megbeszélésekre, H. szakasz: Nemzetbiztonság, 43. oldal, lásd a 31. lábjegyzetet.

([472]) Lásd a 2013. évi igazságügyi és biztonsági törvény 1. szakaszát. A miniszterek nem lehetnek tagok. A tagok az ISC-n belül azon parlamenti ciklus alatt töltik be tisztségüket, amely alatt kinevezték őket. Elmozdíthatók azon ház határozatával, amely kinevezte őket, vagy ha megszűnik képviselői tisztségük, vagy miniszterré válnak. A tag le is mondhat.

([473]) A bizottság jelentései és nyilatkozatai online elérhetők az alábbi linken: https://isc.independent.gov.uk/publications/ Az ISC 2015-ben jelentést adott ki „Adatvédelem és biztonság: Korszerű és átlátható jogi keret" címmel (lásd: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), amelyben megvizsgálta a hírszerző ügynökségek által alkalmazott megfigyelési technikák jogi kereteit, és egy sor ajánlást adott ki, amelyeket ezután figyelembe vettek és beépítettek a nyomozati hatáskörökről szóló, törvénnyé átalakult törvényjavaslatba, a nyomozati hatáskörökről szóló 2016. évi törvénybe. A kormány adatvédelmi és biztonsági jelentésre adott válasza az következő linken érhető el: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf

([474]) A nyomozati hatáskörökről szóló 2016. évi törvény 142., 161. és 183. szakasza.

([475]) A nyomozati hatáskörökről szóló 2016. évi törvény 234. szakasza.

([476]) A nyomozati hatáskörökről szóló 2016. évi törvény 236. szakasza.

([477]) A Parlament Hírszerzési és Biztonsági Bizottsága, Jelentés a nyomozati hatáskörökről szóló törvényjavaslat tervezetéről, elérhető a következő linken: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

nyomozati hatáskörök teljes skáláján érvényesül ([478]). Javasolta továbbá a berendezések zavarásával, a tömeges személyesadat-állományokkal és a kommunikációs adatokkal kapcsolatban javasolt hatáskörök módosítását, és további konkrét módosításokat kért a nyomozati hatáskörök használatára vonatkozó korlátozások és biztosítékok megerősítésére ([479]).

3.3.4. *Jogorvoslat*

(260) A nemzetbiztonsági célú kormányzati hozzáférés területén az érintetteknek rendelkezniük kell azzal a lehetőséggel, hogy független és pártatlan bíróság előtt éljenek jogorvoslati lehetőségekkel abból a célból, hogy a rájuk vonatkozó személyes adatokhoz hozzáférést kapjanak, vagy az ilyen adatokat helyesbíttetni vagy töröltetni tudják ([480]). Az említett bírósági testületnek különösen hatáskörrel kell rendelkeznie arra, hogy a hírszerző ügynökségre kötelező érvényű határozatokat hozzon ([481]). Az Egyesült Királyságban, amint azt a (261)–(271) preambulumbekezdés kifejtette, számos bírósági jogorvoslati út nyújt lehetőséget nyújt az érintetteknek az ilyen jogorvoslatok kérésére és elnyerésére.

3.3.4.1. Az adatvédelmi törvény 4. része alapján rendelkezésre álló jogorvoslati mechanizmusok

(261) A 2018. évi adatvédelmi törvény 165. szakasza értelmében az érintettnek joga van panaszt benyújtani az információügyi biztoshoz, ha az érintett úgy ítéli meg, hogy a rá vonatkozó személyes adatokkal kapcsolatban megsértették az adatvédelmi törvény 4. részét. 2018. Az információügyi biztos hatáskörébe tartozik annak értékelése, hogy az adatkezelő és az adatfeldolgozó megfelel-e a 2018. évi adatvédelmi törvénynek, és tőlük a szükséges lépések megtételének megkövetelése. Ezenkívül a 2018. évi adatvédelmi törvény 4. része értelmében az egyének jogosultak a High Courttól (vagy Skóciában a Court of Sessiontól) kérni az adatkezelő kötelezését az adatokhoz való hozzáféréshez ([482]), az adatkezelés elleni tiltakozáshoz ([483]), a helyesbítéshez vagy a törléshez ([484]) való jog tiszteletben tartására.

(262) A magánszemélyek jogosultak az adatkezelőtől vagy az adatfeldolgozótól kérni a 2018. évi adatvédelmi törvény 4. részében foglalt követelmények megsértése miatt elszenvedett károk megtérítését is ([485]). A kártérítés kiterjed mind az anyagi veszteségre, mind a nem vagyoni kárra, például a sérelemre ([486]).

3.3.4.2. A nyomozati hatáskörökről szóló 2016. évi törvény keretében rendelkezésre álló jogorvoslati mechanizmusok

(263) Az egyének az Investigatory Powers Tribunal előtt nyerhetnek jogorvoslatot a nyomozati hatáskörökről szóló 2016. évi törvény megsértése miatt.

