II

(Nelegislatívne akty)

ROZHODNUTIA

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2021/1772

z 28. júna 2021

podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o primeranej ochrane osobných údajov Spojeným kráľovstvom

[oznámené pod číslom C(2021) 4800]

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) ([1]), a najmä na jeho článok 45 ods. 3,

keďže:

1. ÚVOD

(1) V nariadení (EÚ) 2016/679 sa stanovujú pravidlá prenosu osobných údajov od prevádzkovateľov alebo sprostredkovateľov v Európskej únii do tretích krajín a medzinárodným organizáciám, pokiaľ tieto prenosy patria do rozsahu jeho pôsobnosti. Pravidlá medzinárodných prenosov údajov sú stanovené v kapitole V uvedeného nariadenia, a to v článkoch 44 až 50. Hoci je pre rozmach medzinárodnej spolupráce a cezhraničného obchodu nevyhnutný tok osobných údajov do krajín mimo Európskej únie aj z takýchto krajín, prenosy do tretích krajín nesmú ohrozovať poskytovanú úroveň ochrany osobných údajov v Európskej únii ([2]).

(2) Podľa článku 45 ods. 3 nariadenia (EÚ) 2016/679 môže Komisia prostredníctvom vykonávacieho aktu rozhodnúť, že tretia krajina, územie alebo jeden či viaceré určené sektory v tretej krajine alebo medzinárodná organizácia zaručujú primeranú úroveň ochrany. Za tejto podmienky sa prenosy osobných údajov do tretej krajiny môžu uskutočňovať bez potreby získania ďalšieho povolenia, ako sa stanovuje v článku 45 ods. 1 a v odôvodnení 103 uvedeného nariadenia.

(3) Ako sa uvádza v článku 45 ods. 2 nariadenia (EÚ) 2016/679, prijatie rozhodnutia o primeranosti musí vychádzať z komplexnej analýzy právneho poriadku tretej krajiny, pričom sa vzťahuje na pravidlá uplatniteľné na dovozcov údajov, ako aj na obmedzenia a záruky týkajúce sa prístupu k osobným údajom zo strany orgánov verejnej moci. Komisia musí v rámci svojho posúdenia určiť, či dotknutá tretia krajina zaručuje úroveň ochrany, ktorá v „zásade zodpovedá“ úrovni zabezpečenej v rámci Európskej únie [odôvodnenie 104 nariadenia (EÚ) 2016/679]. Štandard, voči ktorému sa posudzuje „zásadná rovnocennosť“, je štandard stanovený v právnych predpisoch Európskej únie, najmä v nariadení (EÚ) 2016/679, ako aj v judikatúre Súdneho dvora Európskej únie ([3]). V tejto súvislosti má význam aj referenčné kritérium primeranosti Európskeho výboru pre ochranu údajov (ďalej len „EDPBI“) ([4]).

([1]) Ú. v. EÚ L 119, 4.5.2016, s. 1.
([2]) Pozri odôvodnenie 101 nariadenia (EÚ) 2016/679.
([3]) Pozri spomedzi najnovších vec C-311/18, Facebook Ireland/Schrems (ďalej len „Schrems II“), ECLI:EU:C:2020:559.
([4]) Európsky výbor pre ochranu údajov, Referenčné kritérium primeranosti, WP 254 rev. 01, k dispozícii na tomto odkaze: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Ako objasnil Súdny dvor Európskej únie, nie je potrebné, aby bola zaistená rovnaká úroveň ochrany ([5]). Konkrétne prostriedky, ktoré dotknutá tretia krajina využíva na ochranu osobných údajov, sa môžu líšiť od prostriedkov využívaných v Európskej únii, pokiaľ sa v praxi preukáže, že sa nimi účinne zabezpečuje primeraná úroveň ochrany ([6]). V záujme dosiahnutia štandardu primeranosti teda nie je potrebné, aby pravidlá druhej krajiny do detailu zodpovedali pravidlám Únie. Namiesto toho sa skôr overuje, či zahraničný systém ako celok zabezpečuje prostredníctvom hmotnoprávnej úpravy práv na ochranu údajov a ich účinného vykonávania, vymáhania, ako aj dohľadu nad nimi požadovanú úroveň ochrany ([7]).

(5) Komisia dôkladne zanalyzovala právne predpisy a prax Spojeného kráľovstva. Komisia na základe zistení uvedených v odôvodneniach 8 až 270 dospela k záveru, že Spojené kráľovstvo zabezpečuje primeranú úroveň ochrany osobných údajov prenášaných v rámci rozsahu pôsobnosti nariadenia (EÚ) 2016/679 z Európskej únie do Spojeného kráľovstva.

(6) Tento záver sa netýka osobných údajov prenášaných na účely imigračnej kontroly Spojeného kráľovstva ani takých, ktoré inak patria do rozsahu výnimky z určitých práv dotknutých osôb na účely zachovania účinnej imigračnej kontroly (ďalej len „imigračná výnimka“) podľa bodu 4 ods. 1 prílohy 2 k zákonu Spojeného kráľovstva o ochrane údajov. Platnosť a výklad imigračnej výnimky v rámci práva Spojeného kráľovstva nie sú po rozhodnutí odvolacieho súdu Anglicka a Walesu z 26. mája 2021 jednoznačné. Hoci sa uznáva, že práva dotknutých osôb môžu byť v zásade obmedzené na účely imigračnej kontroly ako „dôležitý aspekt verejného záujmu“, odvolací súd zistil, že imigračná výnimka je vo svojej súčasnej forme nezlučiteľná s právom Spojeného kráľovstva, keďže v legislatívnom opatrení chýbajú konkrétne ustanovenia stanovujúce záruky uvedené v článku 23 ods. 2 všeobecného nariadenia Spojeného kráľovstva o ochrane osobných údajov ([8]). Za týchto podmienok by prenosy osobných údajov z Únie do Spojeného kráľovstva, na ktoré sa môže uplatniť imigračná výnimka, mali byť vylúčené z pôsobnosti tohto rozhodnutia ([9]). Po napravení nezlučiteľnosti s právom Spojeného kráľovstva by sa mala imigračná výnimka, ako aj potreba udržiavať obmedzenia pôsobnosti tohto rozhodnutia opätovne posúdiť.

(7) Toto rozhodnutie by nemalo mať vplyv na priame uplatňovanie nariadenia (EÚ) 2016/679 na organizácie usadené v Spojenom kráľovstve, ak sú splnené podmienky týkajúce sa územnej pôsobnosti uvedeného nariadenia stanovené v jeho článku 3.

2. PRAVIDLÁ, KTORÉ SA VZŤAHUJÚ NA SPRACÚVANIE OSOBNÝCH ÚDAJOV

2.1. Ústavný rámec

(8) Spojené kráľovstvo je parlamentnou demokraciou, ktorá má ako hlava štátu konštitučného panovníka. Má suverénny parlament, ktorý je nadriadený všetkým ostatným vládnym inštitúciám, orgán výkonnej moci, ktorý je volený z členov parlamentu a ktorý sa tomuto parlamentu zodpovedá, a nezávislé súdnictvo. Výkonná moc vychádza zo spôsobilosti získať vyslovenie dôvery volenej Dolnej snemovne (House of Commons) a zodpovedá sa obom snemovniam parlamentu, ktoré sú zodpovedné za kontrolu vlády a za prerokúvanie a prijímanie zákonov.

([5]) Vec C-362/14, Schrems (ďalej len „Schrems I“), ECLI:EU:C:2015:650, bod 73.

([6]) Schrems II, bod 74.

([7]) Pozri oznámenie Komisie Európskemu parlamentu a Rade s názvom „Výmena a ochrana osobných údajov v globalizovanom svete“, COM(2017) 7 z 10. januára 2017, oddiel 3.1, s. 6 – 7, k dispozícii na tomto odkaze: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52017DC0007&from=SK.

([8]) Odvolací súd (občianskoprávne oddelenie), Open Rights Group/Secretary of State for the Home Department a Secretary of State for Digital, Culture, Media and Sport, (2021) EWCA Civ 800, body 53 až 56. Odvolací súd zmenil rozhodnutie Vrchného súdu (High Court of Justice), v ktorom bola predtým výnimka posúdená na základe nariadenia (EÚ) 2016/679 (najmä jeho článku 23) a Charty základných práv Európskej únie a v ktorom konštatoval, že výnimka je zákonná [Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor (2019) EWHC 2562].

([9]) Za predpokladu, že príslušné podmienky sú splnené, prenosy na účely imigračnej kontroly Spojeného kráľovstva môžu byť uskutočnené na základe mechanizmov prenosu, ktoré sú stanovené v článkoch 46 až 49 nariadenia (EÚ) 2016/679.

(9) Parlament Spojeného kráľovstva preniesol zodpovednosť za prijímanie právnych predpisov o vnútroštátnych záležitostiach v Škótsku, vo Walese a v Severnom Írsku, ktoré Parlament Spojeného kráľovstva nevyhradil pre seba, na Škótsky parlament, Waleský parlament (Senedd Cymru) a Zhromaždenie Severného Írska. Hoci ochrana údajov je vyhradenou záležitosťou, t. j. rovnaké právne predpisy sa uplatňujú v celej krajine, v ostatných oblastiach politiky relevantných pre toto rozhodnutie sa zodpovednosť preniesla. Napríklad zodpovednosť v rámci systémov trestnej justície vrátane policajnej činnosti v Škótsku a Severnom Írsku sa preniesla na Škótsky parlament, resp. Zhromaždenie Severného Írska. Spojené kráľovstvo nemá kodifikovanú ústavu v zmysle zakotveného konštitutívneho dokumentu. Ústavné zásady sa ustálili postupne, najmä na základe judikatúry a zvyklostí. Súdy uznali ústavnú hodnotu niektorých právnych predpisov, ako je Magna charta, Listina práv z roku 1689 a zákon o ľudských právach z roku 1998. Základné práva jednotlivcov sa formovali ako súčasť ústavy prostredníctvom common law, uvedených právnych predpisov a medzinárodných dohovorov, najmä Európskeho dohovoru o ľudských právach, ktorý Spojené kráľovstvo ratifikovalo v roku 1951. Spojené kráľovstvo v roku 1987 ratifikovalo aj Dohovor Rady Európy o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (dohovor č. 108) ([10]).

(10) Zákonom o ľudských právach z roku 1998 (Human Rights Act) sa začleňujú práva obsiahnuté v Európskom dohovore o ľudských právach do práva Spojeného kráľovstva. Zákonom o ľudských právach sa zaručujú každému jednotlivcovi základné práva a slobody stanovené v článkoch 2 až 12 a článku 14 Európskeho dohovoru o ľudských právach, článkoch 1, 2 a 3 prvého protokolu k nemu a článku 1 trinásteho protokolu k nemu v spojení s článkami 16, 17 a 18 uvedeného dohovoru. Patrí sem právo na rešpektovanie súkromného a rodinného života (a ako súčasť tohto práva aj právo na ochranu údajov) a právo na spravodlivý proces ([11]). Najmä v súlade s článkom 8 uvedeného dohovoru môže štátny orgán do výkonu práva na súkromie zasahovať len v prípadoch, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných.

(11) V súlade so zákonom o ľudských právach z roku 1998 musí byť každá činnosť orgánov verejnej moci zlučiteľná s právom podľa dohovoru ([12]). Okrem toho je potrebné, aby sa primárne a podriadené právne predpisy interpretovali a uplatňovali spôsobom, ktorý je zlučiteľný s právami vyplývajúcim z dohovoru ([13]).

2.2. **Rámec ochrany údajov Spojeného kráľovstva**

(12) Spojené kráľovstvo vystúpilo z Európskej únie 31. januára 2020. Na základe Dohody o vystúpení Spojeného kráľovstva Veľkej Británie a Severného Írska z Európskej únie a z Európskeho spoločenstva pre atómovú energiu ([14]) sa právo Únie naďalej uplatňovalo v Spojenom kráľovstve počas prechodného obdobia do 31. decembra 2020. Legislatívny rámec ochrany osobných údajov v Spojenom kráľovstve pred vystúpením a počas prechodného obdobia pozostával z príslušných právnych predpisov EÚ [najmä nariadenia (EÚ) 2016/679 a smernice Európskeho parlamentu a Rady (EÚ) 2016/680 ([15])] a vnútroštátnych právnych predpisov, najmä zo zákona o ochrane údajov z roku 2018 (Data Protection Act) ([16]), v ktorom sa stanovujú vnútroštátne pravidlá v prípadoch, keď to umožňuje nariadenie (EÚ) 2016/679, pričom sa špecifikuje a obmedzuje uplatňovanie pravidiel nariadenia (EÚ) 2016/679 a transponovanej smernice (EÚ) 2016/680.

([10]) Zásady dohovoru č. 108 boli pôvodne implementované do právneho poriadku Spojeného kráľovstva prostredníctvom zákona o ochrane údajov z roku 1984, ktorý bol nahradený zákonom o ochrane údajov z roku 1998 a následne zákonom o ochrane údajov z roku 2018 (v spojení so všeobecným nariadením Spojeného kráľovstva o ochrane údajov). Spojené kráľovstvo v roku 2018 podpísalo aj protokol, ktorým sa mení Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (známy ako dohovor č. 108+) a v súčasnosti pracuje na ratifikácii dohovoru.

([11]) Články 6 a 8 EDĽP (pozri aj prílohu 1 k zákonu o ľudských právach z roku 1998).

([12]) § 6 zákona o ľudských právach z roku 1998.

([13]) § 3 zákona o ľudských právach z roku 1998.

([14]) Dohoda o vystúpení Spojeného kráľovstva Veľkej Británie a Severného Írska z Európskej únie a z Európskeho spoločenstva pre atómovú energiu 2019/C 384 I/01, XT/21054/2019/INIT (Ú. v. EÚ C 384I, 12. 11. 2019, s. 1), k dispozícii na tomto odkaze: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=SK.

([15]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (Ú. v. EÚ L 119, 4.5.2016, s. 89), k dispozícii na tomto odkaze: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32016L0680&from=SK.

([16]) Zákon o ochrane údajov z roku 2018, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(13) Vláda Spojeného kráľovstva s cieľom pripraviť sa na vystúpenie z EÚ prijala zákon o vystúpení z Európskej únie z roku 2018 ([17]), ktorým sa priamo uplatniteľné právne predpisy Únie začleňujú do práva Spojeného kráľovstva ([18]). Toto tzv. ponechané právo EÚ zahŕňa nariadenie (EÚ) 2016/679 v celom jeho rozsahu (vrátane odôvodnení) ([19]). V súlade s uvedeným zákonom musia súdy Spojeného kráľovstva vykladať nezmenené ponechané právo EÚ v súlade s príslušnou judikatúrou Súdneho dvora a všeobecnými zásadami práva Únie tak, ako boli účinné bezprostredne pred skončením prechodného obdobia (nazývané „ponechaná judikatúra EÚ“, resp. „ponechané všeobecné zásady práva EÚ“) ([20]).

(14) Podľa zákona o vystúpení z Európskej únie z roku 2018 majú ministri Spojeného kráľovstva právomoc prostredníctvom štatutárnych nástrojov zaviesť sekundárne právne predpisy s cieľom vykonať v dôsledku vystúpenia Spojeného kráľovstva z Európskej únie potrebné zmeny v ponechanom práve Európskej únie. Túto právomoc uplatnili prijatím právnych predpisov o ochrane údajov, súkromia a elektronických komunikáciách v dôsledku vystúpenia z EÚ z roku 2019 (DPPEC Regulations) ([21]). Právnymi predpismi o ochrane údajov, súkromí a elektronických komunikáciách sa mení nariadenie (EÚ) 2016/679, ktoré sa do nich zaviedlo prostredníctvom zákona o vystúpení z Európskej únie z roku 2018, zákona o ochrane údajov z roku 2018 a ďalších právnych predpisov o ochrane údajov, aby zodpovedalo vnútroštátnym okolnostiam ([22]).

(15) Právny rámec ochrany osobných údajov v Spojenom kráľovstve po skončení prechodného obdobia teda tvorí:

— všeobecné nariadenie Spojeného kráľovstva o ochrane údajov, ako bolo podľa zákona o vystúpení z Európskej únie z roku 2018 začlenené do práva Spojeného kráľovstva a zmenené právnymi predpismi o ochrane údajov, súkromí a elektronických komunikáciách ([23]), a

— zákon o ochrane údajov z roku 2018 ([24]) zmenený právnymi predpismi o ochrane údajov, súkromí a elektronických komunikáciách.

(16) Keďže sa všeobecné nariadenie Spojeného kráľovstva o ochrane údajov zakladá na právnych predpisoch EÚ, pravidlá ochrany údajov v Spojenom kráľovstve v mnohých aspektoch odzrkadľujú príslušné pravidlá, ktoré sú platné v Európskej únii.

(17) Okrem právomocí, ktoré sa ministrovi priznávajú prostredníctvom zákona o vystúpení z Európskej únie z roku 2018, v niekoľkých ustanoveniach zákona o ochrane údajov z roku 2018 sa ministrovi priznáva právomoc prijímať sekundárne právne predpisy s cieľom zmeniť určité ustanovenia zákona alebo stanoviť doplnkové a dodatočné pravidlá ([25]). Minister dosiaľ uplatnil len právomoc podľa § 137 zákona o ochrane údajov z roku 2018, ktorou bolo

([17]) Zákon o vystúpení z Európskej únie z roku 2018, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2018/16/contents.

([18]) Zámerom a účinkom zákona o vystúpení z Európskej únie z roku 2018 je, že všetky priame právne predpisy Únie, ktoré boli začlenené do práva Spojeného kráľovstva na konci prechodného obdobia, sa začleňujú do práva Spojeného kráľovstva, keďže nadobúdajú účinnosť v práve EÚ bezprostredne pred koncom prechodného obdobia, pozri § 3 zákona o vystúpení z Európskej únie z roku 2018.

([19]) Vo vysvetlivkách k zákonu o vystúpení z Európskej únie z roku 2018 sa špecifikuje: „Ak sú právne predpisy upravené podľa tohto §, súčasťou vnútroštátnych právnych predpisov bude práve znenie samotného právneho predpisu. Bude obsahovať úplné znenie akéhokoľvek nástroja EÚ (vrátane jeho odôvodnení).“ (Vysvetlivky k zákonu o vystúpení z Európskej únie z roku 2018, bod 83, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Podľa informácií, ktoré poskytli orgány Spojeného kráľovstva, vzhľadom na to, že odôvodnenia nie sú záväznými právnymi pravidlami, nebolo ich potrebné meniť rovnakým spôsobom, ako boli zmenené články nariadenia (EÚ) 2016/679 právnymi predpismi o ochrane údajov, súkromí a elektronických komunikáciách (zmeny atď.) (vystúpenie z EÚ) [The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations].

([20]) § 6 zákona o vystúpení z Európskej únie z roku 2018.

([21]) Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (právne predpisy o ochrane údajov, súkromia a elektronických komunikáciách v dôsledku vystúpenia z EÚ z roku 2019), k dispozícii na tomto odkaze: https://www.legislation.gov.uk/uksi/2019/419/contents/made, zmenené právnymi predpismi o ochrane údajov, súkromí a elektronických komunikáciách z roku 2020, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([22]) Tieto zmeny všeobecného nariadenia Spojeného kráľovstva o ochrane údajov a zákona o ochrane údajov z roku 2018 sú väčšinou technického charakteru, ako je vypustenie odkazov na „členské štáty“ alebo úprava terminológie, napr. nahradenie odkazov na nariadenie (EÚ) 2016/679 odkazmi na všeobecné nariadenie Spojeného kráľovstva o ochrane údajov. V niektorých prípadoch boli potrebné zmeny, aby sa zohľadnili výlučne vnútroštátne okolnosti ustanovení, napríklad pokiaľ ide o to, „kto“ je oprávnený prijímať „právne predpisy o primeranosti“ na účely legislatívneho rámca ochrany údajov Spojeného kráľovstva (pozri § 17A zákona o ochrane údajov z roku 2018), t. j. minister namiesto Európskej komisie.

([23]) Všeobecné nariadenie Spojeného kráľovstva o ochrane údajov, Keeling Schedule (zmeny nariadenia), k dispozícii na tomto odkaze: 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]) Zákon o ochrane údajov z roku 2018, Keeling Schedule (zmeny zákona), k dispozícii na tomto odkaze: 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]) Takéto právomoci sú obsiahnuté napríklad v § 16 (právomoc zavádzať v špecifických, úzko vymedzených situáciách ďalšie výnimky z konkrétnych ustanovení všeobecného nariadenia Spojeného kráľovstva o ochrane údajov), § 17A (právomoc prijímať právne predpisy o primeranosti), § 212 a 213 (právomoci iniciovať právne predpisy a vytvárať prechodné ustanovenia) a § 211 (právomoc vykonávať malé a následné zmeny) zákona o ochrane údajov z roku 2018.

prijať právne predpisy o ochrane údajov (poplatky a informácie) (zmena) z roku 2019, v ktorých sa stanovujú okolnosti, keď sú prevádzkovatelia povinní platiť ročný poplatok nezávislému orgánu Spojeného kráľovstva pre ochranu údajov, Komisárovi pre informácie.

(18) Napokon sa ďalšie usmernenia týkajúce sa právnych predpisov Spojeného kráľovstva o ochrane údajov uvádzajú v kódexoch postupov a iných usmerneniach, ktoré prijíma Komisár pre informácie. Aj keď tieto usmernenia nie sú z formálneho hľadiska právne záväzné, majú význam, pokiaľ ide o výklad, a ukazujú, ako Komisár v praxi uplatňuje a presadzuje právne predpisy o ochrane údajov. Konkrétne v § 121 až § 125 zákona o ochrane údajov z roku 2018 sa od Komisára vyžaduje, aby vypracoval kódexy postupov v oblasti poskytovania údajov, priameho marketingu, navrhovania primeranému veku, ochrany údajov a žurnalistiky.

(19) Právny rámec Spojeného kráľovstva, ktorý sa uplatňuje na údaje prenášané podľa tohto rozhodnutia, je teda svojou štruktúrou a hlavnými zložkami veľmi podobný rámcu, ktorý sa uplatňuje v Európskej únii. To zahŕňa aj skutočnosť, že takýto rámec sa neopiera len o povinnosti stanovené vo vnútroštátnom práve, ktoré boli formované právom EÚ, ale aj o povinnosti zakotvené v medzinárodnom práve, najmä prostredníctvom pristúpenia Spojeného kráľovstva k EDĽP a dohovoru č. 108, ako aj o podriadenie tohto rámca pod právomoc Európskeho súdu pre ľudské práva. Tieto povinnosti vyplývajúce z právne záväzných medzinárodných nástrojov, najmä pokiaľ ide o ochranu osobných údajov, sú preto osobitne dôležitým prvkom právneho rámca posudzovaného v tomto rozhodnutí.

2.3. **Vecná a územná pôsobnosť**

(20) Všeobecné nariadenie Spojeného kráľovstva o ochrane údajov sa podobne ako nariadenie (EÚ) 2016/679 vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami alebo na iné spracúvanie v prípade osobných údajov, ktoré tvoria súčasť informačného systému ([26]). Vymedzenie pojmov „osobné údaje“, „dotknutá osoba“ a „spracúvanie“ vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov je totožné s vymedzením pojmov v nariadení (EÚ) 2016/679 ([27]). Všeobecné nariadenie Spojeného kráľovstva o ochrane údajov sa navyše vzťahuje na manuálne neštruktúrované spracúvanie osobných údajov ([28]), ktoré majú v držbe niektoré orgány verejnej moci Spojeného kráľovstva ([29]), hoci zásady a práva vyplývajúce zo všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, ktoré nie sú relevantné pre takéto osobné údaje, sa nevzťahujú na § 24 a § 25 zákona o ochrane údajov z roku 2018. Podobne ako v ustanoveniach nariadenia (EÚ) 2016/679 sa ani všeobecné nariadenie Spojeného kráľovstva o ochrane údajov nevzťahuje na spracúvanie osobných údajov jednotlivcom v rámci výlučne osobnej alebo domácej činnosti ([30]).

(21) Všeobecným nariadením Spojeného kráľovstva o ochrane údajov sa rozširuje jeho pôsobnosť aj na spracúvanie v rámci činnosti, ktorá bezprostredne pred koncom prechodného obdobia nepatrila do pôsobnosti práva Európskej únie (napr. národná bezpečnosť) ([31]) alebo patrila do pôsobnosti kapitoly 2 hlavy 5 Zmluvy o Európskej únii (činnosti spoločnej zahraničnej a bezpečnostnej politiky) ([32]). Všeobecné nariadenie Spojeného kráľovstva o ochrane údajov sa tak, ako to je aj v systéme Európskej únie, nevzťahuje na spracúvanie osobných údajov príslušným orgánom na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo výkonu

([26]) Článok 2 ods. 1 a 5 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov.

([27]) Článok 4 ods. 1 a 2 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov.

([28]) Manuálne neštruktúrované spracúvanie osobných údajov je vymedzené v článku 2 ods. 5 písm. b) ako spracúvanie osobných údajov, ktoré nie je automatizovaným ani štruktúrovaným spracúvaním osobných údajov.

([29]) V článku 2 ods. 1A všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sa stanovuje, že nariadenie sa vzťahuje na manuálne neštruktúrované spracúvanie osobných údajov, ktoré má v držbe orgán verejnej moci podľa zákona o slobodnom prístupe k informáciám. Orgány verejnej moci podľa zákona o slobodnom prístupe k informáciám sú akýmikoľvek orgánmi verejnej moci vymedzenými v zákone o slobodnom prístupe k informáciám z roku 2000 alebo akýmikoľvek škótskymi orgánmi verejnej moci vymedzenými v škótskom zákone o slobodnom prístupe k informáciám z roku 2002 (zákon Škótskeho parlamentu č. 13). a § 21 ods. 5 zákona o ochrane údajov z roku 2018.