(264) Az Investigatory Powers Tribunalt a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény hozta létre, és független a végrehajtó hatalomtól ([487]). A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 65. szakaszának megfelelően a Törvényszék tagjait a királynő nevezi ki ötéves időtartamra. A Törvényszék tagját a királynő mentheti fel a Parlament mindkét házához ([488]) intézett indítvánnyal ([489]).

([478]) Ezeket a magánélet védelméhez kapcsolódó általános feladatokat most a nyomozati hatáskörökről szóló 2016. évi törvény 2. szakaszának (2) bekezdése határozza meg, amely előírja, hogy a nyomozati hatáskörökről szóló 2016. évi törvény alapján eljáró hatóságnak figyelembe kell vennie, hogy amit a parancs, engedély vagy felhívás révén el akarnak érni, észszerűen más, kevésbé beavatkozó jellegű eszközökkel is el lehetne-e érni, és hogy az információ gyűjtésével kapcsolatban a parancs, engedély vagy felhívás alapján alkalmazandó védelem szintje magasabb-e ezen információk kiemelten különleges jellege okán, továbbá a távközlési rendszerek és a postai szolgáltatások integritásához és biztonságához fűződő közérdeket, és. a magánélet védelméhez fűződő közérdek egyéb vonatkozásait.

([479]) Például az ISC kérésére öt napról három munkanapra csökkent azon napok száma, ameddig egy „sürgős” parancs érvénybe léphet, mielőtt azt az igazságügyi biztosnak jóvá kellene hagynia, és az ISC felhatalmazást kapott arra, hogy kérdéseket a nyomozati hatáskörök biztosához utaljon vizsgálat céljából.

([480]) Schrems II. ügy, 194. pont.

([481]) Schrems II. ügy, 197. pont.

([482]) A 2018. évi adatvédelmi törvény 94. szakaszának (11) bekezdése.

([483]) A 2018. évi adatvédelmi törvény 99. szakaszának (4) bekezdése.

([484]) A 2018. évi adatvédelmi törvény 100. szakaszának (1) bekezdése.

([485]) A 2018. évi adatvédelmi törvény 169. szakasza lehetővé teszi „azon személy igényét, aki az adatvédelmi jogszabályok követelményeinek megsértése miatt kárt szenved”. Az Egyesült Királyság hatóságai által szolgáltatott információk szerint a gyakorlatban valószínűleg a követelést vagy panaszt fognak benyújtani a hírszerző ügynökséggel szemben az Investigatory Powers Tribunalhoz, amely széles illetékességgel rendelkezik, kártalanítást/kártérítést ítélhet meg, és amelynél az igényérvényesítés költségmentes.

([486]) A 2018. évi adatvédelmi törvény 169. szakaszának (5) bekezdése.

([487]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 3. melléklete értelmében a tagoknak meghatározott igazságügyi tapasztalattal kell rendelkezniük, és újból kinevezhetők.

([488]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 3. melléklete 1. pontjának (5) bekezdése.

([489]) A „beszéd” a Parlament elé terjesztett indítvány, amelynek célja, hogy az uralkodót megismertesse a Parlament véleményével egy adott kérdésben.

(265) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 65. szakasza szerint a Törvényszék a megfelelő bírósági testület a nyomozati hatáskörökről szóló 2016. évi törvény, a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény szerinti vagy a hírszerző ügynökség által elkövetett bármely magatartás miatt sérelmet szenvedett személy panaszának benyújtására ([490]).

(266) Az Investigatory Powers Tribunalhoz kereset benyújtása előtt („perelhetőségi követelmény") a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 65. szakasza szerint az egyénnek meg kell győződnie arról ([491]), hogy i. a hírszerző ügynökség eljárása vele, vagyonával, bármely általa küldött vagy neki szánt kommunikációval, vagy bármilyen postai szolgáltatás, telekommunikációs szolgáltatás vagy távközlési rendszer igénybevételével kapcsolatos ([492]). Ezenkívül a panaszos meggyőződése szerint a magatartásnak „vitatható körülmények között" kellett történnie ([493]) vagy „azt a hírszerző ügynökség vagy annak képviseletében másnak kell végrehajtania ([494]). Mivel ezt a „meggyőződés" mércét elég tágan értelmezték ([495]), az ügynek a Törvényszék elé terjeszthetőségére alacsony követelmények vonatkoznak.

(267) Amennyiben az Investigatory Powers Tribunal mérlegeli a hozzá benyújtott panaszt, a Törvényszék feladata annak vizsgálata, hogy a panaszban vádolt személyek részt vettek-e a panaszossal kapcsolatos tevékenységben, valamint vizsgálni kell azt a hatóságot, amely állítólag részt vett a jogsértésekben, és hogy az állítólagos magatartás megtörtént-e ([496]). Ha a Törvényszék tárgyal egy ügyet, az eljárásban ugyanazon elveket kell alkalmaznia a határozat hozatalához, amelyeket a bíróság a bírósági felülvizsgálat iránti kérelemre alkalmazna ([497]). Ezenkívül a nyomozati hatáskörökről szóló 2016. évi törvény alapján a parancsok vagy felhívások címzettjei, valamint minden más, állami hivatalban lévő, a rendőrség vagy a rendőrségi nyomozati és felülvizsgálati biztos alkalmazásában álló személy köteles minden olyan dokumentumot és információt feltárni vagy átadni a Törvényszéknek, amelyet a Törvényszék a hatásköre gyakorlásának lehetővé tétele érdekében bekérhet ([498]).

(268) A Törvényszéknek értesítenie kell a panaszost arról, hogy a javára döntött-e vagy sem ([499]). A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 67. szakaszának (6) és (7) bekezdése szerint a Törvényszéknek jogában áll ideiglenes intézkedést hozni, és az általa megfelelőnek tartott kártérítést megítélni vagy egyéb végzést meghozni. Ez lehet a parancs vagy felhatalmazás hatályon kívül helyezését vagy visszavonását elrendelő végzés, valamint a parancs, felhatalmazás vagy felhívás által átruházott bármely hatáskör gyakorlásával megszerzett vagy a hatóságok

([490]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 65. szakaszának (5) bekezdése.

([491]) A „meggyőződés" teszt mércéjéről lásd a Human Rights Watch kontra Secretary of State ügy (2016 UKIPTrib15_165-CH), 41. pontját. Ebben az ügyben a Investigatory Powers Tribunal az Emberi Jogok Európai Bíróságának ítélkezési gyakorlatára hivatkozva úgy ítélte meg, hogy a megfelelő teszt arra, hogy megalapozott-e az a meggyőződés, hogy a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 68. szakaszának (5) bekezdése alá tartozó magatartást a hírszerző ügynökségek bármelyike vagy annak megbízásából más követte el, hogy csak akkor van alapja annak a meggyőződésnek, amely szerint az egyén leplezett intézkedések vagy leplezett intézkedéseket megengedő jogszabályok puszta létével okozott jogsértés áldozatának vallhatja magát, ha képes bizonyítani, hogy személyes helyzete miatt potenciálisan fennáll annak a veszélye, hogy ilyen intézkedéseknek vetik alá.

([492]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 65. szakaszának (4) bekezdése.

([493]) Ezek a körülmények a hatóságok felhatalmazással történt magatartására utalnak (pl. egy parancs, a kommunikáció megszerzésére vonatkozó felhatalmazás/felhívás stb.), vagy ha a körülmények olyanok, hogy (függetlenül attól, hogy van-e ilyen hatóság) a magatartás nem lett volna helyénvaló felhatalmazás, vagy legalábbis annak megfelelő mérlegelése nélkül, hogy ilyen felhatalmazást kell-e kérni. Az igazságügyi biztos által engedélyezett magatartás vitatható körülmények között megvalósult minősül (a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 65. szakasz (7ZA) szakasz), míg a bírói tisztséget betöltő személy engedélyével folytatott egyéb magatartás nem vitatható körülmény (a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 65. szakaszának (7) és (8) bekezdése).

([494]) Az Egyesült Királyság hatóságai által szolgáltatott információk szerint a panasz benyújtásához szükséges alacsony küszöb következtében nem szokatlan, hogy a Törvényszék vizsgálata azt állapítja meg, hogy a panaszost valójában soha nem vizsgálta a hatóság. Az Investigatory Powers Tribunal legfrissebb statisztikai jelentésében szerepel, hogy 2016-ban a Törvényszékhez 209 panasz érkezett, ezek 52 %-át komolytalannak vagy zaklatónak, 25 %-át pedig „határozatlan"-nak ítélték. Az Egyesült Királyság hatóságai kifejtették, hogy ez vagy azt jelenti, hogy nem használtak leplezett tevékenységet/hatásköröket a panaszossal kapcsolatban, vagy hogy alkalmaztak leplezett technikákat, és a Törvényszék megállapította a tevékenység jogszerűségét. Ezenkívül 11 % esetében nem volt hatáskör, azokat visszavonták vagy érvénytelenek voltak, 5 %-ukat elutasították elévülés miatt, 7 %-ukban a panaszos javára döntöttek. Az Investigatory Powers Tribunal 2016. évi statisztikai jelentése, amely az alábbi linken érhető el: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([495]) Lásd a Human Rights Watch kontra Secretary of State ügyet (2016 UKIPTrib15_165-CH). Ebben az ügyben a nyomozati hatáskörrel foglalkozó bíróság az EJEB ítélkezési gyakorlatára hivatkozva úgy ítélte meg, hogy a megfelelő teszt az arról való meggyőződéséhez, hogy a nyomozati hatáskörök (Skócia) szabályozásáról szóló 2000. évi törvény 68. szakasza (5) bekezdésének hatálya alá tartozó magatartást bármelyik hírszerző ügynökség vagy képviseletében más elkövette-e, az, hogy van-e alapja az említett meggyőződésnek, beleértve azt a tényt is, hogy az egyén akkor vallhatja magát leplezett intézkedések vagy a leplezett intézkedéseket megengedő jogszabályok puszta léte által okozott jogsértés áldozatának, ha képes azt bizonyítani, hogy személyes helyzete miatt potenciálisan fennáll annak a veszélye, hogy ilyen intézkedéseknek vetik alá (lásd a Human Rights Watch kontra Secretary of State ügy 41. pontját).