([30]) Článok 2 ods. 2 písm. a) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov.

([31]) Činnosti národnej bezpečnosti patria do pôsobnosti všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, pokiaľ ich nevykonáva príslušný orgán na účely presadzovania práva, v takom prípade sa na ne vzťahuje časť 3 zákona o ochrane údajov z roku 2018, nevykonávajú ich spravodajské služby ani sa nevykonávajú v ich mene, keďže činnosti spravodajských služieb nepatria do pôsobnosti všeobecného nariadenia Spojeného kráľovstva o ochrane údajov a podľa článku 2 ods. 2 písm. c) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sa na ne vzťahuje časť 4 zákona o ochrane údajov z roku 2018. Napríklad policajná zložka môže vykonať bezpečnostnú previerku zamestnanca, aby sa zabezpečilo, že mu je možné dôverovať pri prístupe k materiálom týkajúcim sa národnej bezpečnosti. Napriek tomu, že polícia je príslušným orgánom na účely presadzovania práva, uvedené spracúvanie nie je určené na účel presadzovania práva a vzťahovalo by sa naň všeobecné nariadenie Spojeného kráľovstva o ochrane údajov. Pozri Vysvetľujúci rámec Spojeného kráľovstva pre diskusiu o primeranosti, oddiel H s názvom „Ochrana údajov v oblasti národnej bezpečnosti a rámec vyšetrovacích právomocí“, strana 8, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf.

([32]) Článok 2 ods. 1 písm. a) a b) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov.

trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzania (tzv. účely presadzovania práva) – takéto spracúvanie sa namiesto toho riadi časťou 3 zákona o ochrane údajov z roku 2018, ako je to v prípade smernice (EÚ) 2016/680 podľa práva Európskej únie – ani na spracúvanie osobných údajov spravodajskými službami [Security Service (Bezpečnostná služba), Secret Intelligence Service (Tajná spravodajská služba) a Government Communications Headquarters (Vládne komunikačné ústredie)], na ktoré sa vzťahuje časť 4 zákona o ochrane údajov z roku 2018 ([33]).

(22) Územná pôsobnosť všeobecného nariadenia Spojeného kráľovstva o ochrane osobných údajov je opísaná v článku 3 všeobecného nariadenia Spojeného kráľovstva o ochrane osobných údajov ([34]) a zahŕňa spracúvanie osobných údajov (bez ohľadu na miesto spracúvania) v kontexte činností prevádzkarne prevádzkovateľa alebo sprostredkovateľa v Spojenom kráľovstve, ako aj spracúvanie osobných údajov dotknutých osôb, ktoré sa nachádzajú v Spojenom kráľovstve, ak spracovateľské činnosti súvisia s ponukou tovaru alebo služieb týmto dotknutým osobám alebo so sledovaním ich správania ([35]). Uvedené odráža prístup prijatý v článku 3 smernice (EÚ) 2016/679.

2.4. **Vymedzenie pojmov osobné údaje, prevádzkovateľ a sprostredkovateľ**

(23) Vymedzenie pojmov osobné údaje, prevádzkovateľ a sprostredkovateľ, ako aj vymedzenie pojmu pseudonymizácia stanovené v nariadení (EÚ) 2016/679 sa vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov ponechalo bez ďalších podstatných zmien ([36]). Navyše osobitné kategórie osobných údajov sú vymedzené v článku 9 ods. 1 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov rovnako ako v nariadení (EÚ) 2016/679 („odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby“). V § 205 zákona o ochrane údajov z roku 2018 sa uvádza vymedzenie pojmov „biometrické údaje“ ([37]), „údaje týkajúce sa zdravia“ ([38]) a „genetické údaje“ ([39]).

2.5. **Záruky, práva a povinnosti**

2.5.1. *Zákonnosť a spravodlivosť spracúvania*

(24) Osobné údaje by sa mali spracúvať zákonným a spravodlivým spôsobom.

(25) Zásady zákonnosti, spravodlivosti a transparentnosti a dôvody na zákonné spracúvanie sa zaručujú v práve Spojeného kráľovstva prostredníctvom článku 5 ods. 1 písm. a) a článku 6 ods. 1 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, ktoré sú totožné s príslušnými ustanoveniami nariadenia (EÚ) 2016/679 ([40]). § 8 zákona o ochrane údajov z roku 2018 dopĺňa článok 6 ods. 1 písm. e) uvedením, že spracúvanie osobných údajov podľa článku 6 ods. 1 písm. e) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov

([33]) Článok 2 ods. 2 písm. b) a c) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov.

([34]) Rovnaká územná pôsobnosť sa vzťahuje na spracúvanie osobných údajov podľa časti 2 zákona o ochrane údajov z roku 2018, ktorá dopĺňa všeobecné nariadenie Spojeného kráľovstva o ochrane údajov (§ 207 ods. 1A).

([35]) To najmä znamená, že zákon o ochrane údajov z roku 2018, a teda ani toto rozhodnutie, sa nevzťahuje na korunné dependencie Spojeného kráľovstva (Jersey, Guernsey a Ostrov Man) ani na jeho ostatné zámorské územia, ako sú napríklad Falklandské ostrovy a územie Gibraltáru.

([36]) Článok 4 ods. 1, 2, 5, 7 a 8 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov.

([37]) „Biometrické údaje“ sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov jednotlivca a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tohto jednotlivca, ako napríklad vyobrazenia tváre alebo daktyloskopické údaje.

([38]) „Údaje týkajúce sa zdravia“ sú osobné údaje týkajúce sa fyzického alebo duševného zdravia jednotlivca, vrátane údajov o poskytovaní služieb zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jeho zdravotnom stave.

([39]) „Genetické údaje“ sú osobné údaje týkajúce sa zdedených alebo nadobudnutých genetických charakteristických znakov jednotlivca, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tohto jednotlivca a ktoré vyplývajú najmä z analýzy biologickej vzorky daného jednotlivca.

([40]) Podľa článku 6 ods. 1 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov je spracúvanie zákonné iba vtedy a iba v tom rozsahu, keď: a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov na jeden alebo viaceré konkrétne účely; b) spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy; c) spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa; d) spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby; e) spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi; f) spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobou dieťa.

(nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci prevádzkovateľa) zahŕňa spracúvanie osobných údajov, ktoré je nevyhnutné na výkon spravodlivosti, výkon funkcie niektorej zo snemovní parlamentu, výkon funkcie zverenej osobe na základe zákonného ustanovenia alebo právnej normy, výkon funkcie koruny, ministra koruny alebo ministerstva alebo činnosť na podporu a propagáciu demokratickej angažovanosti.

(26) Pokiaľ ide o vyjadrenie súhlasu (jeden z dôvodov na zákonné spracúvanie), vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov sa ponechávajú aj nezmenené podmienky stanovené v článku 7 nariadenia (EÚ) 2016/679, čo znamená, že prevádzkovateľ musí vedieť preukázať, že dotknutá osoba vyjadrila súhlas, musí sa predložiť písomná žiadosť o súhlas, ktorá je jasne a jednoducho formulovaná, dotknutá osoba musí mať právo kedykoľvek odvolať súhlas a pri posudzovaní, či bol súhlas poskytnutý slobodne, by sa malo zohľadniť, či sa plnenie zmluvy podmieňuje súhlasom so spracúvaním osobných údajov, ktorý nie je na plnenie tejto zmluvy nevyhnutný. Okrem toho je podľa článku 8 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov v kontexte poskytovania služieb informačnej spoločnosti súhlas dieťaťa zákonný, len ak má dieťa aspoň 13 rokov. Patrí tak do vekovej skupiny stanovenej v článku 8 nariadenia (EÚ) 2016/679.

2.5.2. *Spracúvanie osobitných kategórií osobných údajov*

(27) Na spracúvanie „osobitných kategórií“ údajov by sa mali vzťahovať osobitné záruky.

(28) Všeobecné nariadenie Spojeného kráľovstva o ochrane údajov a zákon o ochrane údajov z roku 2018 obsahujú osobitné pravidlá týkajúce sa spracúvania osobitných kategórií osobných údajov, ktoré sú vymedzené v článku 9 ods. 1 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov rovnakým spôsobom ako v nariadení (EÚ) 2016/679 (pozri odôvodnenie 23). Podľa článku 9 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov je spracúvanie osobitných kategórií údajov v zásade zakázané, ak sa neuplatňuje osobitná výnimka.

(29) Týmito výnimkami (uvedenými v článku 9 ods. 2 a 3 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov) sa oproti výnimkám uvedeným v článku 9 ods. 2 a 3 nariadenia (EÚ) 2016/679 nezavádzajú podstatné zmeny. Pokiaľ dotknutá osoba nevyjadrila výslovný súhlas so spracúvaním týchto osobných údajov, spracúvanie osobitných kategórií osobných údajov je povolené len za osobitných a obmedzených okolností. Vo väčšine prípadov musí byť spracúvanie citlivých údajov nevyhnutné na konkrétny účel vymedzený v príslušnom ustanovení [pozri článok 9 ods. 2 písm. b), c), f), g), h), i) a j)].

(30) Okrem toho, ak sa výnimkou podľa článku 9 ods. 2 všeobecného nariadenia o ochrane údajov vyžaduje povolenie prostredníctvom právneho predpisu alebo odkazuje na verejný záujem, v § 10 zákona o ochrane údajov z roku 2018, ako aj v prílohe 1 k zákonu o ochrane údajov z roku 2018 sa ďalej stanovuje, že podmienky musia byť splnené, aby sa mohli uplatniť výnimky. Napríklad v prípade spracúvania citlivých údajov na ochranu „verejného zdravia“ [§ 9 ods. 2 písm. i) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov] sa v časti 1 bode 3 písm. b) prílohy 1 vyžaduje, aby sa takéto spracúvanie okrem toho, že sa musí overiť jeho nevyhnutnosť, vykonávalo „zdravotníckym pracovníkom alebo na jeho zodpovednosť“ alebo „inou osobou, ktorá má povinnosť zachovávať dôvernosť na základe zákonného ustanovenia alebo právnej normy“ vrátane povinnosti zachovávať dôvernosť podľa zavedeného common law.

(31) V prípade, že sa citlivé údaje spracúvajú z dôvodov významného verejného záujmu [(článok 9 ods. 2 písm. g) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov], v časti 2 prílohy 1 k zákonu o ochrane údajov z roku 2018 sa uvádza podrobný zoznam účelov, ktoré možno považovať za dôvody významného verejného záujmu, a stanovujú sa v nej dodatočné podmienky pre každý z týchto účelov. Za významný verejný záujem sa napríklad uznáva podpora rasovej a etnickej rozmanitosti na vyšších úrovniach organizácií. Spracúvanie citlivých údajov na tento konkrétny účel podlieha podrobným požiadavkám vrátane toho, aby sa spracúvanie vykonávalo ako súčasť procesu identifikácie vhodných jednotlivcov na vyššie pozície, bolo nevyhnutné na podporu rasovej a etnickej rozmanitosti a nebolo pravdepodobné, že spôsobí dotknutej osobe významnú škodu alebo významné ťažkosti.

(32) V § 11 ods. 1 zákona o ochrane údajov z roku 2018 sa stanovujú podmienky spracúvania osobných údajov za okolností uvedených v článku 9 ods. 3 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, ktorý súvisí s povinnosťou zachovávať mlčanlivosť. Patria sem aj okolnosti, za ktorých sa spracúvanie vykonáva zdravotníckym alebo sociálnym pracovníkom alebo na jeho zodpovednosť, alebo inou osobou, ktorá má na základe zákonného ustanovenia alebo právnej normy povinnosť zachovávať dôvernosť za daných okolností.

(33) Navyše si mnoho výnimiek uvedených v článku 9 ods. 2 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov vyžaduje vhodné a osobitné záruky, aby sa mohli uplatniť. V závislosti od povahy spracúvania a úrovne rizika pre práva a slobody dotknutých osôb sa v podmienkach spracúvania stanovených v prílohe 1 k zákonu o ochrane údajov z roku 2018 uvádzajú rôzne záruky. V prílohe 1 sa stanovujú podmienky každej príslušnej situácie spracúvania.

(34) V niektorých prípadoch sa zákonom o ochrane údajov z roku 2018 upravuje a obmedzuje typ citlivých údajov, ktoré sa môžu spracúvať v záujme konkrétneho právneho základu, ktorý sa má dodržať. Napríklad v bode 8 prílohy 1 sa povoľuje spracúvanie citlivých údajov na účel podpory rovnosti príležitostí alebo rovnakého zaobchádzania. Táto podmienka spracúvania sa môže uplatniť len vtedy, ak údaje odhaľujú rasový alebo etnický pôvod, náboženské alebo filozofické presvedčenie, sexuálnu orientáciu alebo ide o údaje týkajúce sa zdravia.

(35) V niektorých prípadoch sa zákonom o ochrane údajov z roku 2018 obmedzuje typ prevádzkovateľa, ktorý môže uplatniť podmienku spracúvania. Napríklad v bode 23 prílohy 1 sa stanovuje spracúvanie citlivých údajov vo vzťahu k odpovediam volených zástupcov určeným verejnosti. Táto podmienka spracúvania sa môže uplatniť len vtedy, ak je prevádzkovateľ voleným zástupcom alebo koná na základe jeho poverenia.

(36) V niektorých prípadoch sa v zákone o ochrane údajov z roku 2018 stanovujú obmedzenia kategórií dotknutých osôb na účely podmienky spracúvania, ktorá sa má uplatniť. Napríklad v bode 21 prílohy 1 sa upravuje spracúvanie citlivých údajov v súvislosti so zamestnaneckými dôchodkovými systémami. Táto podmienka sa môže uplatniť len vtedy, ak je daná dotknutá osoba súrodencom, rodičom, starým rodičom alebo prastarým rodičom člena systému.

(37) Okrem toho, ak sa vychádza z výnimiek uvedených v článku 9 ods. 2 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, ktoré sú bližšie špecifikované v § 10 zákona o ochrane údajov z roku 2018, ako aj v prílohe 1 k zákonu o ochrane údajov z roku 2018, od prevádzkovateľa sa vo väčšine prípadov vyžaduje, aby vypracoval „riadny dokument stanovujúci politiku spracúvania“. Musia sa v ňom uviesť postupy prevádzkovateľa na zabezpečenie dodržiavania zásad stanovených v článku 5 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov. Musia sa v ňom stanoviť aj politiky uchovávania a vymazávania, pričom sa uvedie pravdepodobné obdobie uchovávania. Prevádzkovatelia musia tento dokument podľa potreby preskúmať a aktualizovať. Prevádzkovateľ musí dokument stanovujúci politiku uchovávať šesť mesiacov po ukončení spracúvania a na požiadanie ho musí sprístupniť Komisárovi pre informácie ([41]).

(38) Podľa bodu 41 prílohy 1 k zákonu o ochrane údajov z roku 2018 dokument stanovujúci politiku musí vždy sprevádzať rozšírený záznam o spracúvaní. V tomto zázname musia byť poznačené záväzky zahrnuté v dokumente stanovujúcom politiku, t. j. či sa údaje mažú alebo uchovávajú v súlade s politikami. Ak sa politiky nedodržiavajú, v logu musia byť zaznamenané dôvody. V zázname sa musí takisto uviesť, ako spracúvanie spĺňa ustanovenia článku 6 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov (zákonnosť spracúvania) a osobitnú podmienku uvedenú v prílohe 1 k zákonu o ochrane údajov z roku 2018, z ktorej vychádza.

(39) Napokon sa vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov rovnako ako v nariadení (EÚ) 2016/679 stanovujú aj všeobecné záruky pre určité spracovateľské operácie osobitných kategórií údajov. Článkom 35 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sa vyžaduje posúdenie vplyvu na ochranu údajov, ak sa spracúvajú osobitné kategórie údajov vo veľkom rozsahu. Prevádzkovateľ alebo sprostredkovateľ musí podľa článku 37 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov určiť zodpovednú osobu, ak spracúvanie osobitných kategórií údajov vo veľkom rozsahu predstavuje jeho hlavné činnosti.

(40) Pokiaľ ide o osobné údaje týkajúce sa uznania viny za trestné činy a priestupky, článok 10 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov je totožný s článkom 10 nariadenia (EÚ) 2016/679. Umožňuje sa ním spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky len pod kontrolou orgánu verejnej moci alebo ak je spracúvanie povolené vnútroštátnym právom poskytujúcim primerané záruky ochrany práv a slobôd dotknutých osôb.

(41) Ak sa spracúvanie údajov týkajúcich sa uznania viny za trestné činy a priestupky nevykonáva pod kontrolou orgánu verejnej moci, v § 10 ods. 5 zákona o ochrane údajov z roku 2018 sa stanovuje, že takéto spracúvanie sa môže uskutočniť len na konkrétne účely/v osobitných situáciách stanovených v častiach 1, 2 a 3 prílohy 1 k zákonu o ochrane údajov z roku 2018 a podlieha osobitným požiadavkám, ktoré sú stanovené na každý z týchto účelov/pre každú z týchto situácií. Napríklad neziskové subjekty môžu spracúvať údaje týkajúce sa uznania viny za trestné činy, ak spracúvanie vykonáva a) v rámci svojej zákonnej činnosti s primeranými zárukami nadácia, združenie alebo akýkoľvek iný neziskový subjekt s politickým, filozofickým, náboženským alebo odborárskym zameraním a b) pod podmienkou, že i) spracúvanie sa týka výlučne členov alebo bývalých členov subjektu, alebo osôb, ktoré s ním majú pravidelný kontakt v súvislosti s jeho cieľmi, a že ii) bez súhlasu dotknutej osoby sa osobné údaje neposkytnú mimo tohto subjektu.

([41]) Body 38 až 40 prílohy 1 k zákonu o ochrane údajov z roku 2018.

(42) Okrem toho sa v časti 3 prílohy 1 k zákonu o ochrane údajov z roku 2018 stanovujú ďalšie okolnosti, za ktorých sa môžu použiť údaje týkajúce sa uznania viny za trestné činy, ktoré zodpovedajú právnym dôvodom na spracúvanie citlivých údajov uvedeným v článku 9 ods. 2 nariadenia (EÚ) 2016/679 a všeobecného nariadenia Spojeného kráľovstva o ochrane údajov (napr. súhlas dotknutej osoby, životne dôležité záujmy jednotlivca, ak dotknutá osoba nie je právne alebo fyzicky spôsobilá vyjadriť svoj súhlas, ak údaje už preukázateľne zverejnila dotknutá osoba, ak je spracúvanie nevyhnutné na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov atď.).

2.5.3. *Obmedzenie účelu, správnosť, minimalizácia údajov, minimalizácia uchovávania a bezpečnosť údajov*

(43) Osobné údaje by sa mali spracúvať na konkrétny účel a následne by sa mali používať len pokiaľ to nie je nezlučiteľné s daným účelom spracúvania.

(44) Táto zásada sa stanovuje v článku 5 ods. 1 písm. b) nariadenia (EÚ) 2016/679 a v článku 5 ods. 1 písm. b) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sa ponecháva bez zmien. Podmienky ďalšieho zlučiteľného spracúvania podľa článku 6 ods. 4 nariadenia (EÚ) 2016/679 sa takisto ponechávajú v článku 6 ods. 4 písm. a) až e) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov bez podstatných zmien.

(45) Údaje by takisto mali byť správne a v prípade potreby sa mali aktualizovať. Mali by byť aj primerané, relevantné a nie nadmerné vzhľadom na účely, na ktoré sa spracúvajú, a v zásade by sa nemali uchovávať dlhšie, ako je nevyhnutné na účely, na ktoré sa osobné údaje spracúvajú.

(46) Tieto zásady minimalizácie údajov, správnosti a minimalizácie uchovávania sú stanovené v článku 5 ods. 1 písm. c) až e) nariadenia (EÚ) 2016/679 a v článku 5 ods. 1 písm. c) až e) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sa ponechávajú bez zmien.

(47) Osobné údaje by sa navyše mali spracúvať spôsobom, ktorým sa zaručí ich bezpečnosť vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením. Na tento účel by podnikateľské subjekty mali prijať vhodné technické alebo organizačné opatrenia na ochranu osobných údajov pred možnými hrozbami. Tieto opatrenia by sa mali posudzovať s prihliadnutím na stav techniky a súvisiace náklady.

(48) Bezpečnosť údajov sa zakotvuje v práve Spojeného kráľovstva prostredníctvom zásady integrity a dôvernosti uvedenej v článku 5 ods. 1 písm. f) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov a v článku 32 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, ktorý sa týka bezpečnosti spracúvania. Tieto ustanovenia sú totožné s príslušnými ustanoveniami nariadenia (EÚ) 2016/679. Navyše za rovnakých podmienok, ako sú podmienky stanovené v článkoch 33 a 34 nariadenia (EÚ) 2016/679, sa vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov vyžaduje oznámenie porušenia ochrany osobných údajov dozornému orgánu (článok 33 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov) a oznámenie porušenia ochrany osobných údajov dotknutej osobe (článok 34 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov).

2.5.4. *Transparentnosť*

(49) Dotknuté osoby by mali byť informované o hlavných znakoch spracúvania ich osobných údajov.

(50) Zabezpečuje sa to článkami 13 a 14 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, v ktorých sa okrem všeobecnej zásady transparentnosti stanovujú pravidlá o informáciách, ktoré sa majú poskytnúť dotknutej osobe ([42]). Vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov sa neuvádzajú podstatné zmeny týchto pravidiel oproti príslušným článkom nariadenia (EÚ) 2016/679. Požiadavky na transparentnosť uvedené v týchto článkoch však rovnako ako v nariadení (EÚ) 2016/679 podliehajú niekoľkým výnimkám stanoveným v zákone o ochrane údajov z roku 2018 (pozri odôvodnenia 55 až 72).

([42]) Odkazy na rozhodnutia Komisie o primeranosti v článku 13 ods. 1 písm. f) a článku 14 ods. 1 písm. f) sa nahradili odkazmi na rovnocenný nástroj Spojeného kráľovstva, t. j. právne predpisy o primeranosti podľa zákona o ochrane údajov z roku 2018. V článku 14 ods. 5 písm. c) až d) sa navyše nahradili odkazy na právo EÚ alebo právo členského štátu odkazom na vnútroštátne právo [Spojené kráľovstvo ako príklady takéhoto vnútroštátneho práva, ktoré môže patriť do pôsobnosti článku 14 ods. 5 písm. c), uvádza § 7 zákona o obchodníkoch s kovovým šrotom z roku 2013 (Scrap Metal Dealers Act), v ktorom sa stanovujú pravidlá pre register povolení obchodovať s kovovým šrotom, alebo časť 35 zákona o spoločnostiach z roku 2006 (Companies Act), v ktorej sa stanovujú pravidlá pre register spoločností]. Podobne by príklad vnútroštátneho práva, ktorý môže patriť do pôsobnosti článku 14 ods. 5 písm. d), mohol zahŕňať právne predpisy, v ktorých sa stanovujú pravidlá zachovania dôvernosti údajov v zamestnaní, alebo povinnosti premietnuté v pracovných zmluvách, alebo povinnosť zachovávať dôvernosť podľa common law (napríklad spracúvanie osobných údajov zdravotníckymi pracovníkmi, pracovníkmi v oblasti ľudských zdrojov, sociálnymi pracovníkmi).

2.5.5. *Individuálne práva*

(51) Dotknuté osoby by mali mať určité práva, ktoré možno uplatniť voči prevádzkovateľovi alebo sprostredkovateľovi, najmä právo na prístup k údajom, právo namietať proti spracúvaniu a právo na opravu a vymazanie údajov. Tieto práva môžu zároveň podliehať obmedzeniam, pokiaľ sú tieto obmedzenia nevyhnutné a primerané vzhľadom na zabezpečenie verejnej bezpečnosti alebo iných dôležitých cieľov všeobecného verejného záujmu.

2.5.5.1. Hmotné práva

(52) Vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov sa jednotlivcom priznávajú rovnaké vymáhateľné práva ako v nariadení (EÚ) 2016/679. Ustanovenia, v ktorých sa uvádzajú práva jednotlivcov, sa vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov ponechali bez podstatných úprav.

(53) Medzi tieto práva patrí právo dotknutej osoby na prístup k údajom (článok 15 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov), právo na opravu (článok 16 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov), právo na vymazanie (článok 17 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov), právo na obmedzenie spracúvania (článok 18 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov), oznamovacia povinnosť v súvislosti s opravou alebo vymazaním osobných údajov alebo obmedzením spracúvania (článok 19 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov), právo na prenosnosť údajov (článok 20 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov) a právo namietať (článok 21 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov) ([43]). Právo namietať zahŕňa aj právo dotknutej osoby namietať proti spracúvaniu osobných údajov na účel priameho marketingu, ako sa stanovuje v článku 21 ods. 2 a 3 nariadenia (EÚ) 2016/679. Okrem toho podľa § 122 zákona o ochrane údajov z roku 2018 Komisár pre informácie musí vypracovať kódex postupov vo vzťahu k vykonávaniu priameho marketingu v súlade s požiadavkami právnych predpisov o ochrane údajov [a právnych predpisov o súkromí a elektronických komunikáciách (podľa smernice ES) z roku 2003] a ďalšie takéto usmernenia na podporu osvedčených postupov v priamom marketingu, ktoré Komisár považuje za primerané. Úrad Komisára pre informácie v súčasnosti vypracúva kódex v oblasti priameho marketingu ([44]).