([496]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 67. szakaszának (3) bekezdése.

([497]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 67. szakaszának (2) bekezdése.

([498]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 68. szakaszának (6) és (7) bekezdése.

([499]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 68. szakaszának (4) bekezdése.

által bármely más módon birtokolt, bármely személlyel kapcsolatos információk nyilvántartásának megsemmisítésére kötelező végzést ([500]). A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 67A. szakasza szerint a Törvényszék határozata ellen fellebbezni lehet, a Törvényszék vagy az illetékes fellebbviteli bíróság engedélyével.

(269) Végül érdemes megjegyezni, hogy az Investigatory Powers Tribunal szerepét az Emberi Jogok Európai Bírósága előtti jogi eljárások során több alkalommal megvitatták, nevezetesen a Kennedy kontra Egyesült Királyság ügyben ([501]) és újabban a Big Brother Watch és társai kontra Egyesült Királyság ügyben ([502]), amelyben a Bíróság kimondta, hogy „a nyomozati hatáskörrel foglalkozó bíróság erőteljes jogorvoslatot kínált mindenkinek, aki arra gyanakszik, hogy kommunikációját a hírszerző ügynökségek lehallgatták" ([503]).

3.3.4.3. Rendelkezésre álló egyéb jogorvoslati mechanizmusok

(270) Amint az a (109)–(111) preambulumbekezdésben kifejtésre került, az 1998. évi emberi jogi törvény szerinti és az Emberi Jogok Európai Bírósága előtti jogorvoslati lehetőségek ([504]) a nemzetbiztonság területén is elérhetők. A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 65. szakaszának (2) bekezdése kizárólagos illetékességet biztosít az Investigatory Powers Tribunal számára az Emberi Jogi Törvény alapján minden, a hírszerző ügynökségekkel szemben támasztott igény tekintetében ([505]). Ez azt jelenti, ahogyan azt a Legfelsőbb Bíróság megjegyezte: „az, hogy egy adott ügy tényállása az emberi jogi törvénybe ütközik-e, azt elvileg egy olyan független bíróság vetheti fel és döntheti el, amely hozzáférhet az összes vonatkozó anyaghoz, a titkos anyagokat is beleértve. […] Ebben az összefüggésben azt is szem előtt tartjuk, hogy a Törvényszék döntései ellen ma már lehetőség van fellebbezni a megfelelő fellebbviteli bíróságnál (Angliában és Walesben ez a Court of Appeal); és hogy a Legfelsőbb Bíróság nemrégiben úgy döntött, hogy a Törvényszék döntései ellen elvileg bírósági felülvizsgálatnak van helye: lásd: az R (Privacy International) kontra Investigatory Powers Tribunal ügyet (2019, UKSC 22; 2019, 2 WLR 1219)" ([506]).

(271) A fentiekből következik, hogy amikor az Egyesült Királyság bűnüldözési vagy nemzetbiztonsági hatóságai hozzáférnek az e határozat hatálya alá tartozó személyes adatokhoz, az említett hozzáférést olyan törvények szabályozzák, amelyek meghatározzák a hozzáférés feltételeit, és biztosítják, hogy az adatokhoz való hozzáférés és a további felhasználás csak az elérni kívánt bűnüldözési vagy nemzetbiztonsági célkitűzésekhez szükséges és azokkal arányos adatokra korlátozódnak. Ezenkívül az említett hozzáféréshez a legtöbb esetben bírósági szerv előzetes engedélye szükséges, a parancs vagy a közlésre kötelezés jóváhagyása révén, és minden esetben független felügyelet alatt áll. Amint a hatóságok hozzáférnek az adatokhoz, azok feldolgozására – beleértve a további megosztást és a továbbítást is – a 2018. évi adatvédelmi törvény 3. része alapján külön adatvédelmi biztosítékok vonatkoznak, amelyek a bűnüldöző hatóságok általi adatkezelés tekintetében tükrözik az (EU) 2016/680 irányelv, és a hírszerző ügynökségek általi adatkezelés tekintetében a 2018. évi adatvédelmi törvény 4. része szerinti biztosítékokat. Végül az érintettek ezen a területen hatékony közigazgatási és bírósági jogorvoslati jogokkal rendelkeznek, ideértve az adatokhoz való hozzáférést, illetve az említett adatok helyesbítését vagy törlését.

(272) Tekintettel az említett feltételek, korlátozások és biztosítékok e határozat alkalmazásában fennálló jelentőségére, a Bizottság szorosan figyelemmel fogja kísérni az adatokhoz való kormányzati hozzáférést meghatározó, egyesült királyságbeli szabályok alkalmazását és értelmezését. Ez ki fog terjedni a vonatkozó jogalkotási, szabályozási és ítélkezési gyakorlat fejleményeire, valamint az információügyi biztos és más felügyeleti hatóságokezen a területen

([500]) E hatáskörök alkalmazására példa a Liberty és társai kontra the Security Service, SIS, GCHQ ügy (2015 UKIP Trib 13_77-H_2). A Törvényszék a két panaszos javára döntött, mert az egyik esetben a kommunikációjukat a megállapított határidőn túl őrizték, a másikban pedig azért, mert a vizsgálati eljárást nem a Kormányzati Kommunikációs Központ belső szabályai szerint folytatták le. Az első esetben a Bíróság elrendelte a hírszerző ügynökségnek, hogy semmisítsék meg azokat a kommunikációkat, amelyeket a vonatkozó határidőn túl őrzött. A második esetben nem adtak ki megsemmisítési parancsot, mert a kommunikációt nem őrizték meg.

([501]) Kennedy-ügy, lásd a 129. lábjegyzetet.

([502]) Emberi Jogok Európai Bírósága, Big Brother Watch és társai kontra Egyesült Királyság ügy (lásd a fenti 268. lábjegyzetet), 413–415. pont.

([503]) Emberi Jogok Európai Bírósága, Big Brother Watch ügy, 425. pont.

([504]) Ezt szemlélteti például az Emberi Jogok Európai Bíróságának nagytanácsa nemrégiben, a Big Brother Watch és társai kontra Egyesült Királyság ügyben hozott ítélete (lásd a fenti 279. lábjegyzetet), ez lehetővé teszi annak nemzetközi bíróság általi hatékony bírósági ellenőrzését, hogy a hatóságok betartják-e az alapvető jogokat a személyes adatokhoz való hozzáférés során – hasonlóan ahhoz, mint ami az EU tagállamokra vonatkozik. Ezenkívül az Emberi Jogok Európai Bíróságának ítéleteinek végrehajtása felett az Európa Tanács külön felügyeletet gyakorol.

([505]) A Belhaj és társai ügyben (2017 UKSC 3) az ügyvédi titoktartási kötelezettség alá tartozó anyagok lehallgatása jogellenességének megállapítása közvetlenül az EJEE 8. cikkén alapult (lásd a 11. határozatot).

([506]) High Court of Justice, Liberty-ügy (2019 EWHC 2057 (Admin)), 170. pont.

végzett tevékenységére. Kiemelt figyelmet fog fordítani az Emberi Jogok Európai Bírósága vonatkozó ítéleteinek az Egyesült Királyság általi végrehajtására is, ideértve a Miniszteri Bizottsághoz benyújtott „cselekvési tervekben" és „cselekvési jelentésekben" a Bíróság ítéleteinek betartásával összefüggésben meghatározott intézkedéseket.

(4) **KÖVETKEZTETÉS**

(273) A Bizottság úgy véli, hogy az Egyesült Királyság általános adatvédelmi rendelete és a 2018. évi adatvédelmi törvény biztosítja az Európai Unióból továbbított személyes adatok olyan szintű védelmét, amely lényegében megegyezik az (EU) 2016/679 rendelet által garantált védelem szintjével.

(274) A Bizottság ezenfelül úgy ítéli meg, hogy az Egyesült Királyság jogában létező felügyeleti mechanizmusok és jogorvoslati megoldások összességében véve lehetővé teszik, hogy a gyakorlatban azonosítsák és szankcionálják, ha a személyes adatokat kezelő bűnüldözési hatóságok jogsértést követnek el, továbbá jogorvoslatot biztosítanak az érintetteknek, hogy betekinthessenek a rájuk vonatkozó személyes adatokba, és adott esetben helyesbíttethessék vagy töröltethessék ezeket az adatokat.

(275) Végül az Egyesült Királyság jogrendjéről rendelkezésre álló információk alapján a Bizottság úgy véli, hogy azon személyek alapvető jogaiba való beavatkozás, akiknek személyes adatait az Egyesült Királyság hatóságai közérdekből továbbítják az Európai Unióból az Egyesült Királyságba, például bűnüldözési és nemzetbiztonsági célokra, arra korlátozódik, ami a szóban forgó jogszerű cél eléréséhez feltétlenül szükséges, és hogy hatékony jogvédelem áll rendelkezésre ilyen beavatkozás esetén.