(54) Právo dotknutej osoby, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú, stanovené v článku 22 všeobecného nariadenia o ochrane údajov sa takisto ponechalo vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov bez podstatných zmien. V § 14 zákona o ochrane údajov z roku 2018 sa však dopĺňa nový § 3A, v ktorom sa stanovujú záruky pre práva, slobody a oprávnené záujmy dotknutých osôb, ak sa spracúvanie vykonáva podľa článku 22 ods. 2 písm. b) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov. Uplatňuje sa to len vtedy, ak je základom takéhoto rozhodnutia povolenie alebo požiadavka podľa práva Spojeného kráľovstva, a neuplatňuje sa, ak je rozhodnutie nevyhnutné podľa zmluvy alebo je prijaté s výslovným súhlasom dotknutej osoby. Ak sa § 14 zákona o ochrane údajov z roku 2018 uplatňuje, prevádzkovateľ musí čo najskôr písomne oznámiť dotknutej osobe, že sa prijalo rozhodnutie založené výlučne na automatizovanom spracúvaní. Dotknutá osoba má právo požadovať, aby prevádzkovateľ do jedného mesiaca od prijatia oznámenia prehodnotil rozhodnutie, alebo aby prijal nové rozhodnutie, ktoré nie je založené výlučne na automatizovanom spracúvaní. Pokiaľ ide o automatizované rozhodovanie, minister je oprávnený prijať ďalšie záruky. Táto právomoc sa ešte neuplatnila.

2.5.5.2. Obmedzenia individuálnych práv a ďalšie ustanovenia

(55) V zákone o ochrane údajov z roku 2018 sa stanovuje niekoľko obmedzení individuálnych práv, ktoré patria do rámca pôsobnosti článku 23 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov. V tomto rámci sa nezavádzajú žiadne obmedzenia týkajúce sa práva namietať proti priamemu marketingu, ako sa stanovuje v článku 21 ods. 2 a 3 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, ani práva nepodliehať automatizovanému rozhodovaniu, ako sa stanovuje v článku 22 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov.

(56) Obmedzenia sú podrobne uvedené v prílohách 2 až 4 k zákonu o ochrane údajov z roku 2018. Orgány Spojeného kráľovstva vysvetlili, že sa riadia dvomi zásadami: zásada špecifickosti (zavedenie podrobného prístupu, rozdelenie všeobecných obmedzení na viaceré konkrétnejšie ustanovenia) a zásada podmienenosti (každé ustanovenie je doplnené zárukami vo forme obmedzení alebo podmienok s cieľom zabrániť zneužitiu) ([45]).

([43]) V článku 17 ods. 1 písm. e) a článku 17 ods. 3 písm. b) sa nahradili odkazy na právo EÚ alebo právo členského štátu odkazom na vnútroštátne právo {Spojené kráľovstvo ako príklady takéhoto vnútroštátneho práva podľa článku 17 ods. 1 písm. e) uvádza právne predpisy o vzdelávaní (informácie o žiakoch) (Anglicko) z roku 2006 [Education (Pupil Information) (England) Regulations], ktorými sa vyžaduje, aby sa vymazali mená žiakov zo školských registrov po ich odchode zo školy, alebo zákon o zdravotnej starostlivosti z roku 1983 (Medical Act), § 34F, ktorým sa stanovujú pravidlá odstránenia mien z registra všeobecných lekárov alebo registra špecializovaných lekárov}.

([44]) Návrh kódexu postupov sa nachádza na tomto odkaze: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf.

([45]) Vysvetľujúci rámec Spojeného kráľovstva pre diskusiu o primeranosti, oddiel E s názvom „Obmedzenia“, s. 1, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

(57) Obmedzenia uvedené v článku 23 ods. 1 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sú navrhnuté tak, aby sa zabezpečilo ich uplatňovanie iba za špecifických okolností, ak sú nevyhnutné v demokratickej spoločnosti a primerané oprávnenému cieľu, ktorý sledujú. Okrem toho sa v súlade s ustálenou judikatúrou o výklade obmedzení výnimka z režimu ochrany údajov môže uplatniť len v každom konkrétnom prípade, keď je to nevyhnutné a primerané ([46]). Vyžaduje sa, aby overenie nevyhnutnosti bolo „prísne s požiadavkou, aby akýkoľvek zásah do práv dotknutej osoby bol primeraný závažnosti ohrozenia verejného záujmu. Jeho vykonanie si preto vyžaduje klasickú analýzu proporcionality ([47])".

(58) Ciele sledované týmito obmedzeniami zodpovedajú cieľom uvedeným v článku 23 nariadenia (EÚ) 2016/679 s výnimkou obmedzení národnej bezpečnosti a obrany, ktoré sú namiesto toho upravené § 26 zákona o ochrane údajov z roku 2018, ale podliehajú rovnakým požiadavkám nevyhnutnosti a proporcionality (pozri odôvodnenia 63 až 66).

(59) Niektoré z obmedzení, napríklad obmedzenia súvisiace s predchádzaním trestnej činnosti alebo jej odhaľovaním, so zadržaním alebo s trestným stíhaním páchateľov a posúdením alebo výberom dane alebo cla ([48]), umožňujú obmedziť všetky individuálne práva a povinnosti týkajúce sa transparentnosti (s výnimkou práv podľa článku 21 ods. 2 a článku 22). Rozsah ďalších obmedzení sa vzťahuje na povinnosti týkajúce sa transparentnosti a prístupové práva, ako sú obmedzenia súvisiace s dôvernosťou komunikácie medzi advokátom a jeho klientom ([49]), právom na oslobodenie od povinnosti poskytovať informácie, ktoré by viedli k výpovedi vo vlastný neprospech ([50]), a podnikovým financovaním, najmä s predchádzaním obchodovaniu s využitím dôverných informácií ([51]). Niekoľko obmedzení umožňuje obmedziť povinnosť prevádzkovateľa oznámiť porušenie ochrany údajov dotknutej osobe a zásady obmedzenia účelu a zákonnosti, spravodlivosti a transparentnosti spracúvania ([52]).

(60) Niektoré obmedzenia sa automaticky uplatňujú „v plnej miere" na určité typy spracúvania osobných údajov (napríklad uplatňovanie povinností týkajúcich sa transparentnosti a individuálnych práv sa vylučuje, ak sa osobné údaje spracúvajú na účely posúdenia vhodnosti osoby na funkciu sudcu alebo osobné údaje spracúva súd, tribunál alebo jednotlivec pri výkone súdnej právomoci).

(61) Vo väčšine prípadov sa však v príslušnom bode prílohy 2 k zákonu o ochrane údajov z roku 2018 uvádza, že obmedzenie sa uplatňuje len vtedy, ak (a v takom rozsahu, v akom) by uplatňovanie ustanovení „mohlo poškodiť" oprávnený cieľ sledovaný týmto obmedzením: napríklad uvedené ustanovenia všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sa nevzťahujú na osobné údaje spracúvané na účely predchádzania trestnej činnosti alebo jej odhaľovania, zadržania alebo trestného stíhania páchateľov, posúdenia alebo výberu dane alebo cla „v rozsahu, v akom by uplatňovanie týchto ustanovení mohlo poškodiť" ktorúkoľvek z uvedených činností ([53]).

(62) Súdy Spojeného kráľovstva konzistentne vykladajú zásadu „by mohlo poškodiť" ako „veľmi vysokú a vážnu pravdepodobnosť poškodenia identifikovaných verejných záujmov ([54])". Obmedzenie, na ktoré sa vzťahuje overenie kritéria poškodenia, preto možno uplatniť len vtedy a v takom rozsahu, pokiaľ existuje veľmi vysoká a vážna pravdepodobnosť, že by priznanie určitého práva poškodilo príslušný verejný záujem. Prevádzkovateľ je zodpovedný za posúdenie jednotlivých prípadov, či sú tieto podmienky splnené ([55]).

(63) Okrem obmedzení uvedených v prílohe 2 k zákonu o ochrane údajov z roku 2018 je v § 26 toho istého zákona uvedená výnimka, ktorá sa môže uplatňovať na určité ustanovenia všeobecného nariadenia Spojeného kráľovstva o ochrane údajov a zákona o ochrane údajov z roku 2018, ak sa tá výnimka vyžaduje na účely ochrany národnej bezpečnosti alebo na účely obrany. Táto výnimka sa vzťahuje na zásady ochrany údajov (okrem zásady zákonnosti), na povinnosti týkajúce sa transparentnosti, práva dotknutej osoby, povinnosť oznámiť porušenie ochrany údajov, pravidlá pre medzinárodné prenosy, niektoré povinnosti a právomoci Komisára pre informácie a na pravidlá pre prostriedky nápravy, záväzky a sankcie s výnimkou ustanovenia o všeobecných podmienkach ukladania správnych

([46]) Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin), body 40 a 41.
([47]) Guriev/Community Safety Development (United Kingdom) Ltd [2016] EWHC 643 (QB), bod 43. V tejto súvislosti pozri aj Lin/Commissioner of the Police for the Metropolis [2015] EWHC 2484 (QB), bod 80.
([48]) Bod 2 prílohy 2 k zákonu o ochrane údajov z roku 2018.
([49]) Bod 19 prílohy 2 k zákonu o ochrane údajov z roku 2018.
([50]) Bod 20 prílohy 2 k zákonu o ochrane údajov z roku 2018.
([51]) Bod 21 prílohy 2 k zákonu o ochrane údajov z roku 2018.
([52]) Napríklad obmedzenia práva na oznámenie porušenia ochrany údajov sú možné len v súvislosti s trestnou činnosťou a daňami (bod 2 prílohy 2 k zákonu o ochrane údajov z roku 2018), parlamentnými výsadami (bod 13 prílohy 2 k zákonu o ochrane údajov z roku 2018) a so spracúvaním na žurnalistické, akademické, umelecké a literárne účely (bod 26 prílohy 2 k zákonu o ochrane údajov z roku 2018).
([53]) Bod 2 prílohy 2 k zákonu o ochrane údajov z roku 2018.
([54]) R (Lord)/Secretary of State for the Home Department [2003] EWHC 2073 (Admin), bod 100 a Guriev/Community Safety Development (United Kingdom) Ltd [2016] EWHC 643 (QB), bod 43.
([55]) Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor, bod 31.

pokút, ktoré sú uvedené v článku 83 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, a ustanovenia o sankciách v článku 84 toho istého nariadenia. Okrem toho sa v § 28 zákona o ochrane údajov z roku 2018 upravuje uplatnenie článku 9 ods. 1 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, aby sa umožnilo spracúvanie osobitných kategórií údajov podľa tohto článku, pokiaľ sa spracúvanie vykonáva na účely ochrany národnej bezpečnosti alebo na účely obrany a s primeranými zárukami v súvislosti s právami a slobodami dotknutých osôb ([56]).

(64) Výnimka sa môže uplatňovať, iba ak sa to vyžaduje na účely ochrany národnej bezpečnosti alebo obrany. Keďže sa to týka aj ďalších výnimiek, ktoré umožňuje zákon o ochrane údajov z roku 2018, prevádzkovateľ ich musí posudzovať a uplatňovať podľa jednotlivých prípadov. Okrem toho každé uplatnenie výnimky musí byť v súlade s normami v oblasti ľudských práv (na základe zákona o ľudských právach z roku 1998), podľa ktorých akýkoľvek zásah do práv na súkromie by mal byť v demokratickej spoločnosti nevyhnutný a primeraný ([57]).

(65) Tento výklad výnimky potvrdil Komisár pre informácie, ktorý vydal podrobné usmernenie k uplatňovaniu výnimky týkajúcej sa národnej bezpečnosti a obrany, pričom objasnil, že prevádzkovateľ ju musí posudzovať a uplatňovať podľa jednotlivých prípadov ([58]). V usmernení sa zdôrazňuje najmä to, že „toto nie je paušálna výnimka“ a na jej uplatnenie „nestačí, aby sa údaje spracúvali na účely národnej bezpečnosti“. Na druhej strane prevádzkovateľ, ktorý sa na ňu odvoláva, musí „preukázať, že existuje skutočná možnosť nepriaznivých dôsledkov na národnú bezpečnosť“, a v prípade potreby sa od prevádzkovateľa očakáva, že „poskytne [Komisárovi pre informácie] dôkaz, prečo túto výnimku uplatnil“. Usmernenie obsahuje kontrolný zoznam a viacero príkladov na ďalšie objasnenie podmienok, za ktorých je možné odvolať sa na túto výnimku.

(66) Skutočnosť, že údaje sa spracúvajú na účely národnej bezpečnosti alebo obrany, sama osebe nepostačuje na uplatnenie výnimky. Prevádzkovateľ musí posúdiť skutočné dôsledky pre národnú bezpečnosť, ak to musí byť v súlade s konkrétnym ustanovením o ochrane údajov. Výnimka sa môže uplatniť iba na tie konkrétne ustanovenia, o ktorých sa zistilo, že predstavujú riziko a musia sa uplatňovať tak obmedzene, ako je to možné ([59]).

(67) Tento prístup potvrdil tribunál pre informácie (Information Tribunal) ([60]). Vo veci Baker/Secretary of State for the Home Department (ďalej len „Baker/Secretary of State“) rozhodol, že bolo nezákonné uplatniť výnimku týkajúcu sa národnej bezpečnosti ako paušálnu výnimku pre žiadosti o prístup, ktoré dostanú spravodajské služby. Namiesto toho sa výnimka mala uplatňovať v jednotlivých prípadoch, pričom sa mala preskúmať podstata každej žiadosti, a to aj s ohľadom na práva jednotlivcov na rešpektovanie ich súkromného života ([61]).

([56]) Podľa informácií poskytnutých orgánmi Spojeného kráľovstva, ak sa spracúvanie vykonáva v kontexte národnej bezpečnosti, prevádzkovatelia budú pri spracúvaní spravidla uplatňovať posilnené záruky a bezpečnostné opatrenia odrážajúce citlivý charakter spracúvania. Ktoré záruky sú primerané, bude závisieť od toho, aké riziká predstavuje vykonávané spracúvanie. Mohlo by to zahŕňať obmedzenia prístupu k údajom, aby k nim mali prístup iba oprávnené osoby s primeranou bezpečnostnou previerkou, prísne obmedzenia, pokiaľ ide o poskytovanie údajov, a vysoký štandard bezpečnosti uplatňovaný na postupy uchovávania údajov a zaobchádzania s nimi.

([57]) Pozri aj veci Guriev/Community Safety Development (United Kingdom) Ltd [2016] EWHC 643 (QB), bod 45; Lin/Commissioner of the Police for the Metropolis [2015] EWHC 2484 (QB), bod 80.

([58]) Pozri usmernenie Komisára pre informácie o výnimke týkajúcej sa národnej bezpečnosti a obrany, ktoré je k dispozícii na tomto odkaze: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/.

([59]) Podľa príkladu poskytnutého orgánmi Spojeného kráľovstva, ak podozrievaný terorista, ktorého aktívne vyšetruje Bezpečnostná služba (MI5), požiada ministerstvo vnútra o prístup (napríklad preto, že sa zapojil do diskusie s ministerstvom vnútra o otázkach imigrácie), bolo by nevyhnutné zabrániť poskytnutiu akýchkoľvek údajov, ktoré mohla MI5 zdieľať s ministerstvom vnútra a ktoré sa týkajú prebiehajúceho vyšetrovania, čo by mohlo ohroziť citlivé zdroje, metódy alebo techniky a/alebo viesť k zvýšeniu hrozby, ktorú predstavuje daný jednotlivec. Za takých okolností je pravdepodobné, že by sa splnili požiadavky na uplatnenie výnimky podľa § 26 a bola by potrebná výnimka z poskytnutia informácií, aby sa zaručila národná bezpečnosť. Ak by však ministerstvo vnútra malo k dispozícii aj osobné údaje jednotlivca, ktoré by nesúviseli s vyšetrovaním MI5 a mohli by sa poskytnúť bez rizika škôd pre národnú bezpečnosť, výnimka týkajúca sa národnej bezpečnosti by sa nemohla uplatniť pri posudzovaní poskytnutia informácií danému jednotlivcovi. Komisár pre informácie v súčasnosti pripravuje usmernenie, ako by prevádzkovatelia mali pristupovať k využívaniu výnimky podľa § 26. Očakáva sa, že toto usmernenie bude uverejnené do konca marca 2021.

([60]) Tribunál pre informácie bol zriadený na posudzovanie odvolaní týkajúcich sa ochrany údajov podľa zákona o ochrane údajov z roku 1984. V roku 2010 sa tribunál pre informácie stal v rámci reformy britského systému tribunálov súčasťou Všeobecnej regulačnej komory (General Regulatory Chamber) tribunálu prvého stupňa (First Tier Tribunal).

([61]) Pozri vec Baker/Secretary of State for the Home Department [2001] UKIT NSA2 (Baker/Secretary of State).

2.5.6. *Obmedzenia pre osobné údaje spracúvané na žurnalistické, umelecké, akademické a literárne účely, ako aj na archiváciu a výskum*

(68) V článku 85 ods. 2 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sa umožňuje vyňatie osobných údajov spracúvaných na žurnalistické, umelecké, akademické a literárne účely z viacerých ustanovení uvedeného nariadenia. V časti 5 prílohy 2 k zákonu o ochrane údajov z roku 2018 sú stanovené výnimky pre spracúvanie údajov na tieto účely. Možné sú výnimky zo zásad ochrany údajov (okrem zásady integrity a dôvernosti), z právneho základu pre spracúvanie údajov (vrátane osobitných kategórií údajov a údajov týkajúcich sa uznania viny za trestné činy atď.), podmienok vyjadrenia súhlasu, povinností týkajúcich sa transparentnosti, práv dotknutej osoby, povinnosti oznámiť porušenie ochrany údajov, a požiadavky na konzultáciu s Komisárom pre informácie pred začatím vysokorizikového spracúvania údajov a pravidiel pre medzinárodné prenosy ([62]). V tejto súvislosti sa všeobecné nariadenie Spojeného kráľovstva o ochrane údajov neodchyľuje zásadným spôsobom od nariadenia (EÚ) 2016/679, v ktorého článku 85 sa takisto stanovuje možnosť vyňať spracúvanie údajov vykonávané na žurnalistické účely alebo na účely akademickej, umeleckej alebo literárnej tvorby z viacerých požiadaviek stanovených v nariadení (EÚ) 2016/679. Ustanovenia v zákone o ochrane údajov z roku 2018, najmä v časti 5 prílohy 2, sú zlučiteľné so všeobecným nariadením Spojeného kráľovstva o ochrane údajov.

(69) Základné vyváženie, ktoré sa má vykonať podľa článku 85 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, sa týka zistenia, či výnimka z pravidiel ochrany údajov uvedená v odôvodnení 68 je „nevyhnutná na zosúladenie práva na ochranu osobných údajov so slobodou prejavu a právom na informácie“ ([63]). Podľa bodu 26 ods. 2 a 3 prílohy 2 k zákonu o ochrane údajov z roku 2018 uplatňuje Spojené kráľovstvo kritérium „odôvodneného presvedčenia“ s cieľom dosiahnuť toto vyváženie. Aby bola výnimka odôvodnená, musí byť prevádzkovateľ odôvodnene presvedčený, že i) toto zverejnenie je vo verejnom záujme a ii) uplatnenie príslušného ustanovenia všeobecného nariadenia o ochrane údajov by bolo nezlučiteľné so žurnalistickými, s akademickými, umeleckými a literárnymi účelmi. Ako potvrdzuje judikatúra ([64]), kritérium „odôvodneného presvedčenia“ má subjektívnu a objektívnu zložku: je nedostatočné, aby prevádzkovateľ preukázal, že on sám je presvedčený o nemožnosti dosiahnuť súlad. Jeho presvedčenie musí byť odôvodnené, teda aby o tom mohol byť presvedčený aj rozumný človek, ktorý pozná príslušné fakty. Prevádzkovateľ musí preto pri vytváraní svojho presvedčenia vykonať hĺbkovú analýzu, aby mohol preukázať jeho odôvodnenosť. Podľa vysvetlení, ktoré poskytli orgány Spojeného kráľovstva, overenie kritéria „odôvodneného presvedčenia“ sa musí vykonať pri každej posudzovanej výnimke ([65]). Ak sú podmienky splnené, výnimka sa považuje za nevyhnutnú a primeranú podľa právneho poriadku Spojeného kráľovstva.

(70) Podľa § 124 zákona o ochrane údajov z roku 2018 má Komisár pre informácie vypracovať Kódex postupov pre ochranu údajov a žurnalistiku. Práca na tomto kódexe prebieha. Na základe zákona o ochrane údajov z roku 1998 bolo už vydané usmernenie pre túto oblasť, v ktorom sa predovšetkým zdôrazňuje, že aby bolo možné uplatniť danú výnimku, nestačí len vyhlásiť, že súlad s príslušným ustanovením by bol prekážkou pre činnosť žurnalistov, ale musí sa uviesť jednoznačný argument, že príslušné ustanovenie predstavuje prekážku

([62]) Pozri článok 85 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov a časť 5 bod 26 ods. 9 prílohy 2 k zákonu o ochrane údajov z roku 2018.

([63]) V súlade s časťou 5 bodom 26 ods. 2 prílohy 2 k zákonu o ochrane údajov z roku 2018 sa výnimka uplatňuje pri spracúvaní osobných údajov vykonávanom na osobitné účely (žurnalistické účely, akademické účely, umelecké účely a literárne účely), ak sa spracúvanie vykonáva s cieľom zverejnenia žurnalistického, akademického, umeleckého alebo literárneho materiálu a prevádzkovateľ je odôvodnene presvedčený, že uverejnenie tohto materiálu by bolo vo verejnom záujme. Pri rozhodovaní, či by uverejnenie bolo vo verejnom záujme, musí prevádzkovateľ zohľadniť osobitnú dôležitosť verejného záujmu, pokiaľ ide o slobodu prejavu a právo na informácie. Prevádzkovateľ musí okrem toho brať ohľad na kódexy postupov alebo usmernenia týkajúce sa daného uverejňovania (redakčné usmernenia BBC, kódex vysielania telekomunikačného regulačného orgánu Ofcom a kódex postupov vydavateľov). Pre uplatnenie výnimky musí byť prevádzkovateľ navyše odôvodnene presvedčený, že súlad s príslušným ustanovením by bol nezlučiteľný s osobitnými účelmi (bod 26 ods. 3 prílohy 2 k zákonu o ochrane údajov z roku 2018).

([64]) Rozsudok vo veci NT1/Google [2018] EWHC 799 (QB), bod 102 sa týkal diskusie, či bol prevádzkovateľ odôvodnene presvedčený, že uverejnenie je vo verejnom záujme a že súlad s príslušnými ustanoveniami bo nezlučiteľný s osobitnými účelmi. Súd uviedol, že § 32 ods. 1 písm. b) a c) zákona o ochrane údajov z roku 1998 má subjektívnu a objektívnu zložku: prevádzkovateľ musí preukázať svoje presvedčenie, že uverejnenie bude vo verejnom záujme a že toto presvedčenie je objektívne odôvodnené, musí preukázať subjektívne presvedčenie, že súlad s ustanovením, z ktorého sa požaduje výnimka, bude nezlučiteľný s danými osobitnými účelmi.

([65]) Príklad, ako sa uplatňuje kritérium „odôvodneného presvedčenia“, je uvedený v rozhodnutí Komisára pre informácie o uložení pokuty produkčnej spoločnosti True Visions Productions podľa zákona o ochrane údajov z roku 1998. Komisár pre informácie uznal subjektívne presvedčenie prevádzkovateľa médií, že súlad s prvou zásadou ochrany údajov (spravodlivosť a zákonnosť) je nezlučiteľný so žurnalistickými účelmi. Komisár pre informácie však neuznal, že toto presvedčenie je objektívne odôvodnené. Rozhodnutie Komisára pre informácie je dostupné na tomto odkaze: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf.

pre zodpovednú žurnalistiku ([66]). Usmernenie týkajúce sa uplatňovania kritéria verejného záujmu a vyvažovania verejného záujmu so záujmom jednotlivca o súkromie uverejnil aj telekomunikačný regulačný orgán Spojeného kráľovstva Ofcom a spoločnosť BBC v rámci svojich redakčných usmernení ([67]). V usmerneniach sa uvádzajú najmä príklady informácií, ktoré sa môžu považovať za informácie vo verejnom záujme, a vysvetľuje sa potreba schopnosti preukázať, že za konkrétnych okolností daného prípadu verejný záujem prevažuje nad právami na súkromie.

(71) Podobne, ako je to umožnené v článku 89 všeobecného nariadenia o ochrane údajov, aj osobné údaje, ktoré sa spracúvajú na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu alebo na štatistické účely, môžu byť vyňaté z viacerých uvedených ustanovení všeobecného nariadenia Spojeného kráľovstva o ochrane údajov ([68]). Pokiaľ ide o výskum a štatistiku, možné sú výnimky z ustanovení všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, ktoré sa týkajú potvrdenia spracúvania údajov a prístupu k údajom a záruk v súvislosti s prenosom údajov do tretích krajín; práva na opravu; obmedzenia spracúvania údajov a výhrad voči spracúvaniu. Pokiaľ ide o archiváciu vo verejnom záujme, výnimky sú možné aj v súvislosti s oznamovacou povinnosťou týkajúcou sa opravy alebo vymazania osobných údajov, prípadne obmedzenia ich spracúvania, a v súvislosti s právom na prenosnosť údajov.

(72) Podľa bodu 27 ods. 1 a bodu 28 ods. 1 prílohy 2 k zákonu o ochrane údajov z roku 2018 sú výnimky z uvedených ustanovení všeobecného nariadenia Spojeného kráľovstva o ochrane údajov možné, ak by sa uplatnením týchto ustanovení „zabránilo dosiahnutiu“ príslušných účelov „alebo sa ich dosiahnutie závažným spôsobom sťažilo“ ([69]).

(73) Vzhľadom na ich význam v súvislosti s účinným uplatňovaním individuálnych práv bude akýkoľvek príslušný vývoj týkajúci sa výkladu a uplatňovania výnimiek uvedených v texte (ďalších výnimiek vrátane tej, ktorá sa týka zachovania účinnej imigračnej kontroly) v praxi, ako je vysvetlené v odôvodnení 6, vrátane akéhokoľvek ďalšieho vývoja v judikatúre a usmernení Komisára pre informácie a opatrení na presadzovanie práva, riadne zohľadnený v rámci nepretržitého monitorovania tohto rozhodnutia ([70]).

2.5.7. *Obmedzenia týkajúce sa následných prenosov*

(74) Úroveň ochrany osobných údajov prenášaných z Európskej únie prevádzkovateľom alebo sprostredkovateľom v Spojenom kráľovstve nesmie byť oslabená ďalším prenosom takýchto údajov príjemcom v tretej krajine. Takéto „následné prenosy“, ktoré z hľadiska prevádzkovateľa alebo sprostredkovateľa v Spojenom kráľovstve predstavujú medzinárodné prenosy zo Spojeného kráľovstva, by sa mali povoliť len v prípade, že ďalší príjemca mimo Spojeného kráľovstva takisto podlieha pravidlám zabezpečujúcim podobnú úroveň ochrany, aká je zaručená v právnom poriadku Spojeného kráľovstva. Z toho dôvodu je uplatňovanie pravidiel, ktoré sú stanovené vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov a v zákone o ochrane údajov z roku 2018, na medzinárodné prenosy osobných údajov dôležitým faktorom na zabezpečenie kontinuity ochrany v prípade osobných údajov prenášaných z Európskej únie do Spojeného kráľovstva podľa tohto rozhodnutia.

([66]) Podľa usmernenia musia byť organizácie schopné vysvetliť, prečo je súlad s príslušným ustanovením zákona o ochrane údajov z roku 1998 nezlučiteľný so žurnalistickými účelmi. Prevádzkovatelia musia predovšetkým vyvážiť nepriaznivý vplyv, ktorý by mal súlad s ustanovením na žurnalistiku, s nepriaznivým vplyvom, ktorý by mal nesúlad na práva dotknutej osoby. Ak novinár dokáže dosiahnuť svoje redakčné ciele primeraným spôsobom, ktorý je v súlade so štandardnými ustanoveniami zákona o ochrane údajov, prevádzkovatelia to musia zaistiť. Organizácie musia byť schopné odôvodniť použitie obmedzenia týkajúceho sa každého ustanovenia, v prípade ktorého nedodržali súlad. „Data protection and journalism: a guide for the media“ (Ochrana údajov a žurnalistika: usmernenie pre médiá), k dispozícii na tomto odkaze: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf.

([67]) Príklady verejného záujmu by zahŕňali odhaľovanie alebo zisťovanie trestnej činnosti, ochranu verejného zdravia alebo bezpečnosti, odhaľovanie zavádzajúcich tvrdení jednotlivcov alebo organizácií, prípadne zverejnenie nekompetentnosti, ktorá postihuje verejnosť. Pozri usmernenie orgánu Ofcom, k dispozícii na tomto odkaze: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf a redakčné usmernenia spoločnosti BBC, k dispozícii na tomto odkaze: https://www.bbc.com/editorialguidelines/guidelines/privacy.

([68]) Pozri článok 89 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov a časť 6 bod 27 ods. 2 a bod 28 ods. 2 prílohy 2 k zákonu o ochrane údajov z roku 2018.

([69]) Vzťahuje sa na to požiadavka, aby sa osobné údaje spracúvali v súlade s článkom 89 ods. 1 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, ktorý dopĺňa § 19 zákona o ochrane údajov z roku 2018.

([70]) Pozri odôvodnenia (281) až (287).

(75) Režim medzinárodných prenosov osobných údajov zo Spojeného kráľovstva je stanovený v článkoch 44 – 49 všeobecného nariadenia Spojeného kráľovstva o ochrane osobných údajov, je doplnený zákonom o ochrane údajov z roku 2018 a je v podstate totožný s pravidlami, ktoré sú stanovené v kapitole V nariadenia (EÚ) 2016/679 ([71]). Prenosy osobných údajov do tretej krajiny alebo medzinárodnej organizácii sa môžu uskutočniť iba na základe právnych predpisov o primeranosti [ekvivalent rozhodnutia o primeranosti podľa nariadenia (EÚ) 2016/679 v Spojenom kráľovstve], alebo ak sa neuplatnia právne predpisy o primeranosti, prevádzkovateľ alebo sprostredkovateľ poskytne primerané záruky v súlade s článkom 46 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov. Ak sa neuplatnia právne predpisy o primeranosti ani primerané záruky, prenos sa môže uskutočniť iba na základe výnimiek stanovených v článku 49 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov.

(76) Právne predpisy o primeranosti, ktoré prijíma minister, môžu zabezpečiť, že tretia krajina (alebo územie alebo odvetvie v tretej krajine), medzinárodná organizácia, alebo opis ([72]) takej krajiny, územia, odvetvia, alebo organizácie zaručí primeranú úroveň ochrany osobných údajov. Pri posudzovaní primeranosti úrovne ochrany musí minister zohľadniť presne tie isté prvky, ktorých posúdenie Komisiou sa vyžaduje v článku 45 ods. 2 písm. a) až c) nariadenia (EÚ) 2016/679, vykladanom spoločne s odôvodnením 104 nariadenia (EÚ) 2016/679 a s ponechanou judikatúrou EÚ. To znamená, že príslušnou normou pri posudzovaní primeranej úrovne ochrany tretej krajiny bude, či dotknutá tretia krajina zaručuje úroveň ochrany, ktorá „v zásade zodpovedá“ úrovni zabezpečenej v rámci Spojeného kráľovstva.

(77) Pokiaľ ide o postup, na právne predpisy o primeranosti sa vzťahujú „všeobecné“ procedurálne požiadavky stanovené v § 182 zákona o ochrane údajov z roku 2018. V rámci tohto postupu musí pri navrhovaní prijatia budúcich právnych predpisov Spojeného kráľovstva o primeranosti minister konzultovať s Komisárom pre informácie ([73]). Po prijatí ministrom sa tieto právne predpisy predkladajú parlamentu a podliehajú postupu „negatívneho uznesenia“, na základe ktorého môžu obe snemovne parlamentu preskúmať príslušné právne predpisy a v rámci 40-dňovej lehoty predložiť návrh na zrušenie týchto právnych predpisov ([74]).

(78) Podľa § 17 B ods. 1 zákona o ochrane údajov z roku 2018 sa právne predpisy o primeranosti musia preskúmavať v intervaloch najviac štyroch rokov a minister musí priebežne monitorovať vývoj v tretích krajinách a medzinárodných organizáciách, ktorý by mohol ovplyvniť rozhodnutia o právnych predpisoch o primeranosti alebo ich zmeniť. Ak minister zistí, že krajina alebo organizácia už nezabezpečuje primeranú úroveň ochrany osobných údajov, musí v potrebnom rozsahu zmeniť alebo zrušiť tieto právne predpisy a začať konzultácie s dotknutou treťou krajinou alebo medzinárodnou organizáciou s cieľom napraviť nedostatok primeranej úrovne ochrany. Tieto procedurálne aspekty odrážajú aj zodpovedajúce požiadavky v nariadení (EÚ) 2016/679.

([71]) S výnimkou článku 48 nariadenia (EÚ) 2016/679, ktorý sa Spojené kráľovstvo rozhodlo nezaradiť do všeobecného nariadenia Spojeného kráľovstva o ochrane údajov. V tejto súvislosti je predovšetkým potrebné pripomenúť, že štandard, ktorý sa má považovať za taký, ktorý poskytuje primeranú úroveň ochrany, je skôr štandard „zásadnej rovnocennosti“ ako identity, ako to objasnil Súdny dvor Európskej únie (Schrems I, body 73 – 74) a uznal Európsky výbor pre ochranu údajov (Referenčné kritérium primeranosti, strana 3). Ako to Európsky výbor pre ochranu údajov vysvetlil vo svojom Referenčnom kritériu primeranosti, „[c]ieľom preto nie je odzrkadľovať každý jeden bod európskych právnych predpisov, ale stanoviť základné prvky – hlavné požiadavky týchto právnych predpisov“. V tejto súvislosti je dôležité podotknúť, že hoci právny poriadok Spojeného kráľovstva formálne neobsahuje ustanovenie totožné s článkom 48, rovnaký účinok zaručujú ostatné právne ustanovenia a zásady, t. j. že v odpovedi na žiadosť súdu alebo správneho orgánu v tretej krajine o osobné údaje môžu byť osobné údaje prenesené len do tej tretej krajiny, s ktorou je uzavretá medzinárodná dohoda, na základe ktorej je predmetné rozhodnutie súdu alebo administratívne rozhodnutie tretej krajiny uznané alebo vykonávané v Spojenom kráľovstve, alebo ak je prenos založený na jednom z mechanizmov prenosu, ktoré sú uvedené v kapitole V všeobecného nariadenia Spojeného kráľovstva o ochrane osobných údajov. Konkrétnejšie povedané, aby sa vykonal zahraničný rozsudok, súdy v Spojenom kráľovstve musia byť schopné poukázať na common law alebo na právny predpis, ktorý umožňuje vykonateľnosť rozsudku. Ani common law [pozri vec Adams and Others/Cape Industries Plc. (1990) 2 W.L.R. 657], ani právne predpisy však neumožňujú vykonanie zahraničného rozsudku, v ktorom sa požaduje prenos údajov, bez platnej medzinárodnej dohody. V dôsledku toho sú žiadosti o údaje nevykonateľné podľa práva Spojeného kráľovstva, keďže nie je uzavretá taká medzinárodná dohoda. Navyše na akýkoľvek prenos osobných údajov do tretích krajín, a to aj na základe žiadosti zahraničného súdu alebo správneho orgánu, sa naďalej vzťahujú obmedzenia stanovené v kapitole V všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, ktoré sú totožné so zodpovedajúcimi ustanoveniami nariadenia (EÚ) 2016/679, a preto si vyžadujú uplatnenie jedného z dôvodov prenosu, ktoré sú uvedené v kapitole V, v súlade s konkrétnymi požiadavkami, ktoré sa naň vzťahujú podľa tejto kapitoly.

([72]) Orgány Spojeného kráľovstva vysvetlili, že opis krajiny alebo medzinárodnej organizácie sa týka situácie, v ktorej by bolo potrebné vykonať konkrétne a čiastočné určenie primeranosti s cielenými obmedzeniami (napríklad právny predpis o primeranosti len vo vzťahu k určitému typu prenosu údajov).

([73]) Pozri memorandum o porozumení medzi ministrom ministerstva pre digitálnu oblasť, kultúru, médiá a šport (DCMS) a Úradom Komisára pre informácie o úlohe tohto komisára, pokiaľ ide o nové posúdenia Spojeného kráľovstva z hľadiska primeranosti jeho režimu ochrany údajov, k dispozícii na tomto odkaze: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([74]) Ak obe parlamentné snemovne zahlasujú proti takýmto právnym predpisom, tie prestanú mať v konečnom dôsledku ďalšie právne účinky.

(79) Ak neexistujú právne predpisy o primeranosti, medzinárodné prenosy údajov sa môžu uskutočniť, ak prevádzkovateľ alebo sprostredkovateľ poskytne primerané záruky v súlade s článkom 46 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov. Tieto záruky sú podobné zárukám stanoveným v článku 46 nariadenia (EÚ) 2016/679. Zahŕňajú právne záväzné a vykonateľné nástroje medzi orgánmi verejnej moci alebo verejnoprávnymi subjektmi, záväzné vnútropodnikové pravidlá ([75]), štandardné doložky o ochrane údajov, schválené kódexy správania, schválené certifikačné mechanizmy a s povolením Komisára pre informácie zmluvné doložky medzi prevádzkovateľmi (alebo sprostredkovateľmi) alebo administratívne dojednania medzi orgánmi verejnej moci. Pravidlá však boli upravované z procedurálneho hľadiska, aby fungovali v rámci Spojeného kráľovstva, predovšetkým štandardné doložky o ochrane údajov môže prijať minister (§ 17C) alebo Komisár pre informácie (§ 119A) v súlade so zákonom o ochrane údajov z roku 2018.

(80) Ak sa neuplatní rozhodnutie o primeranosti ani primerané záruky, prenos sa môže uskutočniť iba na základe výnimiek stanovených v článku 49 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov ([76]). V rámci všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sa nezavádzajú žiadne podstatné zmeny týkajúce sa výnimiek v porovnaní so zodpovedajúcimi pravidlami v nariadení (EÚ) 2016/679. Podľa všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sa rovnako ako podľa nariadenia (EÚ) 2016/679 určité výnimky dajú uplatniť, iba ak je prenos občasný ([77]). Komisár pre informácie okrem toho vo svojom usmernení k medzinárodným prenosom údajov objasňuje, že: „Mali by ste ich využívať iba ako skutočné „výnimky“ zo všeobecného pravidla, že sa nemá robiť obmedzený prenos, pokiaľ nie je zabezpečený rozhodnutím o primeranosti alebo pokiaľ nie sú poskytnuté primerané záruky ([78])." Pokiaľ ide o prenosy, ktoré sú nevyhnutné z dôležitých dôvodov verejného záujmu [článok 49 ods. 1 písm. d)], minister môže prostredníctvom predpisov špecifikovať okolnosti, za ktorých nie je prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii potrebný z dôležitých dôvodov verejného záujmu. Minister okrem toho môže prostredníctvom predpisov obmedziť prenos určitej kategórie osobných údajov do tretej krajiny alebo medzinárodnej organizácii, ak sa prenos nedá uskutočniť na základe právnych predpisov o primeranosti a minister považuje obmedzenie za nevyhnutné z dôležitých dôvodov verejného záujmu. Žiadne také predpisy zatiaľ neboli prijaté.

(81) Tento rámec pre medzinárodné prenosy údajov sa začal uplatňovať na konci prechodného obdobia ([79]). V bode 4 prílohy 21 k zákonu o ochrane údajov z roku 2018 [zavedenému právnymi predpismi o ochrane údajov, súkromí a elektronických komunikáciách (zmeny atď.) (vystúpenie z EÚ)] je však stanovené, že od konca prechodného obdobia sa s určitými prenosmi osobných údajov zaobchádza tak, ako keby boli založené na právnych predpisoch o primeranosti. Medzi takéto prenosy patria prenosy do štátu Európskeho hospodárskeho priestoru (EHP), na územie Gibraltáru, inštitúcie, orgánu, úradu alebo agentúry Únie, ktoré boli zriadené prostredníctvom alebo na základe Zmluvy o EÚ, a do tretích krajín, na ktoré sa na konci prechodného obdobia vzťahuje rozhodnutie EÚ o primeranosti. Prenosy do týchto krajín preto môžu pokračovať rovnako ako pred vystúpením Spojeného

([75]) V rámci všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sa ponechávajú pravidlá stanovené v článku 47 nariadenia (EÚ) 2016/679, iba sa upravujú tak, aby zodpovedali pravidlám vo vnútroštátnom kontexte, napríklad nahradením odkazov na príslušný dozorný orgán odkazmi na Komisára pre informácie, vymazaním odkazu na mechanizmus konzistentnosti z odseku 1 a vymazaním celého odseku 3.

([76]) Podľa článku 49 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sú prenosy možné, ak je splnená jedna z týchto podmienok: a) dotknutá osoba vyjadrila výslovný súhlas s navrhovaným prenosom po tom, ako bola informovaná o rizikách, ktoré takéto prenosy môžu pre ňu predstavovať z dôvodu absencie rozhodnutia o primeranosti a primeraných záruk; b) prenos je nevyhnutný na plnenie zmluvy medzi dotknutou osobou a prevádzkovateľom alebo na vykonanie predzmluvných opatrení prijatých na žiadosť dotknutej osoby; c) prenos je potrebný na uzatvorenie alebo plnenie zmluvy uzatvorenej v záujme dotknutej osoby medzi prevádzkovateľom a inou fyzickou alebo právnickou osobou; d) prenos je nevyhnutný z dôležitých dôvodov verejného záujmu; e) prenos je nevyhnutný na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov; f) prenos je nevyhnutný na ochranu životne dôležitých záujmov dotknutej osoby alebo iných osôb, ak je dotknutá osoba fyzicky alebo právne nespôsobilá vyjadriť súhlas; g) prenos sa uskutočňuje z registra, ktorý je podľa vnútroštátneho práva určený na poskytovanie informácií verejnosti a ktorý je otvorený na nahliadanie verejnosti alebo akejkoľvek osobe, ktorá vie preukázať oprávnený záujem, ale len pokiaľ sú v tomto konkrétnom prípade splnené podmienky stanovené vnútroštátnym právom na nahliadanie. Okrem toho, ak nie je splnená žiadna z uvedených podmienok, prenos sa môže uskutočniť, len ak nie je opakujúcej sa povahy, týka sa len obmedzeného počtu dotknutých osôb, je nevyhnutný na účely záväzných oprávnených záujmov, ktoré sleduje prevádzkovateľ a nad ktorými neprevažujú záujmy ani práva a slobody dotknutej osoby, a prevádzkovateľ posúdil všetky okolnosti sprevádzajúce prenos údajov a na základe tohto posúdenia poskytol primerané záruky, pokiaľ ide o ochranu osobných údajov.

([77]) V odôvodnení 111 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sa uvádza, že prenosy údajov súvisiace so zmluvou alebo právnym nárokom sa môžu uskutočniť, iba ak sú občasné.

([78]) Usmernenie Komisára pre informácie k medzinárodným prenosom údajov, k dispozícii na tomto odkaze: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7.

([79]) Počas obdobia maximálne šiestich mesiacov, končiaceho najneskôr 30. júna 2021, sa uplatniteľnosť tohto nového rámca musí vykladať so zreteľom na článok 782 Dohody o obchode a spolupráci medzi Európskou úniou a Európskym spoločenstvom pre atómovú energiu na jednej strane a Spojeným kráľovstvom Veľkej Británie a Severného Írska na strane druhej (L 444/14 z 31.12.2020) (ďalej len „Dohoda o obchode a spolupráci medzi EÚ a Spojeným kráľovstvom“), k dispozícii na tomto odkaze: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:22020A1231(01)&from=SK.

kráľovstva z EÚ. Po skončení prechodného obdobia musí minister preskúmať zistenia primeranosti do 4 rokov, t. j. do konca decembra 2024. Podľa vysvetlenia, ktoré poskytli orgány Spojeného kráľovstva, hoci minister musí vykonať takéto preskúmanie do konca decembra 2024, prechodné ustanovenia neobsahujú ustanovenie o ukončení platnosti, to znamená, že ak sa preskúmanie neukončí do konca decembra 2024, príslušné prechodné ustanovenia automaticky neprestanú platiť.

(82) Napokon, pokiaľ ide o budúci vývoj režimu medzinárodných prenosov Spojeného kráľovstva – prostredníctvom prijatia nových právnych predpisov o primeranosti, uzavretia medzinárodných dohôd alebo vývoja iných mechanizmov prenosu – Komisia bude situáciu pozorne monitorovať, posúdi, či sa rôzne mechanizmy prenosu používajú spôsobom, ktorý zabezpečuje kontinuitu ochrany, a ak je to nevyhnutné, prijme vhodné opatrenia na riešenie možných nepriaznivých dôsledkov na takú kontinuitu (pozri odôvodnenia 278 až 287). Keďže EÚ a Spojené kráľovstvo majú pre medzinárodné prenosy podobné pravidlá, očakáva sa, že problematickým rozdielom by sa mohlo vyhnúť prostredníctvom spolupráce, výmeny informácií a výmeny skúseností vrátane výmen medzi Komisárom pre informácie a Európskym výborom pre ochranu údajov.

2.5.8. *Zodpovednosť*

(83) Podľa zásady zodpovednosti sa od subjektov, ktoré spracúvajú údaje, vyžaduje, aby zaviedli vhodné technické a organizačné opatrenia v záujme účinného dodržiavania svojich povinností v oblasti ochrany údajov a aby vedeli takéto dodržiavanie preukázať, najmä príslušnému dozornému orgánu.

(84) Zásada zodpovednosti stanovená v nariadení (EÚ) 2016/679 bola ponechaná v článku 5 ods. 2 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov bez podstatnej zmeny a to isté platí pre článok 24 o zodpovednosti prevádzkovateľa, článok 25 o špecificky navrhnutej a štandardnej ochrane údajov a článok 30 o záznamoch o spracovateľských činnostiach. Ponechané boli aj články 35 a 36 o posúdení vplyvu na ochranu údajov a o predchádzajúcej konzultácii s dozorným orgánom. Články 37 až 39 nariadenia (EÚ) 2016/679 o určení zodpovedných osôb a ich úlohách boli ponechané vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov bez podstatných zmien. Aj ustanovenia článkov 40 a 42 nariadenia (EÚ) 2016/679 o kódexoch správania a o certifikácii boli ponechané vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov ([80]).

2.6. **Dohľad a presadzovanie**

2.6.1. *Nezávislý dohľad*

(85) S cieľom zaistiť, aby bola primeraná úroveň ochrany údajov zabezpečená v praxi, by mal byť zriadený nezávislý dozorný orgán, ktorý bude mať právomoc monitorovať a presadzovať dodržiavanie pravidiel ochrany údajov. Tento orgán by mal pri plnení svojich úloh a výkone svojich právomocí konať úplne nezávisle a nestranne.

(86) V Spojenom kráľovstve vykonáva dohľad a presadzovanie dodržiavania všeobecného nariadenia Spojeného kráľovstva o ochrane údajov a zákona o ochrane údajov z roku 2018 Komisár pre informácie. Komisár pre informácie je „Corporation Sole“, čiže samostatný právny subjekt zložený z jednej osoby. Komisára pre informácie pri jeho práci podporuje jeho úrad. K 31. marcu 2020 mal Úrad Komisára pre informácie 768 stálych zamestnancov ([81]). Hlavným ministerstvom vo vzťahu ku Komisárovi pre informácie je ministerstvo pre digitálnu oblasť, kultúru, médiá a šport (Department for Digital, Culture, Media and Sport) ([82]).

(87) Nezávislosť Komisára je výslovne stanovená v článku 52 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, pričom nedošlo k žiadnym zásadným zmenám článku 52 ods. 1 až 3 všeobecného nariadenia o ochrane údajov. Komisár musí pri plnení svojich úloh a vykonávaní svojich právomocí podľa všeobecného nariadenia Spojeného kráľovstva o ochrane údajov konať úplne nezávisle, nesmie byť pod vonkajším vplyvom, či už priamym

([80]) Ak je to potrebné, tieto odkazy sa nahradia odkazmi na orgány Spojeného kráľovstva. Napríklad podľa § 17 zákona o ochrane údajov z roku 2018 môže Komisár pre informácie alebo národný akreditačný orgán Spojeného kráľovstva akreditovať osobu spĺňajúcu požiadavky stanovené v článku 43 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov na účely monitorovania súladu s certifikáciou.

([81]) Výročná správa a finančné výkazy Komisára pre informácie za roky 2019 – 2020, k dispozícii na tomto odkaze: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

([82]) Ich vzájomný vzťah upravuje dohoda o riadení. Medzi najdôležitejšie povinnosti Ministerstva pre digitálnu oblasť, kultúru, médiá a šport ako hlavného ministerstva patrí najmä: zabezpečiť, aby Komisár pre informácie bol primerane financovaný a mal primerané zdroje; zastupovať záujmy Komisára pre informácie v parlamente a v rámci vzťahov s ďalšími ministerstvami; zabezpečiť zavedenie spoľahlivého vnútroštátneho rámca na ochranu údajov a poskytovať Komisárovi pre informácie usmernenia a podporu v prevádzkových otázkach, ako sú otázky týkajúce sa nehnuteľností, lízingov a obstarávania (dohoda o riadení na roky 2018 – 2021, k dispozícii na tomto odkaze: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

alebo nepriamym, vo vzťahu k týmto úlohám a právomociam, a nesmie od nikoho žiadať ani prijímať pokyny. Komisár sa tiež musí zdržať akéhokoľvek konania nezlučiteľného so svojimi povinnosťami a počas výkonu funkcie nevykonáva žiadnu platenú ani neplatenú pracovnú činnosť nezlučiteľnú s jeho funkciou.

(88) Podmienky vymenovania a odvolania Komisára pre informácie sú stanovené v prílohe 12 k zákonu o ochrane údajov z roku 2018. Komisára pre informácie vymenúva jej veličenstvo na odporúčanie vlády na základe spravodlivého a otvoreného výberového konania. Uchádzač musí mať primeranú kvalifikáciu, zručnosti a schopnosti. V súlade s kódexom riadenia verejných menovaní ([83]) zostaví poradná hodnotiaca komisia zoznam menovateľných kandidátov. Predtým, ako minister ministerstva pre digitálnu oblasť, kultúru, médiá a šport dokončí svoje rozhodnutie, príslušný užší výbor parlamentu musí vykonať kontrolu pred vymenovaním. Stanovisko výboru sa zverejňuje ([84]).