(276) Ezért e határozat megállapításaira figyelemmel olyan határozatot kell hozni, hogy az Egyesült Királyság megfelelő szintű védelmet biztosít az (EU) 2016/679 rendelet az Európai Unió Alapjogi Chartájára figyelemmel értelmezett 45. cikkének értelmében.

(277) Ez a következtetés az Egyesült Királyság vonatkozó belföldi rendszerén és nemzetközi kötelezettségvállalásain alapul, különös tekintettel az Emberi Jogok Európai Egyezményének betartására és az Emberi Jogok Európai Bírósága joghatóságának való alávetésre. Az említett nemzetközi kötelezettségek folyamatos betartása ezért különösen fontos eleme az e határozat alapját képező értékelésnek.

(5) **E HATÁROZAT ÉS AZ ADATVÉDELMI HATÓSÁGOK INTÉZKEDÉSÉNEK JOGHATÁSAI**

(278) A tagállamok és szerveik kötelesek megtenni az ahhoz szükséges intézkedéseket, hogy betartsák az uniós intézmények jogi aktusait, mivel az utóbbiak vélelmezhetően jogszerűek, és ennélfogva mindaddig joghatásokat váltanak ki, amíg azokat vissza nem vonják, megsemmisítés iránti kereset alapján meg nem semmisítik, illetve előzetes döntéshozatal iránti kérelem vagy jogellenességi kifogás következtében nem nyilvánítják érvénytelennek.

(279) Következésképpen a Bizottságnak az (EU) 2016/679 rendelet 45. cikkének (3) bekezdése alapján elfogadott megfelelőségi határozata kötelező a címzett tagállamok valamennyi szervére, így a független felügyeleti hatóságokra nézve is. E határozat alkalmazásának időtartama alatt különösen az európai uniós adatkezelőtől vagy adatfeldolgozótól az egyesült királyságbeli adatkezelőkhöz vagy adatfeldolgozókhoz történő továbbításra további engedély megszerzése nélkül kerülhet sor.

(280) Ugyanakkor emlékeztetni kell arra, hogy az (EU) 2016/679 irányelv 58. cikkének (5) bekezdése alapján, és amint azt a Bíróság a Schrems-ítéletben ([507]) kifejtette, amennyiben egy nemzeti adatvédelmi hatóság megkérdőjelezi – ideértve a panaszra történő eljárást is – a Bizottság megfelelőségi határozatának az egyén magánélethez és adatvédelemhez fűződő alapvető jogaival való összeegyeztethetőségét, a nemzeti jognak biztosítania kell a jogorvoslati lehetőségeket, amelyek lehetővé teszik számára, hogy a nemzeti bíróságok előtt a kifogásokra hivatkozzon annak érdekében, hogy azok esetlegesen előzetes döntéshozatali eljárást kezdeményezhessenek e határozat érvényességének vizsgálata céljából ([508]).

([507]) Schrems-ügy, 65. pont.

([508]) Schrems-ügy, 65. pont: Ezzel összefüggésben a nemzeti jogalkotó feladata, hogy előírja azon jogorvoslati lehetőségeket, amelyek lehetővé teszik az érintett nemzeti felügyelő hatóság számára, hogy a nemzeti bíróságok előtt az általa megalapozottnak talált kifogásokra hivatkozzon annak érdekében, hogy amennyiben az utóbbiak osztják e hatóságnak a bizottsági határozat érvényessége tekintetében fennálló kétségeit, előzetes döntéshozatali eljárást kezdeményezhessenek e határozat érvényességének vizsgálata céljából.

(6) E HATÁROZAT NYOMON KÖVETÉSE, FELFÜGGESZTÉSE, VISSZAVONÁSA VAGY MÓDOSÍTÁSA

(281) Az (EU) 2016/679 rendelet 45. cikkének (4) bekezdése értelmében a Bizottságnak folyamatosan figyelemmel kell kísérnie az Egyesült Királyságban az e határozat elfogadását követő fejleményeket annak értékelése érdekében, hogy az továbbra is biztosítja-e a lényegében azonos szintű védelmet. Az említett nyomon követés ebben az esetben különösen fontos, mivel az Egyesült Királyság egy olyan új adatvédelmi rendszert fog igazgatni, alkalmazni és végrehajtani, amelyre már nem vonatkozik az európai uniós jog, és amely változhat. Ebben a tekintetben különös figyelmet fognak fordítani a személyes adatok harmadik országokba történő továbbítására vonatkozó egyesült királyságbeli szabályok gyakorlati alkalmazására, valamint annak az e határozat alapján továbbított adatok esetében nyújtott védelem szintjére gyakorolt hatására; az egyéni jogok gyakorlásának hatékonyságára, ideértve az ilyen jogok alóli kivételeket vagy korlátozásokat érintő törvényi és gyakorlati fejleményeket (nevezetesen a határt átlépő személyforgalom hatékony ellenőrzésének fenntartásával kapcsolatosakat); valamint a kormányzati hozzáféréssel kapcsolatos korlátozások és biztosítékok betartására. Többek között az ítélkezési gyakorlat alakulása és az információügyi biztos és más független testületek általi felügyelet fog adatokat szolgáltatni a Bizottság általi nyomon követéshez.