(89) Komisár pre informácie vykonáva svoju funkciu najviac sedem rokov. Žiadna osoba nemôže byť vymenovaná za Komisára pre informácie viac ako raz. Z funkcie ho môže odvolať jej veličenstvo na základe jej určenému prejavu vôle oboch snemovní parlamentu (tzv. Address) ([85]). Žiadosť o odvolanie Komisára pre informácie možno predložiť niektorej zo snemovní parlamentu, len ak minister predloží správu, v ktorej uvedie, že je presvedčený, že Komisár pre informácie sa dopustil závažného pochybenia a/alebo že Komisár už nespĺňa podmienky požadované na výkon svojich funkcií ([86]).

(90) Financovanie Komisára pre informácie pochádza z troch zdrojov: i) poplatky za ochranu údajov, ktoré platia prevádzkovatelia a ktoré sú stanovené právnymi predpismi ministra ([87]) [právne predpisy o ochrane údajov (poplatky a informácie) z roku 2018], pričom tvoria 85 – 90 % ročného rozpočtu Úradu Komisára pre informácie ([88]); ii) subvencie, ktoré môže vláda poskytnúť Komisárovi pre informácie. Tieto subvencie sa využívajú najmä na financovanie prevádzkových nákladov Komisára pre informácie, pokiaľ ide o úlohy nesúvisiace s ochranou údajov ([89]); a iii) poplatky účtované za služby ([90]). V súčasnosti sa neúčtujú žiadne takéto poplatky.

(91) Všeobecné funkcie Komisára pre informácie v súvislosti so spracúvaním osobných údajov, na ktoré sa vzťahuje všeobecné nariadenie Spojeného kráľovstva o ochrane údajov, sú stanovené v článku 57 uvedeného nariadenia a dôsledne odrážajú zodpovedajúce pravidlá nariadenia (EÚ) 2016/679. Medzi jeho úlohy patrí monitorovanie a presadzovanie všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, podpora informovanosti verejnosti, vybavovanie sťažností podávaných dotknutými osobami, vedenie vyšetrovaní atď. Okrem toho sú v § 115 zákona o ochrane údajov z roku 2018 stanovené ďalšie všeobecné funkcie Komisára, ku ktorým patrí povinnosť poskytovať poradenstvo parlamentu, vláde a iným inštitúciám a orgánom v oblasti legislatívnych a administratívnych opatrení týkajúcich sa ochrany práv a slobôd jednotlivcov, pokiaľ ide o spracúvanie osobných údajov, ako aj právomoc vydávať, z vlastnej iniciatívy Komisára alebo na požiadanie, stanoviská určené parlamentu,

([83]) Kódex riadenia verejných menovaní, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf.

([84]) Druhá správa zo zasadnutia Výboru Dolnej snemovne pre kultúru, médiá a šport 2015 – 2016, k dispozícii na tomto odkaze: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([85]) „Address“ je návrh predložený parlamentu, ktorého cieľom je upovedomiť monarchu o stanoviskách parlamentu k určitej téme.

([86]) Bod 3 ods. 3 prílohy 12 k zákonu o ochrane údajov z roku 2018.

([87]) § 137 zákona o ochrane údajov z roku 2018, pozri odôvodnenie 17.

([88]) § 137 a 138 zákona o ochrane údajov z roku 2018 obsahujú niekoľko záruk na zabezpečenie toho, aby poplatky boli stanovené na primeranej úrovni. V § 137 ods. 4 sa konkrétne uvádzajú záležitosti, ktoré musí minister zohľadniť pri vydávaní právnych predpisov, v ktorých sa stanovuje suma, ktorú musia zaplatiť rôzne organizácie. Navyše sa v § 138 ods. 1 a § 182 zákona o ochrane údajov z roku 2018 tiež stanovuje zákonná požiadavka, že minister je ešte pred prijatím týchto právnych predpisov povinný uskutočniť konzultácie s Komisárom pre informácie a inými zástupcami osôb, na ktoré by sa tieto právne predpisy mohli vzťahovať, a to v záujme zohľadnenia ich názorov. Komisár pre informácie je okrem toho podľa § 138 ods. 2 zákona o ochrane údajov z roku 2018 povinný priebežne preskúmavať fungovanie právnych predpisov o poplatkoch a môže ministrovi predložiť návrhy na ich zmenu. A napokon, s výnimkou prípadov, keď sa právne predpisy prijímajú len s cieľom zohľadniť zvýšenie indexu maloobchodných cien (v takom prípade budú podliehať postupu tzv. negatívneho uznesenia parlamentu), tieto právne predpisy podliehajú postupu kladného uznesenia a môžu sa prijať až po tom, ako ich každá z komôr parlamentu schváli svojim uznesením.

([89]) V dohode o riadení sa ozrejmilo, že minister môže prideliť Komisárovi pre informácie prostriedky z financií, ktoré poskytol parlament podľa prílohy 12 bodu 9 k zákonu o ochrane údajov z roku 2018. Po konzultácii s Komisárom pre informácie poskytne Ministerstvo pre digitálnu oblasť, kultúru, médiá a šport tomuto komisárovi príslušné sumy (subvencie) na pokrytie jeho administratívnych nákladov a plnenie funkcií vo vzťahu k viacerým osobitným úlohám vrátane slobody informácií (dohoda o riadení na roky 2018 – 2021, bod 1.12, pozri poznámku pod čiarou č. 82).

([90]) Pozri § 134 zákona o ochrane údajov z roku 2018.

vláde alebo iným inštitúciám a orgánom, ako aj verejnosti k akejkoľvek otázke týkajúcej sa ochrany osobných údajov. V záujme zachovania nezávislosti justície nie je Komisár pre informácie oprávnený vykonávať svoje funkcie v súvislosti so spracúvaním osobných údajov jednotlivcom konajúcim v rámci súdnej právomoci, resp. súdom či tribunálom konajúcim v rámci svojej súdnej právomoci. Dohľad nad justíciou však vykonávajú špecializované orgány (pozri odôvodnenia 99 až 103).

2.6.2. *Presadzovania vrátane sankcií*

(92) Právomoci Komisára pre informácie sú stanovené v článku 58 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, a to bez zavedenia akýchkoľvek podstatných zmien oproti zodpovedajúcemu článku nariadenia (EÚ) 2016/679. V zákone o ochrane údajov z roku 2018 sú stanovené doplňujúce pravidlá týkajúce sa spôsobu vykonávania týchto právomocí. Komisár má predovšetkým tieto právomoci: a) nariadiť prevádzkovateľovi a sprostredkovateľovi (a za určitých okolností akejkoľvek inej osobe), aby poskytli potrebné informácie prostredníctvom oznámenia („informačné oznámenie“) ([91]); b) vykonávať vyšetrovania a audity prostredníctvom oznámenia o posúdení, v ktorom sa môže vyžadovať, aby prevádzkovateľ alebo sprostredkovateľ povolil Komisárovi pre informácie vstúpiť do určených priestorov, skontrolovať alebo preskúmať dokumenty alebo vybavenie, vypočuť osoby, ktoré spracúvajú osobné údaje v mene prevádzkovateľa („oznámenie o posúdení“) ([92]); c) získať iným spôsobom prístup k dokumentom prevádzkovateľov a sprostredkovateľov a prístup do ich priestorov v súlade s § 154 zákona o ochrane údajov z roku 2018 („právomoci na vstup a inšpekciu“); d) vykonávať nápravné právomoci, a to aj prostredníctvom varovaní a napomenutí, alebo vydávať príkazy prostredníctvom presadzovacieho oznámenia, v ktorom sa od prevádzkovateľov, resp. sprostredkovateľov vyžaduje, aby prijali alebo sa zdržali prijatia konkrétnych krokov, a to vrátane príkazu prevádzkovateľovi alebo sprostredkovateľovi, aby vykonal čokoľvek uvedené v článku 58 ods. 2 písm. c) až g) a písm. j) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov („presadzovacie oznámenie“) ([93]); e) udeľovať správne pokuty vo forme oznámenia o uložení sankcie (ďalej len „oznámenie o uložení sankcie“) ([94]). Správne pokuty môžu byť udelené aj vtedy, keď orgán verejnej moci nedodrží ustanovenia nariadenia Spojeného kráľovstva o ochrane osobných údajov ([95]).

(93) Okolnosti, za ktorých Komisár pre informácie vydáva informačné oznámenie, oznámenie o posúdení, presadzovacie oznámenie alebo oznámenie o uložení sankcie, sa stanovujú v jeho regulačnej politike ([96]). V presadzovacom oznámení, ktoré je reakciou na nesplnenie povinnosti prevádzkovateľa alebo sprostredkovateľa, sa môžu stanoviť iba požiadavky, ktoré Komisár považuje za vhodné na účely nápravy nesplnenia povinnosti. Presadzovacie oznámenia a oznámenia o uložení sankcie sa môžu vydávať prevádzkovateľovi alebo sprostredkovateľovi v súvislosti s porušením ustanovení kapitoly II všeobecného nariadenia Spojeného kráľovstva o ochrane údajov (zásady spracúvania), článkov 12 až 22 (práva dotknutej osoby), článkov 25 až 39 (povinnosti prevádzkovateľov a sprostredkovateľov) a článkov 44 až 49 (medzinárodné prenosy) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov. Presadzovacie oznámenie sa môže vydať, aj keď prevádzkovateľ nesplnil požiadavku zaplatiť poplatok stanovený v právnych predpisoch podľa § 137 zákona o ochrane údajov z roku 2018. Okrem toho sa presadzovacie oznámenie môže vydať monitorujúcemu subjektu podľa článku 41 alebo poskytovateľovi certifikácie, ak si nesplnia svoje povinnosti podľa všeobecného nariadenia Spojeného kráľovstva o ochrane údajov. Oznámenie o uložení sankcie je možné vydať aj osobe, ktorá nedodržala informačné oznámenie, oznámenie o posúdení alebo presadzovacie oznámenie.

(94) V oznámení o uložení sankcie sa vyžaduje, aby príslušná osoba zaplatila Komisárovi pre informácie sumu uvedenú v oznámení. Pri určovaní toho, či sa má určitej osobe vydať oznámenie o uložení sankcie, a pri určovaní výšky sankcie musí Komisár pre informácie zohľadniť skutočnosti uvedené v článku 83 ods. 1 a 2 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, ktoré sú totožné so zodpovedajúcimi pravidlami nariadenia (EÚ) 2016/679 ([97]). Podľa článku 83 ods. 4 a 5 je maximálna výška správnej pokuty v prípade nesplnenia povinností

([91]) § 142 zákona o ochrane údajov z roku 2018 (s výhradou obmedzení stanovených v § 143 zákona o ochrane údajov z roku 2018).

([92]) § 146 zákona o ochrane údajov z roku 2018 (s výhradou obmedzení stanovených v § 147 zákona o ochrane údajov z roku 2018).

([93]) § 149 až 151 zákona o ochrane údajov z roku 2018 (s výhradou obmedzení stanovených v § 152 zákona o ochrane údajov z roku 2018).

([94]) § 155 zákona o ochrane údajov z roku 2018 a článok 83 nariadenia Spojeného kráľovstva o ochrane osobných údajov.

([95]) Vyplýva to z § 155 ods. 1 zákona o ochrane údajov z roku 2018 v spojení s § 149 ods. 2 a 5 zákona o ochrane údajov z roku 2018 a z §156 ods. 4 zákona o ochrane údajov z roku 2018, ktorým sa obmedzuje vydávanie oznámení o uložení sankcie, pokiaľ ide o Komisárov pre majetok koruny (Crown Estate Commissioners) a prevádzkovateľov na kráľovskom dvore podľa § 209 ods. 4 zákona o ochrane údajov z roku 2018.

([96]) Regulačná politika, k dispozícii na tomto odkaze: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.

([97]) Vrátane povahy a závažnosti porušenia (pri zohľadnení povahy, rozsahu alebo účelu dotknutého spracúvania, ako aj počtu dotknutých osôb, na ktoré malo vplyv, a rozsahu škody, ktorú utrpeli), úmyselného alebo nedbanlivého charakteru porušenia, akýchkoľvek opatrení prijatých prevádzkovateľom s cieľom zmierniť škodu, ktorú utrpeli dotknuté osoby, miery zodpovednosti prevádzkovateľa alebo sprostredkovateľa (so zreteľom na technické a organizačné opatrenia vykonané prevádzkovateľom alebo sprostredkovateľom), akýchkoľvek relevantných predchádzajúcich porušení zo strany prevádzkovateľa alebo sprostredkovateľa, miery spolupráce s Komisárom, kategórií osobných údajov, ktorých sa porušenie týka, akýchkoľvek iných priťažujúcich alebo poľahčujúcich okolností prípadu, ako napríklad získaných finančných výhod alebo strát, ktorým sa zabránilo, priamo alebo nepriamo, v súvislosti s porušením.

uvedených v týchto ustanoveniach 8 700 000 GBP, respektíve 17 500 000 GBP. V prípade podniku môže Komisár pre informácie uložiť pokutu ako percentuálny podiel svetového ročného obratu, ak je tá suma vyššia. Tieto sumy sú rovnako ako v ekvivalentných ustanoveniach nariadenia (EÚ) 2016/679 stanovené na úrovni 2 % a 4 % v článku 83 ods. 4, respektíve ods. 5. V prípade nedodržania informačného oznámenia, oznámenia o posúdení alebo presadzovacieho oznámenia je maximálna výška sankcie, ktorú je možné uložiť na základe oznámenia o uložení sankcie, 17 500 000 GBP alebo v prípade podniku 4 % svetového ročného obratu.

(95) Všeobecným nariadením Spojeného kráľovstva o ochrane údajov a zákonom o ochrane údajov z roku 2018 sa posilnili aj ďalšie právomoci Komisára pre informácie. Komisár teraz môže napríklad vykonávať povinné audity týkajúce sa všetkých prevádzkovateľov a sprostredkovateľov s použitím oznámení o posúdení, zatiaľ čo podľa predchádzajúceho právneho predpisu, zákona o ochrane údajov z roku 1998, mal Komisár túto právomoc iba vo vzťahu k ústrednej štátnej správe a zdravotníckym organizáciám, pričom ostatné subjekty museli s auditom súhlasiť.

(96) Od zavedenia nariadenia (EÚ) 2016/679 Komisár pre informácie vybavuje približne 40 000 sťažností dotknutých osôb ročne ([98]) a okrem toho vykonáva približne 2 000 vyšetrovaní *ex officio* ([99]). Väčšina sťažností sa týka práv na prístup k údajom a poskytovania údajov. Komisár na základe vyšetrovania prijíma opatrenia v oblasti presadzovania v širokej škále odvetví. Konkrétnejšie, podľa najnovšej výročnej správy Komisára pre informácie (2019 – 2020) ([100]) vydal Komisár počas vykazovaného obdobia 54 informačných oznámení, osem oznámení o posúdení, sedem presadzovacích oznámení, štyri varovania, osem žalôb a 15 pokút ([101]).

(97) To zahŕňa niekoľko značných peňažných sankcií uložených podľa nariadenia (EÚ) 2016/679 a zákona o ochrane údajov z roku 2018. Komisár pre informácie konkrétne v októbri 2020 uložil britskej leteckej spoločnosti pokutu vo výške 20 miliónov GBP za porušenie ochrany údajov, ktoré malo vplyv na viac ako 400 000 zákazníkov. Koncom októbra 2020 bola medzinárodnej hotelovej sieti uložená pokuta vo výške 18,4 milióna GBP za to, že nedokázala zaistiť bezpečnosť osobných údajov miliónov zákazníkov, a v novembri 2020 bola britskému poskytovateľovi služieb, ktorý online predáva vstupenky na podujatia, uložená pokuta vo výške 1,25 milióna GBP za nedostatočnú ochranu platobných údajov zákazníkov ([102]).

(98) Okrem toho, že Komisár pre informácie má právomoci v oblasti presadzovania opísané v odôvodnení 92, určité porušenia právnych predpisov o ochrane údajov predstavujú trestné činy, a preto môžu podliehať trestnoprávnym sankciám (§ 196 zákona o ochrane údajov z roku 2018). To sa týka napríklad vedomého alebo neuváženého získania alebo poskytnutia osobných údajov bez súhlasu prevádzkovateľa, poskytnutia prístupu k osobným údajom inej osobe bez súhlasu prevádzkovateľa ([103]), opätovnej identifikácie anonymizovaných osobných údajov bez súhlasu prevádzkovateľa zodpovedného za anonymizáciu osobných údajov ([104]), úmyselného bránenia Komisárovi pre informácie pri výkone jeho právomocí v súvislosti s kontrolou osobných údajov v súlade s medzinárodnými záväzkami ([105]), vydávania nepravdivých vyhlásení o odpovedi na informačné oznámenie alebo zničenia informácií v súvislosti s informačným oznámením a oznámením o posúdení ([106]).

([98]) Podľa informácií poskytnutých orgánmi Spojeného kráľovstva nebolo v období, na ktoré sa vzťahuje výročná správa Komisára pre informácie za roky 2019 – 2020, zistené žiadne porušenie približne v 25 % prípadov, asi v 29 % prípadov bola dotknutá osoba požiadaná, aby buď po prvýkrát predložila svoje pochybnosti prevádzkovateľovi, aby počkala na odpoveď prevádzkovateľa, alebo aby pokračovala v prebiehajúcom dialógu s prevádzkovateľom, zhruba v 17 % prípadov nebolo zistené žiadne porušenie, ale prevádzkovateľovi bolo predložené odporúčanie, približne v 25 % prípadov Komisár pre informácie zistil porušenie a buď poskytol prevádzkovateľovi odporúčanie, alebo bol prevádzkovateľ požiadaný, aby prijal určité opatrenia, asi v 3 % prípadov bolo prijaté rozhodnutie, že sťažnosť nepatrí do oblasti pôsobnosti nariadenia (EÚ) 2016/679, a zhruba 1 % prípadov sa postúpilo inému orgánu pre ochranu údajov v rámci Európskeho výboru pre ochranu údajov.

([99]) Komisár pre informácie môže iniciovať tieto vyšetrovania na základe informácií prijatých z rôznych zdrojov vrátane oznámení o porušení ochrany osobných údajov, postúpení zo strany iných orgánov verejnej moci Spojeného kráľovstva alebo zahraničných orgánov pre ochranu údajov a sťažností predložených jednotlivcami alebo organizáciami občianskej spoločnosti.

([100]) Výročná správa a finančné výkazy Komisára pre informácie za roky 2019 – 2020 (pozri poznámku pod čiarou č. 81).

([101]) Podľa predchádzajúcej výročnej správy vzťahujúcej sa na roky 2018 – 2019 vydal Komisár pre informácie v súlade so zákonom o ochrane údajov z roku 1998 počas vykazovaného obdobia 22 oznámení o uložení sankcie, ktorých výška dosahovala celkovo 3 010 610 GBP vrátane dvoch pokút vo výške 500 000 GBP (maximum povolené podľa zákona o ochrane údajov z roku 1998). Po odhaleniach týkajúcich sa spoločnosti Cambridge Analytica viedol Komisár pre informácie v roku 2018 najmä vyšetrovanie využívania analýzy údajov na politické účely. Výsledkom vyšetrovania bola politická správa, súbor odporúčaní, pokuta vo výške 500 000 GBP uložená spoločnosti Facebook a presadzovacie oznámenie adresované spoločnosti AggregateIQ, kanadskému sprostredkovateľovi údajov, v ktorom sa spoločnosti nariaďovalo vymazať osobné údaje občanov Spojeného kráľovstva a osôb s pobytom na území Spojeného kráľovstva, ktoré uchovávala (pozri Výročnú správu a finančné výkazy Komisára pre informácie za roky 2018 – 2019, k dispozícii na tomto odkaze https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

([102]) Zhrnutie prijatých opatrení presadzovania práva sa uvádza na webovom sídle Komisára pre informácie a je k dispozícii na tomto odkaze: https://ico.org.uk/action-weve-taken/enforcement/.

([103]) § 170 zákona o ochrane údajov z roku 2018.

([104]) § 171 zákona o ochrane údajov z roku 2018.

([105]) § 119 zákona o ochrane údajov z roku 2018.

([106]) § 144 a § 148 zákona o ochrane údajov z roku 2018.

2.6.3. *Dohľad nad justíciou*

(99) Dohľad nad spracúvaním osobných údajov súdmi a justíciou je dvojaký. Ak súdny úradník alebo súd nekoná v rámci súdnej právomoci, dohľad vykonáva Komisár pre informácie. Ak prevádzkovateľ koná v rámci súdnej právomoci, Komisár pre informácie nemôže plniť svoje funkcie dohľadu ([107]) a dohľad vykonávajú osobitné orgány. Uvedené odráža prístup prijatý v nariadení (EÚ) 2016/679 (článok 55 ods. 3).

(100) Konkrétne v druhom scenári, pokiaľ ide o súdy Anglicka a Walesu a ich tribunály prvého stupňa a vyššie tribunály (First-tier and Upper Tribunals of England and Wales), takýto dohľad vykonáva súdna rada pre ochranu údajov (Judicial Data Protection Panel) ([108]). Okrem toho šéf justície Anglicka a Walesu (Lord Chief Justice) a šéf tribunálov (Senior President of Tribunals) vydali oznámenie o ochrane osobných údajov ([109]), v ktorom sa uvádza, ako súdy v Anglicku a Walese spracúvajú osobné údaje na účely plnenia súdnej funkcie. Podobné oznámenie vydali súdy Severného Írska ([110]) a Škótska ([111]).

(101) Okrem toho v Severnom Írsku vymenoval šéf justície Severného Írska (Lord Chief Justice of Northern Ireland) sudcu Vrchného súdu (High Court) za sudcu pre dohľad nad údajmi (Data Supervisory Judge) ([112]). Vydal tiež usmernenia pre severoírsku justíciu o tom, čo robiť v prípade straty alebo potenciálnej straty údajov a o postupe riešenia akýchkoľvek otázok, ktoré z toho vyplývajú ([113]).

(102) V Škótsku šéf justície Lord President vymenoval sudcu pre dohľad nad údajmi (Data Supervisory Judge), ktorý vyšetruje všetky sťažnosti z dôvodu ochrany údajov. Stanovuje sa tak v pravidlách súdnych sťažností, ktoré odrážajú pravidlá stanovené pre Anglicko a Wales ([114]).

(103) Napokon na najvyššom súde (Supreme Court) je vymenovaný jeden zo sudcov tohto súdu, aby vykonával dohľad nad ochranou údajov.

2.6.4. *Náprava*

(104) V záujme zabezpečenia primeranej ochrany, a najmä vymáhania individuálnych práv, by dotknutá osoba mala mať k dispozícii účinné správne a súdne prostriedky nápravy vrátane náhrady škôd.

([107]) § 117 zákona o ochrane údajov z roku 2018.

([108]) Súdna rada pre ochranu údajov je zodpovedná za poskytovanie usmernení a odbornej prípravy pre justíciu. Zaoberá sa aj sťažnosťami dotknutých osôb v súvislosti so spracúvaním osobných údajov súdmi, tribunálmi a jednotlivcami konajúcimi v rámci súdnej právomoci. Cieľom súdnej rady pre ochranu údajov je poskytnúť prostriedky na riešenie akejkoľvek sťažnosti. Ak sťažovateľ nebol spokojný s rozhodnutím tejto rady a poskytol dodatočné dôkazy, rada môže svoje rozhodnutie prehodnotiť. Hoci samotná súdna rada pre ochranu údajov neukladá finančné sankcie, ak sa domnieva, že došlo k dostatočne závažnému porušeniu zákona o ochrane údajov z roku 2018, môže vec postúpiť justičnému vyšetrovaciemu úradu (Judicial Conduct Investigation Office), ktorý sťažnosť vyšetrí. Ak sa sťažnosti vyhovie, je vecou lorda kancelára a šéfa justície Anglicka a Walesu (alebo vyššieho sudcu povereného konať v jeho mene), aby rozhodli, aké kroky by sa mali podniknúť proti dotknutej osobe zastávajúcej príslušný úrad. V poradí závažnosti by to mohlo zahŕňať: formálnu radu, formálne varovanie, napomenutie a v konečnom dôsledku odvolanie z funkcie. Ak je jednotlivec nespokojný so spôsobom, akým justičný vyšetrovací úrad (Judicial Conduct Investigation Office) vyšetroval sťažnosť, svoju sťažnosť môže ďalej predložiť ombudsmanovi pre menovania a správanie sudcov (Judicial Appointments and Conduct Ombudsman) (pozri https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Tento ombudsman má právomoc požiadať justičný vyšetrovací úrad (Judicial Conduct Investigation Office) o opätovné preskúmanie sťažnosti a môže navrhnúť, aby bola sťažovateľovi vyplatená náhrada škody, ak sa domnieva, že utrpel škodu v dôsledku nesprávneho úradného postupu.

([109]) Oznámenie o ochrane osobných údajov šéfa justície Anglicka a Walesu (Lord Chief Justice) a šéfa tribunálov (Senior President of Tribunals) je k dispozícii na tomto odkaze: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([110]) Oznámenie o ochrane osobných údajov šéfa justície Severného Írska (Lord Chief Justice of Northern Ireland) je k dispozícii na tomto odkaze: https://judiciaryni.uk/data-privacy.

([111]) Oznámenie o ochrane osobných údajov pre škótske súdy a tribunály je k dispozícii na tomto odkaze: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([112]) Sudca pre dohľad nad údajmi poskytuje justícii usmernenie a vyšetruje porušenia a/alebo sťažnosti v súvislosti so spracúvaním osobných údajov súdmi alebo jednotlivcami konajúcimi v rámci súdnej právomoci.

([113]) Ak sa sťažnosť alebo porušenie považujú za závažné, postúpia sa v súlade s kódexom postupov pre sťažnosti (Code of practice on Complaints) vydaným šéfom justície Severného Írska (Lord Chief Justice of Northern Ireland) súdnemu úradníkovi pre sťažnosti (Judicial Complaints Officer) na ďalšie vyšetrovanie. Výsledkom takejto sťažnosti môžu byť: žiadne ďalšie opatrenia, poradenstvo, odborná príprava alebo mentorstvo, neformálne varovanie, formálne varovanie, konečné varovanie, obmedzenie praxe alebo postúpenie správnemu tribunálu. Kódex postupov pre sťažnosti vydaný šéfom justície Severného Írska (Lord Chief Justice of Northern Ireland) je k dispozícii na tomto odkaze: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp.__1.pdf.

([114]) Sudca pre dohľad nad údajmi (Data Supervisory Judge) vyšetruje každú odôvodnenú sťažnosť, ktorá sa postupuje šéfovi justície Lord President, ktorý má právomoc vydávať rady, formálne varovanie alebo napomenutie, ak to považuje za potrebné (rovnocenné pravidlá existujú pre členov tribunálov a sú k dispozícii na tomto odkaze: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

(105) Po prvé, dotknutá osoba má právo podať sťažnosť Komisárovi pre informácie, ak sa domnieva, že v súvislosti s osobnými údajmi, ktoré sa jej týkajú, došlo k porušeniu zákona o ochrane údajov z roku 2018 ([115]). Vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov sa ponechávajú pravidlá uvedené v článku 77 nariadenia (EÚ) 2016/679 týkajúce sa tohto práva bez podstatných zmien. To isté platí pre článok 57 ods. 1 písm. f) a ods. 2, v ktorých sa stanovujú úlohy Komisie v súvislosti s vybavovaním sťažností. Ako sa uvádza v odôvodneniach 92 a 98, Komisár pre informácie má právomoc posúdiť dodržiavanie všeobecného nariadenia Spojeného kráľovstva o ochrane údajov a zákona o ochrane údajov z roku 2018 prevádzkovateľom a sprostredkovateľom a požadovať od nich, aby v prípade nedodržiavania tohto zákona prijali potrebné kroky, resp. aby sa zdržali prijatia potrebných krokov, ako aj uložiť pokuty.

(106) Po druhé vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov a v zákone o ochrane údajov z roku 2018 sa stanovuje právo na prostriedok nápravy voči rozhodnutiu Komisára pre informácie. Podľa článku 78 ods. 1 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov má jednotlivec právo na účinný súdny prostriedok nápravy voči právne záväznému rozhodnutiu Komisára pre informácie, ktoré sa ho týka. Sudca v rámci súdneho preskúmania prešetrí rozhodnutie, ktoré je napadnuté v žalobe, a posúdi, či Komisár pre informácie konal v súlade so zákonom. Navyše, ak Komisár pre informácie nevybaví sťažnosť predloženú dotknutou osobou primerane, podľa článku 78 ods. 2 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov ([116])má sťažovateľ prístup k súdnemu prostriedku nápravy. Môže sa obrátiť na tribunál prvého stupňa, aby Komisárovi pre informácie nariadil prijať primerané kroky v reakcii na sťažnosť alebo informovať sťažovateľa o pokroku dosiahnutom v súvislosti so sťažnosťou ([117]). Okrem toho sa každá osoba, ktorá dostane od Komisára pre informácie ktorékoľvek z uvedených oznámení (informačné oznámenie, oznámenie o posúdení, presadzovacie oznámenie alebo oznámenie o uložení sankcie), môže odvolať na tribunál prvého stupňa ([118]). Ak sa tribunál domnieva, že rozhodnutie Komisára pre informácie nie je v súlade so zákonom alebo že Komisár pre informácie mal uplatniť svoju voľnú úvahu inak, tribunál musí odvolaniu vyhovieť, resp. musí vydať iné oznámenie alebo prijať iné rozhodnutie, ktoré mohol vydať alebo prijať Komisár pre informácie.

(107) Po tretie jednotlivci môžu získať súdne prostriedky nápravy voči prevádzkovateľom a sprostredkovateľom priamo na súdoch podľa článku 79 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov a § 167 zákona o ochrane údajov z roku 2018. Ak súd na návrh dotknutej osoby dospeje k záveru, že došlo k porušeniu práv dotknutej osoby v zmysle právnych predpisov o ochrane údajov, môže nariadiť prevádzkovateľovi v súvislosti so spracúvaním alebo sprostredkovateľovi konajúcemu v mene tohto prevádzkovateľa, aby podnikol kroky uvedené v súdnom príkaze alebo aby sa zdržal prijatia krokov uvedených v súdnom príkaze.

(108) Okrem toho podľa článku 82 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov a § 168 zákona o ochrane údajov z roku 2018 má každá osoba, ktorá utrpela materiálnu alebo nemateriálnu škodu v dôsledku porušenia všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, právo na náhradu utrpenej škody od prevádzkovateľa alebo sprostredkovateľa. Pravidlá týkajúce sa náhrady škody a zodpovednosti uvedené v článku 82 ods. 1 až 5 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov sú totožné so zodpovedajúcimi pravidlami uvedenými v nariadení (EÚ) 2016/679. Podľa § 168 zákona o ochrane údajov z roku 2018 zahŕňa nemajetková škoda aj ťažkosti. Podľa článku 80 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov má dotknutá osoba takisto právo poveriť zastupiteľský orgán alebo organizáciu, aby v jej mene (podľa článku 77 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov) podali sťažnosť Komisárovi pre informácie a aby v jej mene uplatnili práva uvedené v článkoch 78 (právo na účinný súdny prostriedok nápravy voči rozhodnutiu Komisára pre informácie), 79 (právo na účinný súdny prostriedok nápravy voči prevádzkovateľovi alebo sprostredkovateľovi) a 82 (právo na náhradu škody a zodpovednosť) všeobecného nariadenia Spojeného kráľovstva o ochrane údajov.

(109) Po štvrté, pokiaľ sa akákoľvek osoba domnieva, že orgány verejnej moci porušili jej práva vrátane práva na súkromie a ochranu údajov, môže popri uvedených prostriedkoch nápravy dosiahnuť nápravu na súdoch Spojeného kráľovstva podľa zákona o ľudských právach z roku 1998 ([119]). Jednotlivec, ktorý tvrdí, že orgán verejnej moci konal (alebo navrhuje konať) spôsobom, ktorý je nezlučiteľný s právom vyplývajúcim z dohovoru, a teda protiprávny podľa § 6 ods. 1 zákona o ľudských právach z roku 1998, môže podať návrh na začatie konania proti tomuto orgánu na príslušnom súde alebo tribunáli, resp. sa dovolávať príslušných práv v akomkoľvek súdnom konaní, ak je (alebo by mohol byť) obeťou protiprávneho činu.

(110) Ak súd zistí, že akýkoľvek akt orgánu verejnej moci je nezákonný, môže v rámci svojich právomocí nariadiť akúkoľvek nápravu alebo vydať akýkoľvek príkaz, ktoré považuje za vhodné a primerané ([120]). Súd môže takisto vyhlásiť ustanovenie primárneho práva za nezlučiteľné s právom zaručeným dohovorom.

([115]) Článok 77 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov.

([116]) V § 166 zákona o ochrane údajov z roku 2018 sa konkrétne uvádzajú tieto situácie: a) Komisár pre informácie nepodnikne primerané kroky v reakcii na sťažnosť, b) Komisár pre informácie neposkytne sťažovateľovi informácie o pokroku v súvislosti so sťažnosťou alebo o jej výsledku pred uplynutím 3-mesačnej lehoty, ktorá začína plynúť od prijatia sťažnosti týmto komisárom, alebo c) v prípade, že posúdenie sťažnosti Komisárom pre informácie počas tohto obdobia ešte nie je ukončené, ak neposkytne sťažovateľovi takéto informácie počas nasledujúcich 3 mesiacov.

([117]) Článok 78 ods. 2 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov a § 166 zákona o ochrane údajov z roku 2018.

([118]) Článok 78 ods. 1 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov a § 162 zákona o ochrane údajov z roku 2018.

([119]) § 7 ods. 1 zákona o ľudských právach z roku 1998. Podľa § 7 ods. 7 je osoba obeťou protiprávneho činu len vtedy, ak by bola obeťou na účely článku 34 Európskeho dohovoru o ľudských právach, ak bol v súvislosti s týmto činom podaný návrh na začatie konania na Európskom súde pre ľudské práva.

([120]) § 8 ods. 1 zákona o ľudských právach z roku 1998.

(111) Jednotlivec môže napokon za porušenie práv zaručených Európskym dohovorom o ľudských právach po vyčerpaní vnútroštátnych prostriedkov nápravy dosiahnuť nápravu pred Európskym súdom pre ľudské práva.

3. PRÍSTUP K OSOBNÝM ÚDAJOM PRENÁŠANÝM Z EURÓPSKEJ ÚNIE ORGÁNMI VEREJNEJ MOCI V SPOJENOM KRÁĽOVSTVE A ICH POUŽÍVANIE TÝMITO ORGÁNMI

(112) Komisia posúdila aj právny rámec Spojeného kráľovstva pre získavanie a následné používanie osobných údajov, ktoré prenášajú podnikateľským subjektom v Spojenom kráľovstve orgány verejnej moci Spojeného kráľovstva vo verejnom záujme, a to najmä na účely presadzovania trestného práva a na účely národnej bezpečnosti (ďalej len „prístup vlády“). Komisia pri posudzovaní toho, či by podmienky, na základe ktorých sa vláde poskytuje prístup k údajom prenášaným do Spojeného kráľovstva podľa tohto rozhodnutia, spĺňali kritérium „zásadnej rovnocennosti“ v súlade s článkom 45 ods. 1 nariadenia (EÚ) 2016/679, ako ho vykladá Súdny dvor Európskej únie so zreteľom na Chartu základných práv, zohľadnila najmä tieto kritériá.

(113) Po prvé akékoľvek obmedzenie práva na ochranu osobných údajov musí byť stanovené zákonom a v samotnom právnom základe, ktorý povoľuje zasahovanie do takéhoto práva, sa musí vymedzovať, do akého rozsahu možno uplatňovanie príslušného práva obmedziť ([121]).

(114) Po druhé v záujme splnenia požiadavky proporcionality, podľa ktorej sa v demokratickej spoločnosti musia výnimky z ochrany osobných údajov a obmedzenia ochrany osobných údajov uplatňovať len do prísne nevyhnutnej miery, aby boli splnené konkrétne ciele všeobecného záujmu, ktoré sú rovnocenné s cieľmi uznávanými Úniou, sa v právnych predpisoch dotknutej tretej krajiny povoľujúcich zasahovanie musia stanovovať jasné a presné pravidlá upravujúce rozsah a uplatňovanie takýchto opatrení a zavádzať minimálne záruky, aby osoby, ktorých údaje boli prenesené, mali dostatočné záruky umožňujúce účinne chrániť ich osobné údaje pred rizikom zneužitia ([122]). V týchto právnych predpisoch sa musia najmä vymedziť okolnosti a podmienky, za akých možno prijať opatrenie upravujúce spracúvanie takýchto údajov ([123]), ako aj stanoviť povinnosť podrobiť splnenie takých požiadaviek nezávislému dohľadu ([124]).

(115) Po tretie takéto právne predpisy musia byť právne záväzné podľa vnútroštátneho práva a tieto právne požiadavky musia byť nielen záväzné pre orgány, ale aj vymožiteľné na súdoch proti orgánom dotknutej tretej krajiny ([125]). Dotknuté osoby musia mať najmä možnosť uplatniť právne prostriedky nápravy pred nezávislým a nestranným súdom, aby mali prístup k osobným údajom, ktoré sa ich týkajú, alebo dosiahnuť opravu alebo vymazanie takýchto údajov ([126]).

3.1. **Všeobecný právny rámec**

(116) Prístup vlády ako výkon právomoci orgánu verejnej moci v Spojenom kráľovstve sa musí uskutočňovať v plnom súlade so zákonom. Spojené kráľovstvo ratifikovalo Európsky dohovor o ľudských právach (pozri odôvodnenie 9) a orgány verejnej moci v Spojenom kráľovstve sú povinné konať v súlade s týmto dohovorom ([127]). V článku 8 dohovoru sa stanovuje, že akýkoľvek zásah do súkromného života musí byť v súlade so zákonom, v záujme jedného z cieľov uvedených v článku 8 ods. 2 a primeraný vzhľadom na tento cieľ. V článku 8 sa takisto požaduje, aby bol zásah „predvídateľný“, t. j. aby mal jasný, prístupný základ v zákone, a aby zákon obsahoval primerané záruky na zabránenie zneužitiu.

(117) Európsky súd pre ľudské práva vo svojej judikatúre okrem toho špecifikuje, že akýkoľvek zásah do práva na súkromie a ochranu údajov by mal podliehať účinnému, nezávislému a nestrannému systému dohľadu, ktorý musí zabezpečiť buď sudca, alebo iný nezávislý orgán ([128]) (napr. správny orgán alebo parlamentný orgán).

([121]) Pozri vec Schrems II, body 174 – 175 a citovanú judikatúru. Čo sa týka prístupu orgánov verejnej moci členských štátov, pozri aj vec C-623/17 Privacy International, ECLI:EU:C:2020:790, bod 65; a spojené veci C-511/18, C-512/18 a C-520/18 La Quadrature du Net and Others, ECLI:EU:C:2020:791, bod 175.

([122]) Pozri vec Schrems II, body 176 a 181, ako aj citovanú judikatúru. Pokiaľ ide o prístup orgánov verejnej moci členských štátov, pozri aj vec Privacy International, bod 68; a La Quadrature du Net and Others, bod 132.

([123]) Pozri vec Schrems II, bod 176. Pokiaľ ide o prístup orgánov verejnej moci členských štátov, pozri aj vec Privacy International, bod 68; a La Quadrature du Net and Others, bod 132.

([124]) Pozri vec Schrems II, bod 179.

([125]) Pozri vec Schrems II, body 181 – 182.

([126]) Pozri vec Schrems I, bod 95 a vec Schrems II, bod 194. V tejto súvislosti Súdny dvor Európskej únie zdôraznil najmä to, že dodržiavanie článku 47 Charty základných práv, v ktorom sa zaručuje právo na účinný prostriedok nápravy pred nezávislým a nestranným súdom, „prispieva k úrovni ochrany požadovanej v rámci Únie a […] Komisia [ho musí] konštatovať skôr, než prijme rozhodnutie o primeranosti podľa článku 45 ods. 1 nariadenia“ (EÚ) 2016/679 (vec Schrems II, bod 186).

([127]) § 6 zákona o ľudských právach z roku 1998.

([128]) Európsky súd pre ľudské práva, Klass and others/Nemecko, žaloba č. 5029/71, body 17 – 51.

(118) Navyše sa jednotlivcom musia poskytnúť účinné prostriedky nápravy a Európsky súd pre ľudské práva objasnil, že prostriedky nápravy musí ponúkať nezávislý a nestranný orgán, ktorý prijal svoj vlastný rokovací poriadok, je zložený z členov, ktorí musia zastávať alebo zastávali vysoké sudcovské funkcie alebo sú skúsenými právnikmi, a nesmie existovať žiadne dôkazné bremeno, ktoré treba splniť, aby bolo možné podať na tomto orgáne sťažnosť. Pri preskúmavaní sťažností jednotlivcov by mal mať nezávislý a nestranný orgán prístup ku všetkým relevantným informáciám vrátane uzavretých materiálov. Napokon by mal mať právomoc napraviť nedodržanie právnych predpisov ([129]).

(119) Spojené kráľovstvo v roku 2018 takisto ratifikovalo Dohovor Rady Európy o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (dohovor č. 108) a podpísalo protokol, ktorým sa mení Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (známy ako dohovor č. 108+) ([130]). V článku 9 dohovoru č. 108 sa uvádza, že výnimky zo zásad všeobecnej ochrany údajov (článok 5 Kvalita údajov), z pravidiel upravujúcich osobitné kategórie údajov (článok 6 Osobitné kategórie údajov) a z práv dotknutých osôb (článok 8 Ďalšie záruky pre dotknutú osobu) sú prípustné len vtedy, ak sa takáto výnimka stanovuje vo vnútroštátnom právnom poriadku danej strany a ak predstavuje opatrenie potrebné v demokratickej spoločnosti na ochranu bezpečnosti štátu, verejnej bezpečnosti, menových záujmov štátu alebo potláčanie trestnej činnosti, alebo ochranu dotknutej osoby, alebo práv a slobôd iných ([131]).

(120) Zo skutočnosti, že Spojené kráľovstvo je členom Rady Európy, dodržiava Európsky dohovor o ľudských právach a je podriadené právomoci Európskeho súdu pre ľudské práva, preto preň vyplýva niekoľko povinností zakotvených v medzinárodnom práve, ktoré zasadzujú jeho systém prístupu vlády do rámca založeného na zásadách, zárukách a individuálnych právach podobných tým, ktoré zaručuje právo EÚ a ktoré sa uplatňujú na členské štáty. Ako sa zdôrazňuje v odôvodnení 19, pretrvávajúce dodržiavanie týchto nástrojov je preto mimoriadne dôležitým prvkom posúdenia, na ktorom sa zakladá toto rozhodnutie.

(121) Okrem toho sú osobitné záruky ochrany údajov a práva na ochranu údajov zaručené zákonom o ochrane údajov z roku 2018, keď údaje spracúvajú orgány verejnej moci vrátane orgánov presadzovania práva a národných bezpečnostných orgánov.

(122) Konkrétne režim spracúvania osobných údajov v kontexte presadzovania trestného práva sa stanovuje v časti 3 zákona o ochrane údajov z roku 2018, ktorý bol prijatý na transponovanie smernice (EÚ) 2016/680. Časť 3 zákona o ochrane údajov z roku 2018 sa vzťahuje na spracúvanie osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu ([132]).

(123) Pojem „príslušný orgán“ je vymedzený v § 30 zákona o ochrane údajov z roku 2018 ako osoba uvedená v prílohe 7 k zákonu o ochrane údajov z roku 2018, ako aj akákoľvek iná osoba v rozsahu, v akom má zákonné funkcie na ktorýkoľvek z účelov presadzovania práva ([133]). Ako je to vysvetlené ďalej v texte (pozri odôvodnenie 139), isté príslušné orgány (napríklad Národná kriminálna agentúra) môžu za istých okolností využiť právomoci poskytnuté na základe zákona o vyšetrovacích právomociach z roku 2016 (Investigatory Power Act 2016). V tomto prípade sa záruky stanovené v zákone o vyšetrovacích právomociach z roku 2016 uplatnia popri zárukách stanovených v časti 3 zákona o ochrane údajov z roku 2018. Spravodajské služby (Tajná spravodajská služba, Bezpečnostná služba a Vládne komunikačné ústredie) nie sú „príslušnými orgánmi“ ([134]) patriacimi do rozsahu pôsobnosti časti 3 zákona o ochrane údajov z roku 2018, a preto sa v nej uvedené pravidlá nevzťahujú na žiadnu z ich činností. Konkrétna časť zákona o ochrane údajov z roku 2018 (časť 4) sa venuje spracúvaniu osobných údajov spravodajskými službami (pre podrobnejšie informácie pozri odôvodnenie 125).

([129]) Európsky súd pre ľudské práva, Kennedy/United Kingdom, žaloba č. 26839/05, (ďalej len „Kennedy“), body 167 a 190.

([130]) Viac informácií o Európskom dohovore o ľudských právach a o jeho začlenení do právneho poriadku Spojeného kráľovstva prostredníctvom zákona o ľudských právach z roku 1998, ako aj o dohovore č. 108 sa uvádza v odôvodnení 9.

([131]) Podobne sú v súlade s článkom 11 dohovoru č. 108+ obmedzenia určitých osobitných práv a povinností v rámci dohovoru na účely národnej bezpečnosti alebo predchádzania, vyšetrovania a stíhania trestnej činnosti a výkonu trestných sankcií prípustné len vtedy, ak je takéto obmedzenie stanovené vo vnútroštátnom poriadku, rešpektuje podstatu základných práv a slobôd a predstavuje nevyhnutné a primerané opatrenie v demokratickej spoločnosti. Nezávislému a účinnému preskúmaniu a dohľadu v súlade s vnútroštátnymi právnymi predpismi príslušnej strany dohovoru musia podliehať aj spracovateľské činnosti na účely národnej bezpečnosti a obrany.

([132]) § 31 zákona o ochrane údajov z roku 2018.

([133]) Príslušné orgány uvedené v prílohe 7 nezahŕňajú len policajné zložky, ale aj všetky ministerstvá Spojeného kráľovstva, ako aj iné orgány s vyšetrovacími funkciami [napr. Komisár daňového a colného orgánu jej veličenstva (Commissioner for Her Majesty's Revenue and Customs), Národná kriminálna agentúra (National Crime Agency), Waleský daňový úrad (Welsh Revenue Authority), Úrad pre hospodársku súťaž a trhy (Competition and Markets Authority) alebo Kataster nehnuteľností jej veličenstva (Her Majesty's Land Register)], vyšetrovacie orgány, iné orgány s pôsobnosťou v oblasti trestnej spravodlivosti a ďalšie subjekty alebo organizácie vykonávajúce činnosti v oblasti presadzovania práva (na zozname v prílohe 7 k zákonu o ochrane údajov z roku 2018 sú medzi nimi uvedení aj riaditelia prokuratúry, riaditeľ prokuratúry pre Severné Írsko alebo Komisia pre informácie).

([134]) § 30 ods. 2 zákona o ochrane údajov z roku 2018.

(124) Podobne ako v smernici (EÚ) 2016/680 sa v časti 3 zákona o ochrane údajov z roku 2018 stanovujú zásady zákonnosti a spravodlivosti ([135]), obmedzenia účelu ([136]), minimalizácie údajov ([137]), správnosti ([138]), minimalizácie uchovávania ([139]) a bezpečnosti ([140]). V právnom predpise sa ukladajú osobitné povinnosti týkajúce sa transparentnosti ([141]) a jednotlivcom sa poskytuje právo na prístup ([142]), opravu a vymazanie ([143]) a právo nepodliehať automatizovanému rozhodovaniu ([144]). Od príslušných orgánov sa takisto požaduje, aby vykonávali špecificky navrhnutú a štandardnú ochranu údajov, uchovávali záznamy o spracovateľských činnostiach a v prípade určitých spracovateľských operácií vykonávali posúdenia vplyvu na ochranu údajov a vopred konzultovali s Komisárom pre informácie ([145]). Podľa § 56 zákona o ochrane údajov z roku 2018 sú povinní preukázať súlad. Okrem toho sa od nich požaduje, aby zaviedli primerané opatrenia na zaistenie bezpečnosti spracúvania ([146]) a v prípade porušenia ochrany údajov podliehajú osobitným povinnostiam vrátane oznámenia takéhoto porušenia Komisárovi pre informácie a dotknutým osobám ([147]). Rovnako ako v prípade smernice (EÚ) 2016/680 aj tu sa stanovuje požiadavka, aby prevádzkovateľ (pokiaľ ním nie je súd alebo iný súdny orgán konajúci v rámci súdnej právomoci) vymenoval zodpovednú osobu ([148]), ktorá pomáha prevádzkovateľovi plniť si svoje povinnosti, ako aj monitorovať tento súlad ([149]). V právnom predpise sa okrem toho stanovujú osobitné požiadavky na medzinárodné prenosy osobných údajov do tretích krajín alebo medzinárodným organizáciám na účely presadzovania práva s cieľom zabezpečiť kontinuitu ochrany ([150]). Komisia spolu s týmto rozhodnutím prijala rozhodnutie o primeranosti na základe článku 36 ods. 3 smernice (EÚ) 2016/680, keďže zistila, že režim ochrany údajov platný pre spracúvanie údajov orgánmi Spojeného kráľovstva príslušnými na presadzovanie trestného práva zabezpečuje úroveň ochrany, ktorá v zásade zodpovedá úrovni zaručenej smernicou (EÚ) 2016/680.