(282) Az Egyesült Királyság hatóságainak haladéktalanul tájékoztatniuk kell a Bizottságot az Egyesült Királyság jogrendjének minden olyan lényeges változásáról, amely hatást gyakorol az e határozat tárgyát képező jogi keretre, valamint személyes adatok az e határozatban értékelt kezelésével kapcsolatos gyakorlatok minden változásáról, mind a személyes adatok adatkezelők és adatfeldolgozók általi, az Egyesült Királyság általános adatvédelmi rendelete szerinti kezelését, mind a személyes adatokhoz a közigazgatási szervek általi hozzáférést illető korlátozásokat és biztosítékokat illetően. Ennek ki kell terjednie a (281) preambulumbekezdésben említett elemekkel kapcsolatos fejleményekre.

(283) Továbbá annak lehetővé tétele érdekében, hogy a Bizottság hatékonyan lássa el nyomonkövetési feladatát, a tagállamoknak tájékoztatniuk kell a Bizottságot a nemzeti adatvédelmi hatóságok minden vonatkozó lépéséről, különösen az uniós érintetteknek a személyes adatok Európai Unióból az egyesült királyságbeli adatkezelők vagy adatfeldolgozók felé történő továbbításával kapcsolatos kérései vagy panaszai tekintetében. A Bizottságot továbbá tájékoztatni kell minden arra utaló információról, hogy a bűnügyek megelőzéséért, nyomozásáért, felderítéséért vagy a vádemelésért, illetve a nemzetbiztonságért felelős egyesült királyságbeli közigazgatási szervek intézkedései nem biztosítják a megfelelő szintű védelmet.

(284) Amennyiben a rendelkezésre álló információk, különösen az e határozat nyomon követéséből származó, vagy az Egyesült Királyság vagy a tagállamok hatóságai által szolgáltatott információk arra utalnak, hogy az Egyesült Királyság által biztosított védelem szintje már nem feltétlenül megfelelő, a Bizottságnak erről haladéktalanul tájékoztatnia kell az Egyesült Királyság illetékes hatóságait, és kérheti a megfelelő intézkedések meghatározott, három hónapot meg nem haladó határidőn belüli meghozatalát. Szükség esetén ez a határidő egy meghatározott időtartammal meghosszabbítható, figyelembe véve a szóban forgó kérdés jellegét és/vagy a meghozandó intézkedéseket. Például egy ilyen eljárás azokban az esetekben indul, amennyiben az újbóli adattovábbítás – ideértve a miniszter által elfogadott új megfelelőségi rendeleteket vagy az Egyesült Királyság által kötött nemzetközi megállapodásokat – már nem a védelem az (EU) 2016/679 rendelet 44. cikke értelmében vett folytonosságát biztosító biztosítékok mellett történik.

(285) Ha az említett határidő lejártakor az Egyesült Királyság illetékes hatóságai nem hozzák meg ezeket az intézkedéseket, vagy más módon nem bizonyítják kielégítően, hogy e határozat továbbra is a megfelelő szintű védelmen alapul, a Bizottság megindítja az (EU) 2016/679 rendelet 93. cikkének (2) bekezdésében említett eljárást e határozat részleges vagy teljes felfüggesztése vagy hatályon kívül helyezése céljából.

(286) Ennek alternatívájaként a Bizottságnak ezt az eljárást e határozat módosítása céljából indítja meg, különösen az adattovábbításra további feltételek előírásával vagy a megfelelőség megállapítása hatályának azokra az adattovábbításokra korlátozásával, amelyek esetében biztosított a megfelelő szintű védelem folyamatossága.

(287) Megfelelően indokolt, rendkívül sürgős esetben a Bizottság élni fog azzal a lehetőséggel, hogy az (EU) 2016/679 rendelet 93. cikkének (3) bekezdésében említett eljárásnak megfelelően azonnal alkalmazandó, a határozatot felfüggesztő, hatályon kívül helyező vagy módosító végrehajtási jogi aktusokat fogadjon el.

(7) A HATÁROZAT TARTAMA ÉS MEGÚJÍTÁSA

(288) A Bizottságnak figyelembe kell vennie, hogy a kilépési megállapodásban előírt átmeneti időszak lejártával és amint az EU – Egyesült Királyság kereskedelmi és együttműködési megállapodás 782. cikke szerinti ideiglenes rendelkezés hatályát veszti, egy új adatvédelmi rendszert fog igazgatni, alkalmazni és végrehajtani azzal összehasonlítva, amely akkor volt érvényben, amikor az Európai Unió joga kötötte. Ez nevezetesen az e határozatban értékelt adatvédelmi keret módosításával vagy változásával, valamint egyéb releváns fejleményekkel járhat.