(125) Časť 4 zákon o ochrane údajov z roku 2018 sa vzťahuje na každé spracúvanie spravodajskými službami alebo v ich mene. Stanovujú sa v nej hlavné zásady ochrany údajov (zákonnosť, spravodlivosť a transparentnosť ([151]), obmedzenie účelu ([152]), minimalizácia údajov ([153]), správnosť ([154]), minimalizácia uchovávania ([155]) a bezpečnosť ([156])) a zavádzajú sa v nej podmienky spracúvania osobitných kategórií údajov ([157]), stanovujú sa práva dotknutých osôb ([158]), zavádza sa požiadavka špecificky navrhnutej

([135]) § 35 zákona o ochrane údajov z roku 2018.
([136]) § 36 zákona o ochrane údajov z roku 2018.
([137]) § 37 zákona o ochrane údajov z roku 2018.
([138]) § 38 zákona o ochrane údajov z roku 2018.
([139]) § 39 zákona o ochrane údajov z roku 2018.
([140]) § 40 zákona o ochrane údajov z roku 2018.
([141]) § 44 zákona o ochrane údajov z roku 2018.
([142]) § 45 zákona o ochrane údajov z roku 2018.
([143]) § 46 a § 47 zákona o ochrane údajov z roku 2018.
([144]) § 49 a § 50 zákona o ochrane údajov z roku 2018.
([145]) § 56 – 65 zákona o ochrane údajov z roku 2018.
([146]) § 66 zákona o ochrane údajov z roku 2018.
([147]) § 67 – 68 zákona o ochrane údajov z roku 2018.
([148]) § 69 – § 71 zákona o ochrane údajov z roku 2018.
([149]) § 67 – 68 zákona o ochrane údajov z roku 2018.
([150]) Časť 3 kapitola 5 zákona o ochrane údajov z roku 2018.
([151]) Podľa § 86 ods. 6 zákona o ochrane údajov z roku 2018 sa pri určovaní spravodlivosti a transparentnosti spracúvania musí prihliadať na spôsob získavania údajov. V tomto zmysle je požiadavka spravodlivosti a transparentnosti splnená, ak sa údaje získajú od osoby, ktorá je zákonne oprávnená alebo od ktorej sa zákonom vyžaduje, aby ich poskytla.
([152]) Podľa § 87 zákona o ochrane údajov z roku 2018 musia byť účely spracúvania konkrétne určené, výslovne uvedené a legitímne. Údaje sa nesmú spracúvať spôsobom, ktorý nie je zlučiteľný s účelom, na ktorý boli získané. Podľa § 87 ods. 3 zákona o ochrane údajov z roku 2018 možno ďalšie zlučiteľné spracúvanie osobných údajov povoliť len vtedy, ak je prevádzkovateľ zákonom oprávnený spracúvať údaje na tento účel a spracúvanie je nevyhnutné a primerané tomuto inému účelu. Spracúvanie by sa malo považovať za zlučiteľné, ak spracúvanie pozostáva zo spracúvania na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu alebo na štatistické účely a podlieha primeraným zárukám (§ 87 ods. 4 zákona o ochrane údajov z roku 2018).
([153]) Osobné údaje musia byť primerané, relevantné a nie nadmerné (§ 88 zákona o ochrane údajov z roku 2018).
([154]) Osobné údaje musia byť presné a aktuálne (§ 89 zákona o ochrane údajov z roku 2018).
([155]) Osobné údaje sa nesmú uchovávať dlhšie, ako je potrebné (§ 90 zákona o ochrane údajov z roku 2018).
([156]) Šiesta zásada ochrany údajov spočíva v tom, že osobné údaje sa musia spracúvať spôsobom, ktorý zahŕňa prijatie primeraných bezpečnostných opatrení, pokiaľ ide o riziká, ktoré vyplývajú zo spracovania osobných údajov. Riziká zahŕňajú (okrem iného) náhodný alebo neoprávnený prístup k osobným údajom alebo ich zničenie, stratu, použitie, zmenu alebo zverejnenie (§ 91 zákona o ochrane údajov z roku 2018). V § 107 sa takisto vyžaduje, aby 1. každý prevádzkovateľ zaviedol primerané bezpečnostné opatrenia zodpovedajúce rizikám vyplývajúcim zo spracúvania osobných údajov a 2. v prípade automatizovaného spracúvania vykonal každý prevádzkovateľ a každý sprostredkovateľ preventívne alebo zmierňujúce opatrenia založené na hodnotení rizika.
([157]) § 86 ods. 2 písm. b) a príloha 10 k zákonu o ochrane údajov z roku 2018.
([158]) Kapitola 3 časti 4 zákona o ochrane údajov z roku 2018, najmä práva: prístupu, opravy a vymazania, ako aj právo namietať proti spracúvaniu a nepodliehať automatizovanému rozhodovaniu, právo zasahovať do automatizovaného rozhodovania a byť informovaný o tomto rozhodovaní. Okrem toho musí prevádzkovateľ dotknutej osobe poskytnúť informácie o spracovaní jej osobných údajov. Ako je to vysvetlené v usmernení Komisára pre informácie o spracúvaní spravodajskými službami, jednotlivci môžu uplatňovať všetky svoje práva (vrátane žiadosti o opravu) prostredníctvom sťažnosti podanej Komisárovi pre informácie alebo predložením záležitostí súdu (pozri usmernenie Komisára pre informácie o spracúvaní spravodajskými službami, k dispozícii na tomto odkaze https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

ochrany údajov ([159]) a upravujú sa v nej medzinárodné prenosy osobných údajov ([160]). Komisár pre informácie nedávno vydal podrobné usmernenie o spracúvaní údajov spravodajskými službami podľa časti 4 zákona o ochrane údajov z roka 2018 ([161]).

(126) Zároveň sa v § 110 zákona o ochrane údajov z roku 2018 stanovuje výnimka z osobitných ustanovení v časti 4 zákona o ochrane údajov z roku 2018 ([162]), ak je táto výnimka potrebná na zabezpečenie národnej bezpečnosti. Tejto výnimky sa možno dovolávať na základe analýzy jednotlivých prípadov ([163]). Ako vysvetlili orgány Spojeného kráľovstva a potvrdila judikatúra súdov, prevádzkovatelia musia zvážiť skutočné dôsledky pre národnú bezpečnosť alebo obranu, ak mali povinnosť dodržiavať konkrétne ustanovenia o ochrane údajov a ak mohli primerane dodržať toto obvyklé pravidlo bez toho, aby to malo vplyv na národnú bezpečnosť alebo obranu“ ([164]). To, či sa výnimka použila primerane, podlieha dohľadu Komisára pre informácie ([165]).

(127) Okrem toho, pokiaľ ide o možnosť obmedziť uplatňovanie vyššie uvedených ustanovení v záujme ochrany „národnej bezpečnosti“, prevádzkovateľ môže podľa § 111 zákona o ochrane údajov z roku 2018 požiadať o osvedčenie podpísané ministrom vlády alebo generálnym prokurátorom, v ktorom sa potvrdzuje, že obmedzenie takýchto práv je nevyhnutným a primeraným opatrením na ochranu národnej bezpečnosti ([166]).

(128) Vláda Spojeného kráľovstva vydala v rámci zákona o ochrane údajov z roku 2018 usmernenie na pomoc prevádzkovateľom pri zvažovaní, či požiadať o osvedčenie o záujme národnej bezpečnosti, v ktorom sa predovšetkým zdôrazňuje, že akékoľvek obmedzenie práv dotknutých osôb na zaistenie národnej bezpečnosti musí byť primerané a nevyhnutné ([167]). Všetky osvedčenia o záujme národnej bezpečnosti sa musia uverejniť na webovom sídle Komisára pre informácie ([168]).

([159]) § 103 zákona o ochrane údajov z roku 2018.

([160]) § 109 zákona o ochrane údajov z roku 2018. Prenos osobných údajov medzinárodným organizáciám alebo krajinám mimo Spojeného kráľovstva je možný, ak je prenos nevyhnutným a primeraným opatrením vykonávaným na účely zákonných funkcií prevádzkovateľa alebo na iné účely stanovené v osobitných ustanoveniach zákona o bezpečnostných službách z roku 1989 a zákona o spravodajských službách z roku 1994.

([161]) Usmernenie Komisára pre informácie, pozri poznámku pod čiarou č. 158.
§ 30 zákona o ochrane údajov z roku 2018 a príloha 7 k zákonu o ochrane údajov z roku 2018.

([162]) V § 110 ods. 2 zákona o ochrane údajov z roku 2018 sa uvádzajú ustanovenia, z ktorých je povolená výnimka. Zahŕňa zásady ochrany údajov (okrem zásady zákonnosti), práva dotknutých osôb, povinnosť informovať Komisára pre informácie o porušení ochrany údajov, kontrolné právomoci Komisára pre informácie v súlade s medzinárodnými záväzkami, ako aj jeho niektoré právomoci v oblasti presadzovania práva, ustanovenia, na základe ktorých sa určité porušenia ochrany údajov považujú za trestný čin, a ustanovenia týkajúce sa osobitných účelov spracúvania, ako sú žurnalistické, akademické alebo umelecké účely.

([163]) Pozri vec Baker/Secretary of State, pozri poznámku pod čiarou č. 61.

([164]) Vysvetľujúci rámec Spojeného kráľovstva pre diskusiu o primeranosti, oddiel H s názvom „Ochrana údajov v oblasti národnej bezpečnosti a rámec vyšetrovacích právomocí“, s. 15 – 16 (pozri poznámku pod čiarou č. 31). Pozri tiež rozsudok Baker/Secretary of State (pozri poznámku pod čiarou č. 61), v ktorom súd zrušil osvedčenie o záujme národnej bezpečnosti vydané ministerstvom vnútra a potvrdil uplatnenie výnimky týkajúcej sa národnej bezpečnosti vzhľadom na to, že neexistoval dôvod stanoviť paušálnu výnimku týkajúcu sa povinnosti odpovedať na žiadosti o prístup a že umožnenie takejto výnimky za každých okolností bez analýzy jednotlivých prípadov presahovalo rámec toho, čo bolo potrebné a primerané na ochranu národnej bezpečnosti.

([165]) Pozri Memorandum o porozumení medzi Komisárom pre informácie a spravodajskými službami Spojeného kráľovstva, podľa ktorého sa Komisár pre informácie v prípade prijatia sťažnosti od dotknutej osoby bude chcieť uistiť, že v danej otázke sa postupovalo správne a že použitie výnimky bolo v príslušnom prípade náležité. Memorandum o porozumení medzi Úradom Komisára pre informácie a spravodajskými službami Spojeného kráľovstva, bod 16, k dispozícii na tomto odkaze: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf.

([166]) Zákonom o ochrane údajov z roku 2018 bola zrušená možnosť vydať osvedčenie podľa § 28 ods. 2 zákona o ochrane údajov z roku 1998. Možnosť vydania „starých osvedčení“ však stále existuje, a to v rozsahu, v aktom to vyplýva z možnosti, ktorá historicky existuje podľa zákona o ochrane údajov z roku 1998 (pozri bod 17 časti 5 prílohy 20 k zákonu o ochrane údajov z roku 2018). Táto možnosť je však veľmi vzácna a uplatní sa len v obmedzenom počte prípadov, ako napr. keď subjekt údajov napadne uplatnenie výnimky v záujme národnej bezpečnosti vo vzťahu k spracúvaniu zo strany orgánu verejnej moci, ktorý toto spracúvanie uskutočnil na základe zákona o ochrane údajov z roku 1998. Treba poznamenať, že v takýchto prípadoch sa uplatnia všetky ustanovenia § 28 zákona o ochrane údajov z roku 1998, a teda aj ustanovenie umožňujúce subjektu údajov napadnúť príslušné osvedčenie na súde.

([167]) Usmernenie vlády Spojeného kráľovstva k osvedčeniam o záujme národnej bezpečnosti podľa zákona o ochrane údajov z roku 2018, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf. Orgány Spojeného kráľovstva vysvetlili, že hoci je osvedčenie presvedčivým dôkazom toho, že pokiaľ ide o údaje alebo spracúvanie uvedené v osvedčení, výnimka je uplatniteľná, neodstraňuje sa ňou požiadavka, aby prevádzkovateľ zvážil, či je výnimku potrebné uplatňovať v jednotlivých prípadoch.

([168]) Podľa § 130 zákona o ochrane údajov z roku 2018 môže Komisár pre informácie rozhodnúť, že sa nesmie uverejniť znenie určitého osvedčenia, resp. jeho časť, ak by to bolo v rozpore so záujmom národnej bezpečnosti, alebo ak by to bolo inak v rozpore s verejným záujmom, resp. ak by to mohlo ohroziť bezpečnosť ktorejkoľvek osoby. V takýchto prípadoch však Komisár pre informácie uverejní skutočnosť, že takéto osvedčenie bolo vydané.

(129) Osvedčenie by malo mať pevne stanovené obdobie nie dlhšie ako päť rokov, aby ho mohol výkonný orgán pravidelne preskúmavať ([169]). V osvedčení sa uvedú osobné údaje alebo kategórie osobných údajov, na ktoré sa vzťahuje výnimka, ako aj ustanovenia zákona o ochrane údajov z roku 2018, na ktoré sa výnimka vzťahuje ([170]).

(130) Je dôležité poznamenať, že osvedčenia o záujme národnej bezpečnosti nedávajú dodatočný dôvod na to, aby boli obmedzené práva na ochranu údajov z dôvodov národnej bezpečnosti. Inými slovami, prevádzkovateľ alebo sprostredkovateľ sa môže odvolávať na osvedčenie len vtedy, keď dospel k záveru, že je potrebné odvolávať sa na výnimku v záujme národnej bezpečnosti, ktorá, ako už bolo vysvetlené, sa musí uplatňovať v jednotlivých prípadoch ([171]). Aj keď sa na predmetnú vec vzťahuje osvedčenie o záujme národnej bezpečnosti, Komisár pre informácie môže preskúmať, či v konkrétnom prípade bolo uplatnenie výnimky v záujme národnej bezpečnosti odôvodnené ([172]).

(131) Každá osoba, ktorej sa vydanie osvedčenia priamo týka, sa môže proti osvedčeniu ([173]) odvolať na vyšší tribunál (Upper Tribunal) ([174]) alebo, ak sa v osvedčení identifikujú údaje prostredníctvom všeobecného opisu, napadnúť uplatňovanie osvedčenia na konkrétne údaje ([175]). Tribunál preskúma rozhodnutie o vydaní osvedčenia a rozhodne, či existovali opodstatnené dôvody na vydanie tohto osvedčenia ([176]). Môže zohľadniť širokú škálu otázok vrátane nevyhnutnosti, primeranosti a zákonnosti pri zvažovaní vplyvu na práva dotknutých osôb a vyvažovaní potreby zabezpečiť národnú bezpečnosť. V dôsledku toho môže tribunál rozhodnúť, že osvedčenie sa nevzťahuje na konkrétne osobné údaje, ktoré sú predmetom odvolania ([177]).

(132) Iný súbor možných obmedzení sa týka obmedzení, ktoré sa podľa prílohy 11 k zákonu o ochrane údajov z roku 2018 uplatňujú na určité ustanovenia časti 4 zákona o ochrane údajov z roku 2018 ([178]) s cieľom chrániť iné dôležité ciele všeobecného verejného záujmu alebo chránené záujmy, ako napríklad parlamentné výsady, dôvernosť komunikácie medzi advokátom a jeho klientom, vedenie súdnych konaní alebo bojovú účinnosť ozbrojených síl ([179]). Uplatňovanie týchto ustanovení je buď oslobodené pre určité kategórie informácií („výnimky na základe kategórie“), alebo je oslobodené v rozsahu, v akom by uplatňovanie týchto ustanovení mohlo ohroziť chránený záujem („výnimky na základe ujmy“) ([180]). Výnimky na základe ujmy sa môžu uplatniť len vtedy, ak by uplatňovanie uvedených ustanovení o ochrane údajov mohlo byť na ujmu príslušnému osobitnému záujmu. Použitie výnimky musí byť preto vždy odôvodnené odkazom na príslušnú ujmu, ktorá by mohla nastať v konkrétnom prípade. Výnimky na základe kategórie možno uplatniť len v súvislosti so špecifickou, úzko vymedzenou kategóriou

([169]) Usmernenie vlády Spojeného kráľovstva k osvedčeniam o záujme národnej bezpečnosti, bod 15, pozri poznámku pod čiarou č. 167.

([170]) Usmernenie vlády Spojeného kráľovstva k osvedčeniam o záujme národnej bezpečnosti, bod 5, pozri poznámku pod čiarou č. 167.

([171]) Pozri poznámku pod čiarou č. 164.

([172]) V § 102 zákona o ochrane údajov z roku 2018 sa stanovuje, že prevádzkovateľ musí byť schopný preukázať, že splnil požiadavky zákona o ochrane údajov z roku 2018. To znamená, že spravodajská služba by musela Komisárovi pre informácie preukázať, že pri odvolávaní sa na výnimku zvážila osobitné okolnosti prípadu. Komisár pre informácie okrem toho uverejňuje aj záznam o osvedčeniach o záujme národnej bezpečnosti, k dispozícii na tomto odkaze: je k dispozícii na tomto odkaze: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([173]) § 111 ods. 3 zákona o ochrane údajov z roku 2018.

([174]) Vyšší tribunál (Upper Tribunal) je súd príslušný na rozhodovanie o odvolaniach proti rozhodnutiam nižších správnych súdov a má osobitnú právomoc, pokiaľ ide o priame odvolania proti rozhodnutiam určitých vládnych orgánov.

([175]) § 111 ods. 5 zákona o ochrane údajov z roku 2018.

([176]) Vo veci Baker/Secretary of State (pozri poznámku pod čiarou č. 61), tribunál pre informácie zrušil osvedčenie o záujme národnej bezpečnosti vydané ministerstvom vnútra vzhľadom na to, že neexistoval dôvod stanoviť paušálnu výnimku týkajúcu sa povinnosti odpovedať na žiadosti o prístup a že umožnenie takejto výnimky za každých okolností bez analýzy jednotlivých prípadov presahovalo rámec toho, čo bolo potrebné a primerané na ochranu národnej bezpečnosti.

([177]) Usmernenie vlády Spojeného kráľovstva k osvedčeniam o záujme národnej bezpečnosti, bod 25, pozri poznámku pod čiarou č. 167.

([178]) Patria sem: i) zásady ochrany údajov podľa časti 4 s výnimkou požiadavky zákonnosti spracovania podľa prvej zásady a skutočnosti, že spracúvanie musí spĺňať jednu z príslušných podmienok stanovených v prílohách 9 a 10; ii) práva dotknutých osôb a iii) povinnosti týkajúce sa oznamovania porušení Komisárovi pre informácie.

([179]) V časti 4 zákona o ochrane údajov z roku 2018 je stanovený právny rámec, ktorý sa vzťahuje na všetky tipy spracúvania osobných údajov vykonaných spravodajskými službami (a nielen na vykonávanie ich úloh týkajúcich sa národnej bezpečnosti). Preto sa časť 4 vzťahuje aj na prípady, keď spravodajské služby spracúvajú údaje napríklad na účely riadenia ľudských zdrojov, v kontexte sporu alebo v kontexte verejného obstarávania. Obmedzenia uvedené v prílohe 11 sa majú vzťahovať najmä na prípady týchto iných kontextov. Napríklad v kontexte sporu so zamestnancom je možné odvolať sa na obmedzenie na účely „súdneho konania“ alebo v kontexte verejného obstarávania je možné odvolať sa na obmedzenie na účely „rokovania“ atď. Odráža sa to aj v usmernení Komisára pre informácie o spracúvaní údajov spravodajskými službami, v ktorom sa ako príklad uplatňovania obmedzení uvedených v prílohe 11 uvádza rokovanie o dohode medzi spravodajskou službou a bývalým zamestnancom, ktorý si uplatňuje zamestnanecký nárok (pozri poznámku pod čiarou č. 161). Treba uviesť aj to, že rovnaké obmedzenia sú podľa časti 2 prílohy 2 k zákonu o ochrane údajov z roku 2018 dostupné pre ostatné verejné orgány.

([180]) Podľa vysvetľujúceho rámca Spojeného kráľovstva medzi „výnimky na základe kategórie“ patria: i) informácie o udelení čestných titulov koruny (Crown honours and dignities); ii) dôvernosť komunikácie medzi advokátom a jeho klientom; iii) dôverné údaje o zamestnaní, odbornej príprave alebo vzdelávaní a iv) odpovede v písomných skúškach a známky zo skúšok. „Výnimky na základe ujmy“ sa týkajú týchto záležitostí: i) predchádzanie trestnej činnosti alebo jej odhaľovanie, zadržanie a trestné stíhanie páchateľov; ii) parlamentné výsady; iii) súdne konania; iv) bojová účinnosť ozbrojených síl koruny; v) hospodársky blahobyt Spojeného kráľovstva; vi) rokovania s dotknutou osobou; vii) vedecký alebo historický výskum alebo štatistické účely; viii) archivácia vo verejnom záujme. Vysvetľujúci rámec Spojeného kráľovstva pre diskusiu o primeranosti, oddiel H s názvom National Security (Národná bezpečnosť), s. 13 (pozri poznámku pod čiarou č. 31).

informácií, pre ktorú sa výnimka udeľuje. Z hľadiska účelu a účinku sú podobné niekoľkým výnimkám zo všeobecného nariadenia Spojeného kráľovstva o ochrane údajov (podľa prílohy 2 k zákonu o ochrane údajov z roku 2018), ktoré zase odrážajú výnimky stanovené v článku 23 všeobecného nariadenia o ochrane údajov.

(133) Z uvedeného vyplýva, že obmedzenia a podmienky sú zavedené podľa platných právnych predpisov Spojeného kráľovstva, a to aj v zmysle ich výkladu súdmi a Komisie pre informácie, aby sa zabezpečilo, že tieto obmedzenia a výnimky zostanú v medziach toho, čo je nevyhnutné a primerané na ochranu národnej bezpečnosti.

3.2. **Prístup k osobným údajom a ich používanie zo strany orgánov verejnej moci Spojeného kráľovstva na účely presadzovania trestného práva**

(134) Právne predpisy Spojeného kráľovstva ukladajú niekoľko obmedzení prístupu k osobným údajom a ich používania na účely presadzovania trestného práva a v tejto oblasti poskytujú mechanizmy dohľadu a nápravy, ktoré sú v súlade s požiadavkami uvedenými v odôvodneniach 113 až 115 tohto rozhodnutia. Podmienky, za ktorých sa takýto prístup môže uskutočniť, a záruky, ktoré sa vzťahujú na uplatnenie týchto právomocí, sa podrobne posudzujú v nasledujúcich oddieloch.

3.2.1. *Právne základy a uplatniteľné obmedzenia/záruky*

(135) Podľa zásady zákonnosti zaručenej podľa § 35 zákona o ochrane údajov z roku 2018 je spracúvanie osobných údajov na ktorýkoľvek z účelov presadzovania práva zákonné len vtedy, ak je založené na zákone a dotknutá osoba vyjadrila súhlas so spracúvaním na tento účel ([181]) alebo ak je spracúvanie nevyhnutné na splnenie úlohy, ktorú na tento účel vykonáva príslušný orgán.

3.2.1.1. Príkazy na domovú prehliadku a príkazy na predloženie dôkazov

(136) V právnom rámci Spojeného kráľovstva je získavanie osobných údajov od podnikateľských subjektov vrátane tých, ktoré by spracúvali údaje prenášané z EÚ podľa tohto rozhodnutia o primeranosti, prípustné na účely presadzovania trestného práva, a to na základe príkazov na domovú prehliadku ([182]) a príkazov na predloženie dôkazov ([183]).

(137) Príkazy na domovú prehliadku vydáva súd obvykle na žiadosť vyšetrovateľa. Umožňujú vyšetrovateľovi vstup do priestorov s cieľom prehľadať ich v snahe nájsť materiály alebo osoby, ktoré sú relevantné pre jeho vyšetrovanie, a zadržať všetko, na čo sa vzťahuje povolenie prehliadky vrátane akýchkoľvek relevantných dokumentov alebo materiálov obsahujúcich osobné údaje ([184]). Podľa príkazu na predloženie dôkazov, ktorý takisto musí vydať súd, musí osoba, ktorá je v ňom uvedená, predložiť materiál, ktorý vlastní alebo má pod kontrolou, alebo poskytnúť k nemu prístup. Žiadateľ musí súdu zdôvodniť, prečo je príkaz nevyhnutný, ako aj dôvod, prečo je to vo verejnom záujme. Existuje viacero zákonom stanovených právomocí, na základe ktorých je možné vydávať príkazy na domovú prehliadku a príkazy na predloženie dôkazov. Každé

([181]) V prípade scenára primeranosti využívanie súhlasu nie je podľa všetkého relevantné, keďže v prípade prenosu údaje od dotknutej osoby v EÚ nebude na základe súhlasu priamo získavať orgán presadzovania práva Spojeného kráľovstva.

([182]) Pokiaľ ide o príslušný právny základ, pozri § 8 a nasl. zákona o polícii a dôkazoch v trestných veciach z roku 1984 (PACE) pre Anglicko a Wales, § 10 a nasl. nariadenia o polícii a dôkazoch v trestných veciach z roku 1989 (Police and Criminal Evidence Order) pre Severné Írsko a v prípade Škótska ho stanovuje common law [pozri § 46 trestného zákona z roku 2016 (Criminal Justice Act) pre Škótsko] a § 23B škótskeho trestného práva (Criminal Law) (konsolidácia). Právny základ v prípade príkazu na domovú prehliadku vydaného po zatknutí tvorí § 18 zákona o polícii a dôkazoch v trestných veciach z roku 1984 (pre Anglicko a Wales), § 20 a nasl. nariadenia (Severného Írska) o polícii a dôkazoch v trestných veciach z roku 1989 a v prípade Škótska ho stanovuje common law [pozri § 46 trestného zákona (Škótska) z roku 2016]. Orgány Spojeného kráľovstva upresnili, že príkaz na domovú prehliadku vydáva súd na žiadosť vyšetrovateľa. Umožňujú vyšetrovateľovi vstup do priestorov s cieľom prehľadať ich v snahe nájsť materiály alebo osoby, ktoré sú relevantné pre jeho vyšetrovanie; vykonanie príkazu si často bude vyžadovať pomoc policajného strážnika (constable).

([183]) Ak sa vyšetrovanie týka legalizácie príjmu z trestnej činnosti (vrátane konfiškácie a občianskoprávneho konania o vymáhaní), relevantným právnym základom pre žiadosť o príkaz na predloženie dôkazov je § 345 a nasl. v prípade Anglicka, Walesu a Severného Írska a § 380 a nasl. zákona o príjmoch z trestnej činnosti z roku 2002 (Proceeds of Crime Act) v prípade Škótska. Ak sa vyšetrovanie týka iných oblastí ako legalizácie príjmu z trestnej činnosti, žiadosť o príkaz na predloženie dôkazov možno podať podľa § 9 zákona o polícii a dôkazoch v trestných veciach z roku 1984 pre Anglicko a Wales a prílohy 1 k nemu a § 10 a nasl. nariadenia (Severného Írska) o polícii a dôkazoch v trestných veciach z roku 1989 pre Severné Írsko. V prípade Škótska sa získava podľa common law [pozri § 46 trestného zákona (Škótska) z roku 2016 a § 23B trestného práva (konsolidácia) (Škótska)]. Orgány Spojeného kráľovstva upresnili, že podľa príkazu na predloženie dôkazov je osoba, ktorá je v ňom uvedená, povinná predložiť materiál, ktorý vlastní alebo má pod kontrolou, alebo poskytnúť k nemu prístup (pozri bod 4 prílohy 1 k zákonu o polícii a dôkazoch v trestných veciach z roku 1984).