(289) Ezért helyénvaló előírni, hogy ezt a határozatot a hatálybalépésétől számított négy évig kell alkalmazni.

(290) Amennyiben különösen az e határozat nyomon követéséből származó információk azt jelzik, hogy az Egyesült Királyságban biztosított védelmi szint megfelelőségére vonatkozó megállapítások még mindig ténybelileg és jogilag indokoltak, a Bizottság e határozat alkalmazásának megszűnése előtt legkésőbb hat hónappal megindítja az e határozat annak időbeli hatálya elvileg további négy évvel történő meghosszabbításával történő módosítására irányuló eljárást. Az e határozatot módosító, említett végrehajtási jogi aktusokat az (EU) 2016/679 rendelet 93. cikkének (2) bekezdésében említett eljárással összhangban kell elfogadni.

(8) ZÁRÓ MEGÁLLAPÍTÁSOK

(291) Az Európai Adatvédelmi Testület közzétette véleményét ([509]), amely e határozat kidolgozásakor figyelembevételre került.

(292) Az e határozatban előírt intézkedések összhangban vannak a 2016/679/EU rendelet 93. cikkével létrehozott bizottság véleményével,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

(1) Az (EU) 2016/679 rendelet 45. cikkének alkalmazásában az Egyesült Királyság biztosítja az (EU) 2016/679 rendelet hatálya alá tartozó, az Európai Unióból az Egyesült Királyságba továbbított személyes adatok megfelelő szintű védelmét.

(2) Ez a határozat nem terjed ki a határt átlépő személyforgalom Egyesült Királyság általi ellenőrzése céljaira továbbított vagy azon személyes adatokra, amelyek egyébként a határt átlépő személyforgalom hatékony ellenőrzése fenntartása céljából az érintettek jogai alóli, az Egyesült Királyság 2018. évi adatvédelmi törvényének 2. melléklete 4. pontjának (1) bekezdése szerinti egyes kivételek hatálya alá tartoznak.

2. cikk

Az érintett tagállam haladéktalanul tájékoztatja a Bizottságot, amikor a személyes adataik kezelése tekintetében az egyének védelme érdekében a tagállam illetékes felügyeleti hatóságai gyakorolják az (EU) 2016/679 rendelet 58. cikke értelmében vett hatáskörüket az 1. cikkben meghatározott alkalmazási körön belüli adattovábbítások tekintetében.

3. cikk

(1) A Bizottság folyamatosan figyelemmel kíséri az e határozat alapját képező jogi keret alkalmazását – ideértve az újbóli adattovábbítások lebonyolításának, az egyéni jogok gyakorlásának és az egyesült királyságbeli hatóságok e határozat alapján továbbított adatokhoz való hozzáférésnek feltételeit – annak értékelése céljából, hogy Egyesült Királyság az 1. cikk értelmében továbbra is megfelelő szintű védelmet biztosít-e.

(2) A tagállamok és a Bizottság tájékoztatják egymást az olyan esetekről, amikor az információügyi biztos vagy bármely egyéb illetékes egyesült királyságbeli hatóság nem biztosítja az e határozat alapjául szolgáló jogi keretnek való megfelelést.

(3) A tagállamok és a Bizottság tájékoztatják egymást bármely arra utaló körülményről, hogy az egyesült királyságbeli hatóságoknak az egyének személyes adataik védelméhez fűződő jogába történő beavatkozása túllépi a feltétlenül szükséges mértéket vagy nem létezik hatékony jogvédelem az említett beavatkozásokkal szemben.

(4) Ha a Bizottság arra utaló jeleket észlel, hogy a megfelelő szintű védelem már nem biztosított, a Bizottság tájékoztatja az Egyesült Királyság illetékes hatóságait, és felfüggesztheti, hatályon kívül helyezheti vagy módosíthatja ezt a határozatot.

([509]) 14/2021 vélemény az Európai Bizottságnak a személyes adatok Egyesült Királyságban történő megfelelő védelméről szóló, az (EU) 2016/679 rendelet szerinti végrehajtási határozattervezetéről, elérhető a következő linken: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

(5) A Bizottság felfüggesztheti, hatályon kívül helyezheti vagy módosíthatja ezt a határozatot, ha az Egyesült Királyság kormánya együttműködésének hiánya miatt a Bizottság nem tudja megállapítani, hogy az 1. cikk (1) bekezdésében szereplő megállapítás fennáll-e.

4. cikk

Ez a határozat 2025. június 27-én hatályát veszti, kivéve, ha az (EU) 2016/679 rendelet 93. cikkének (2) bekezdésében említett eljárással összhangban meghosszabbítják.

5. cikk

Ennek a határozatnak a tagállamok a címzettjei.

Kelt Brüsszelben, 2021. június 28-án.

a Bizottság részéről
Didier REYNDERS
a Bizottság tagja