([184]) Napríklad zákon o polícii a dôkazoch v trestných veciach z roku 1984 v § 8 a § 18 obsahuje právomoci zaistiť a zadržať všetko, na čo sa vzťahuje povolenie prehliadky.

ustanovenie zahŕňa svoj vlastný súbor zákonných podmienok, ktoré musia byť splnené na to, aby bol príkaz na domovú prehliadku ([185]) alebo príkaz na predloženie dôkazov ([186]) vydaný.

(138) Príkazy na predloženie dôkazov a príkazy na domovú prehliadku možno napadnúť prostredníctvom súdneho preskúmania ([187]). Pokiaľ ide o záruky, všetky orgány príslušné na presadzovanie trestného práva, ktoré patria do rozsahu pôsobnosti časti 3 zákona o ochrane údajov z roku 2018, môžu získať prístup k osobným údajom – čo je forma spracúvania – len v súlade so zásadami a s požiadavkami stanovenými

([185]) Napríklad § 8 a 18 zákona o polícii a dôkazoch v trestných veciach upravujú právomoc zmierovacieho sudcu povoliť príkaz a príslušníka policajného zboru vykonať prehliadku nehnuteľnosti. V prvom prípade (§ 8) sa musí zmierovací sudca pred vydaním príkazu najprv presvedčiť, že existujú opodstatnené dôvody domnievať sa, že: i) bol spáchaný žalovateľný trestný čin; ii) v priestoroch sa nachádza materiál, ktorý má pravdepodobne pre vyšetrovanie trestného činu značnú hodnotu (či už samotný, alebo spolu s inými materiálmi); iii) materiál pravdepodobne bude relevantným dôkazom; iv) neobsahuje ani nezahŕňa položky, na ktoré sa vzťahuje povinnosť advokáta zachovávať mlčanlivosť, vylúčený materiál alebo materiál, na ktorý sa vzťahuje osobitný postup; a v) bez použitia príkazu by nebolo možné vstup získať. V druhom prípade sa § 18 umožňuje príslušníkovi policajného zboru prehľadať priestory osoby zatknutej za žalovateľný trestný čin pre iný materiál ako materiál, na ktorý sa vzťahuje povinnosť advokáta zachovávať mlčanlivosť, ak má odôvodnené podozrenie, že sa v priestoroch nachádzajú dôkazy, ktoré sa týkajú tohto trestného činu alebo iného podobného alebo súvisiaceho žalovateľného trestného činu. Takáto prehliadka sa musí obmedziť na odhalenie tohto materiálu a musí byť písomne povolená príslušníkom policajného zboru aspoň s hodnosťou inšpektora (inspector), pokiaľ to nie je na vyšetrovanie trestného činu nevyhnutné. V takom prípade je nutné čo najskôr po jej vykonaní informovať príslušníka policajného zboru aspoň s hodnosťou inšpektora. Je potrebné zaznamenať dôvody prehliadky a povahu hľadaných dôkazov. Okrem toho sa v § 15 a § 16 zákona o polícii a dôkazoch v trestných veciach z roku 1984 poskytujú zákonné záruky, ktoré sa pri podávaní žiadosti o vydanie príkazu na domovú prehliadku musia dodržiavať. V § 15 sa stanovujú požiadavky, ktoré sa vzťahujú na získanie príkazu na domovú prehliadku [vrátane obsahu žiadosti podanej strážnikom (constable) a skutočnosti, že v príkaze na domovú prehliadku sa musí okrem iného uviesť zákonné ustanovenie, na základe ktorého sa vydáva, a, pokiaľ je to možné, uviesť predmety a osoby, ktoré sa majú hľadať, a priestory, ktoré sa majú prehľadávať]. V § 16 sa upravuje, ako sa musí prehliadka na základe príkazu vykonať (napríklad: v § 16 ods. 5 sa stanovuje, že príslušník policajného zboru vykonávajúci príkaz predloží používateľovi priestorov kópiu príkazu; v § 16 ods. 11 sa stanovuje povinnosť uchovávať príkaz počas obdobia 12 mesiacov po jeho vykonaní; v § 16 ods. 12 sa stanovuje, že používateľ priestorov má počas tohto obdobia právo nahliadnuť do príkazu, ak si to želá). Tieto § pomáhajú zabezpečiť súlad s článkom 8 EDĽP (pozri napríklad Kent Pharmaceuticals/Director of the Serious Fraud Office [2002] EWHC 3023 (QB) at [30] by Lord Woolf CJ). Nedodržanie týchto záruk môže viesť k tomu, že sa prehliadka vyhlási za nezákonnú [napríklad R (Brook)/Preston Crown Court [2018] EWHC 2024 (Admin), [2018] ACD 95; R (Superior Import/Export Ltd)/Revenue and Customs Commissioners [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115 a R (F)/Blackfriars Crown Court [2014] EWHC 1541 (Admin)]. § 15 a § 16 zákona o polícii a dôkazoch v trestných veciach z roku 1984 sú doplnené kódexom B zákona o polícii a dôkazoch v trestných veciach, čo je kódex postupov, ktorým sa upravuje výkon policajných právomocí pri prehliadke priestorov.

([186]) Napríklad pri vydávaní príkazov na predloženie dôkazov podľa zákona o príjmoch z trestnej činnosti z roku 2002 by okrem nutnosti existencie opodstatnených dôvodov na splnenie podmienok stanovených v § 346 ods. 2 zákona o príjmoch z trestnej činnosti mali existovať opodstatnené dôvody domnievať sa, že daná osoba vlastní alebo má pod kontrolou takto špecifikovaný materiál a že materiál pravdepodobne má značnú hodnotu. Okrem toho ďalšou požiadavkou na vydanie príkazu na predloženie dôkazov je, že musia existovať opodstatnené dôvody domnievať sa, že je vo verejnom záujme, aby sa materiál predložil alebo aby sa k nemu poskytol prístup so zreteľom na a) pravdepodobný prínos pre vyšetrovanie v prípade, že sa materiál získa; a b) okolnosti, za ktorých osoba uvedená v žiadosti ako osoba, ktorá podľa všetkého vlastní alebo má pod kontrolou materiál, ktorý obsahuje informácie. Podobne sa musí súd, ktorý zvažuje žiadosť o príkaz na predloženie dôkazov podľa prílohy 1 k zákonu o polícii a dôkazoch v trestných veciach z roku 1984, presvedčiť, že sú splnené osobitné podmienky. V prílohe 1 k zákonu o polícii a dôkazoch v trestných veciach sa stanovujú najmä dva samostatné alternatívne súbory podmienok, z ktorých jeden musí byť splnený predtým, než sudca vydá príkaz na predloženie dôkazov. Podľa prvého súboru sa vyžaduje, aby sudca mal opodstatnené dôvody domnievať sa že i) bol spáchaný žalovateľný trestný čin; ii) materiál hľadaný v priestoroch je materiálom, na ktorý sa vzťahuje osobitný postup alebo je jeho súčasťou, ale nie je vylúčeným materiálom; iii) má pravdepodobne pre vyšetrovanie trestného činu značnú hodnotu, či už samotný, alebo spolu s inými materiálmi; iv) a pravdepodobne bude relevantným dôkazom; v) sa vykonali pokusy získať materiál iným spôsobom alebo sa pokusy nevykonali, pretože nemohli byť úspešné; a vi) po zvážení prínosu pre vyšetrovanie a okolností, za ktorých ho daná osoba vlastní, je vo verejnom záujme, aby sa materiál predložil alebo aby sa k nemu poskytol prístup. Podľa druhého súboru podmienok sa vyžaduje toto: i) v priestoroch sa nachádza materiál, na ktorý sa vzťahuje osobitný postup, alebo vylúčený materiál; ii) keby nebolo zákazu prehliadok vykonávaných na základe právnych predpisov prijatých pred zákonom o polícii a dôkazoch v trestných veciach pre osobitný postup, vylúčený materiál alebo materiál, na ktorý sa vzťahuje povinnosť advokáta zachovávať mlčanlivosť, mohol byť vydaný príkaz na domovú prehliadku s cieľom nájsť materiál; a iii) bolo by vhodné takto postupovať.

([187]) Súdne preskúmanie je právny postup, ktorým možno napadnúť rozhodnutia verejného orgánu na Vrchnom súde. Súdy „preskúmajú" napadnuté rozhodnutie a rozhodnú, či s prihliadnutím na koncepcie/zásady verejného práva možno rozhodnutie dôvodne považovať za protiprávne. Základnými dôvodmi súdneho preskúmania je predovšetkým nezákonnosť, nelogickosť, nesprávny postup, oprávnené očakávanie a ľudské práva. Na základe kladného výsledku súdneho preskúmania môže súd nariadiť niekoľko rôznych prostriedkov nápravy; najbežnejším z nich je príkaz na zrušenie (ktorým by sa zrušilo pôvodné rozhodnutie – t. j. rozhodnutie o vydaní príkazu na domovú prehliadku), za určitých okolností to môže zahŕňať aj priznanie finančnej náhrady. Ďalšie podrobnosti o súdnom preskúmaní v Spojenom kráľovstve sú k dispozícii v usmerneniach k správnemu rozhodovaniu s názvom „Judge Over Your Shoulder – a guide to good decision-making", ktoré uverejňuje právne oddelenie vlády a sú k dispozícii na nasledujúcom odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf.

v zákone o ochrane údajov z roku 2018 (pozri odôvodnenia 122 a 124). Žiadosť podaná ktorýmkoľvek orgánom presadzovania práva by preto mala byť v súlade so zásadou, podľa ktorej musia byť účely spracúvania konkrétne určené, výslovne uvedené a legitímne ([188]) a osobné údaje spracúvané príslušným orgánom musia byť na tento účel relevantné a nie nadmerné ([189]).

3.2.1.2. Vyšetrovacie právomoci na účely presadzovania práva

(139) Na účely predchádzania len závažným trestným činom alebo ich odhaľovania ([190]) môžu niektoré orgány presadzovania práva, napríklad Národná kriminálna agentúra alebo policajný prezident ([191]), využiť cielené vyšetrovacie právomoci podľa zákona o vyšetrovacích právomociach z roku 2016. V tomto prípade sa záruky stanovené v zákone o vyšetrovacích právomociach z roku 2016 uplatnia popri zárukách stanovených v časti 3 zákona o ochrane údajov z roku 2018. Konkrétne vyšetrovacie právomoci, na ktoré sa uvedené orgány presadzovania práva môžu spoľahnúť, sú: cielené zachytávanie (časť 2 zákona o vyšetrovacích právomociach z roku 2016), získavanie údajov o komunikácii (časť 3 zákona o vyšetrovacích právomociach z roku 2016), uchovávanie údajov o komunikácii (časť 4 zákona o vyšetrovacích právomociach z roku 2016) a cielené zasahovanie do zariadení (časť 5 zákona o vyšetrovacích právomociach z roku 2016). Zachytávanie zahŕňa získavanie obsahu komunikácie ([192]), zatiaľ čo získavanie a uchovávanie údajov o komunikácii nie je zamerané na získanie obsahu komunikácie, ale na informácie o tom, „kto“, „kedy“, „kde“ a „ako“ sa na komunikácii zúčastnil. Tieto informácie zahŕňajú napríklad čas a trvanie komunikácie, telefónne číslo alebo e-mailovú adresu odosielateľa a príjemcu komunikácie a niekedy polohu zariadení, z ktorých sa komunikácia uskutočnila, predplatiteľa telefónnej služby alebo účet s rozpísanými položkami ([193]). Zasahovanie do zariadení predstavuje súbor postupov používaných na získanie rôznych údajov zo zariadení, medzi ktoré patria počítače, tablety a smartfóny, ako aj káble, elektrické rozvody a pamäťové zariadenia ([194]).

(140) Právomoci v oblasti cieleného zachytávania sa môžu použiť aj vtedy, keď je to „nevyhnutné na účely vykonania ustanovení nástroja vzájomnej pomoci EÚ alebo medzinárodnej dohody o vzájomnej pomoci“ (tzv. príkaz na vzájomnú pomoc ([195])). Príkazy na vzájomnú pomoc sú k dispozícii len v súvislosti so zachytávaním, nie so získavaním údajov o komunikácii ani so zasahovaním do zariadení. Tieto cielené právomoci sú upravené aj zákonom o vyšetrovacích právomociach z roku 2016 ([196]), ktorým sa spolu so zákonom o regulácii vyšetrovacích právomocí z roku 2000 (Regulation of Investigatory Powers Act) pre Anglicko, Wales a Severné Írsko a zákonom (Škótska) o regulácii vyšetrovacích právomocí z roku 2000 pre Škótsko poskytuje právny základ a stanovujú uplatniteľné obmedzenia a záruky pre využívanie takýchto právomocí. Zákonom o vyšetrovacích právomociach z roku 2016 sa stanovuje režim využívania hromadných vyšetrovacích právomocí, hoci tieto právomoci nie sú k dispozícii orgánom presadzovania práva (využívať ich môžu len spravodajské služby) ([197]).

([188]) § 36 ods. 1 zákona Spojeného kráľovstva o ochrane údajov z roku 2018.

([189]) § 37 zákona Spojeného kráľovstva o ochrane údajov z roku 2018.

([190]) V § 263 ods. 1 zákona o vyšetrovacích právomociach z roku 2016 sa stanovuje, že „závažný trestný čin“ je trestný čin, pri ktorom možno odôvodnene očakávať, že dospelá osoba, ktorá dosiaľ nebola odsúdená, bude odsúdená na trest odňatia slobody na tri roky alebo viac, alebo čin, ktorý zahŕňa použitie násilia, má za následok značný finančný zisk alebo ho vykonal veľký počet osôb. Okrem toho na účely získavania údajov o komunikácii podľa časti 4 zákona o vyšetrovacích právomociach z roku 2016 sa v § 87 ods. 10B stanovuje, že „závažný trestný čin“ je trestný čin, za ktorý možno uložiť trest odňatia slobody na 12 mesiacov alebo viac, alebo trestný čin spáchaný osobou, ktorá nie je fyzickou osobou, alebo ktorý zahŕňa ako svoju neoddeliteľnú súčasť odoslanie komunikácie alebo narušenie súkromia dotknutej osoby.

([191]) O príkaz na cielené zachytávanie môžu požiadať predovšetkým tieto orgány presadzovania práva: generálny riaditeľ Národnej kriminálnej agentúry (National Crime Agency), komisár metropolitnej polície (Commissioner of Police of the Metropolis), náčelník policajného zboru Severného Írska (Chief Constable of the Police Service of Northern Ireland), náčelník policajného zboru Škótska (Chief Constable of the Police Service of Scotland), Komisár daňového a colného orgánu jej veličenstva, vedúci Obrannej spravodajskej služby (Chief of Defence Intelligence) a subjekt, ktorý je príslušným orgánom krajiny alebo územia mimo Spojeného kráľovstva na účely nástroja vzájomnej pomoci EÚ alebo medzinárodnej dohody o vzájomnej pomoci (§ 18 ods. 1 zákona o vyšetrovacích právomociach z roku 2016).

([192]) Pozri § 4 zákona o vyšetrovacích právomociach z roku 2016.

([193]) Pozri § 261 ods. 5 zákona o vyšetrovacích právomociach z roku 2016 a Kódex postupov pre hromadné získavanie údajov o komunikácii, ktorý je k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, bod 2.9.

([194]) Kódex postupov pre zasahovanie do zariadení, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, bod 2.2.

([195]) Príkaz na vzájomnú pomoc oprávňuje orgán Spojeného kráľovstva poskytnúť pomoc orgánu mimo územia Spojeného kráľovstva pri zachytávaní a poskytovaní zachyteného materiálu takémuto orgánu v súlade s medzinárodným nástrojom vzájomnej pomoci (§ 15 ods. 4 zákona o vyšetrovacích právomociach z roku 2016).

([196]) Zákonom o vyšetrovacích právomociach z roku 2016 (pozri: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) sa nahradili jednotlivé právne predpisy týkajúce sa zachytávania komunikácie, zasahovania do zariadení a získavania údajov o komunikácii, najmä časť I zákona o regulácii vyšetrovacích právomocí z roku 2000, ktorou sa stanovil predchádzajúci všeobecný legislatívny rámec pre uplatňovanie vyšetrovacích právomocí orgánmi presadzovania práva a národnými bezpečnostnými orgánmi.

([197]) § 138 ods. 1, § 158 ods. 1, § 178 ods. 1, § 199 ods. 1 zákona o vyšetrovacích právomociach z roku 2016.

(141) Orgány, aby mohli vykonávať tieto právomoci, musia získať príkaz ([198]) vydaný príslušným orgánom ([199]) a schválený nezávislým Komisárom pre justíciu ([200]) (tzv. postup dvojitého zabezpečenia). Získanie takéhoto príkazu podlieha overeniu kritéria nevyhnutnosti a proporcionality ([201]). Keďže tieto cielené vyšetrovacie právomoci, ktoré stanovuje zákon o vyšetrovacích právomociach z roku 2016, sú rovnaké ako tie, ktoré majú k dispozícii národné bezpečnostné služby, podmienky, obmedzenia a záruky uplatniteľné na takéto právomoci sú podrobnejšie rozobraté v oddiele o prístupe k osobným údajom a ich používaní zo strany orgánov verejnej moci Spojeného kráľovstva na účely národnej bezpečnosti (pozri odôvodnenia 177 a ďalšie).

3.2.2. *Ďalšie používanie získaných informácií*

(142) Poskytovanie údajov orgánom presadzovania práva inému orgánu na iné účely ako tie, na ktoré boli pôvodne získané (tzv. následné poskytnutie) podlieha určitým podmienkam.

(143) Podobne ako v článku 4 ods. 2 smernice (EÚ) 2016/680 sa aj § 36 ods. 3 zákona o ochrane údajov z roku 2018 umožňuje, aby sa osobné údaje získané príslušným orgánom na účely presadzovania práva mohli ďalej spracúvať (či už pôvodným prevádzkovateľom alebo iným prevádzkovateľom) na akýkoľvek iný účel presadzovania práva za predpokladu, že prevádzkovateľ je zo zákona oprávnený spracúvať údaje na tento iný účel a predmetné spracovanie je daný účel nevyhnutné a primerané ([202]). V takom prípade sa na spracúvanie vykonávané prijímajúcim orgánom uplatnia všetky záruky stanovené v časti 3 zákona o ochrane údajov z roku 2018 uvedené v odôvodneniach 122 a 124.

(144) V právnom poriadku Spojeného kráľovstva výslovne umožňujú takéto následné poskytovanie údajov rôzne právne predpisy. Predovšetkým v i) zákone o digitálnom hospodárstve z roku 2017 (Digital Economy Act) sa umožňuje vzájomné poskytovanie údajov medzi orgánmi verejnej moci na viaceré účely, napríklad v prípade akéhokoľvek podvodu voči verejnému sektoru, ktorý by zahŕňal ujmu alebo hrozbu ujmy pre orgány verejnej moci ([203]), resp. v prípade dlhu voči orgánu verejnej moci alebo korune ([204]); v ii) zákone o trestnej činnosti a súdoch z roku 2013 sa umožňuje poskytovanie informácií Národnej kriminálnej agentúre ([205]) na účely boja proti závažnej a organizovanej trestnej činnosti, jej vyšetrovania a stíhania; v iii) zákone o závažnej trestnej činnosti z roku 2007 sa umožňuje orgánom verejnej moci sprístupňovať informácie organizáciám na boj proti podvodom na účely predchádzania podvodom ([206]).

(145) V týchto právnych predpisoch sa výslovne stanovuje, že poskytnutie informácií by sa malo uskutočniť v súlade so zásadami stanovenými v zákone o ochrane údajov z roku 2018. Okrem toho policajná akadémia College of Policing vydala autorizovanú profesijnú prax poskytovania informácií ([207]) s cieľom pomôcť polícii pri plnení jej povinností v oblasti ochrany údajov podľa

([198]) V časti 2 kapitole 2 zákona o vyšetrovacích právomociach z roku 2016 sa stanovuje obmedzený počet prípadov, keď možno zachytávanie vykonávať bez príkazu. Patrí sem: zachytávanie so súhlasom odosielateľa alebo príjemcu, zachytávanie na administratívne účely alebo na účely presadzovania práva, zachytávanie v určitých zariadeniach (vo väzniciach, v psychiatrických liečebniach a zariadeniach učených na zaistenie cudzincov), ako aj zachytávanie v súlade s príslušnou medzinárodnou dohodou.

([199]) Vo väčšine prípadov je orgánom, ktorý vydáva príkazy podľa zákona o vyšetrovacích právomociach z roku 2016, minister. Zatiaľ čo škótski ministri sú splnomocnení vydávať príkazy na cielené zachytávanie, príkazy na vzájomnú pomoc a príkazy na cielené zasahovanie do zariadení, ak sa osoby alebo priestory, kde sa má zachytávanie vykonávať, a zariadenie, do ktorého sa má zasahovať, nachádzajú v Škótsku (pozri § 22 a § 103 zákona o vyšetrovacích právomociach z roku 2016). V prípade cieleného zasahovania do zariadení môže vedúci orgánu presadzovania práva (ako sa uvádza v časti 1 a časti 2 prílohy 6 k zákonu o vyšetrovacích právomociach z roku 2016) vydať príkaz za podmienok stanovených v § 106 zákona o vyšetrovacích právomociach z roku 2016.

([200]) Komisári pre justíciu pomáhajú Komisárovi pre vyšetrovacie právomoci, nezávislému orgánu, ktorý vykonáva funkcie dohľadu nad používaním vyšetrovacích právomocí spravodajskými službami (podrobnejšie v odôvodnení 162 a nasl.).

([201]) Pozri najmä § 19 a 23 zákona o vyšetrovacích právomociach z roku 2016.

([202]) § 36 ods. 3 zákona o ochrane údajov z roku 2018.

([203]) § 56 zákona o digitálnom hospodárstve z roku 2017, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2017/30/section/56.

([204]) § 48 zákona o digitálnom hospodárstve z roku 2017.

([205]) § 7 zákona o trestnej činnosti a súdoch z roku 2013, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2013/22/section/7.

([206]) § 68 zákona o závažnej trestnej činnosti z roku 2007, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2007/27/contents.

([207]) Autorizovaná profesijná prax poskytovania informácií, k dispozícii na tomto odkaze: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, zákona o ochrane osobných údajov a zákona o ľudských právach Spojeného kráľovstva z roku 1998. Súlad poskytnutia údajov s uplatniteľným právnym rámcom na ochranu údajov samozrejme podlieha súdnemu preskúmaniu ([208]).

(146) Okrem toho, podobne ako v článku 9 smernice (EÚ) 2016/680, sa v zákone o ochrane údajov z roku 2018 stanovuje, že osobné údaje získané na akýkoľvek účel presadzovania práva sa môžu spracúvať na účel, ktorý nie je presadzovaním práva, ak je spracúvanie povolené zákonom ([209]).

(147) Tento typ poskytovania zahŕňa dva scenáre: 1. ak orgán presadzovania trestného práva poskytuje údaje orgánu na presadzovanie iného práva, ako je trestné právo, ktorý nie je spravodajskou službou (napr. finančný alebo daňový orgán, orgán na ochranu hospodárskej súťaže, úrad starostlivosti o mládež); 2. ak orgán presadzovania trestného práva poskytuje údaje spravodajskej službe. V prvom scenári bude spracúvanie osobných údajov patriť do rozsahu pôsobnosti všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, ako aj do časti 2 zákona o ochrane údajov z roku 2018. Komisia posúdila záruky stanovené vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov a v časti 2 zákona o ochrane údajov z roku 2018 v odôvodneniach 12 až 111 a dospela k záveru, že Spojené kráľovstvo zabezpečuje primeranú úroveň ochrany osobných údajov prenášaných v rámci rozsahu pôsobnosti nariadenia (EÚ) 2016/679 z Európskej únie do Spojeného kráľovstva.

(148) V druhom scenári, teda pokiaľ ide o poskytovanie údajov získaných orgánom presadzovania trestného práva spravodajskej službe na účely národnej bezpečnosti, je právnym základom, ktorý umožňuje takéto poskytnutie, § 19 zákona o boji proti terorizmu z roku 2008 ([210]). Podľa tohto zákona môže každá osoba poskytnúť informácie ktorejkoľvek zo spravodajských služieb na účely plnenia ktorejkoľvek z funkcií tejto služby vrátane „národnej bezpečnosti“.

(149) Pokiaľ ide o podmienky, za ktorých sa údaje môžu poskytnúť na účely národnej bezpečnosti, zákon o spravodajských službách ([211]) a zákon o bezpečnostných službách ([212]) obmedzujú schopnosť spravodajských služieb získavať údaje na to, čo je nevyhnutné na plnenie ich zákonných funkcií. Orgány presadzovania práva, ktoré chcú poskytnúť údaje spravodajským službám, musia okrem funkcií týchto služieb, ktoré sú stanovené v zákone o spravodajských službách a v zákone o bezpečnostných službách, zvážiť niekoľko faktorov/obmedzení ([213]). V § 20 zákona o boji proti terorizmu z roku 2008 sa jasne uvádza, že akékoľvek poskytnutie údajov podľa § 19 musí byť stále v súlade s právnymi predpismi o ochrane údajov; čo znamená, že sa uplatňujú všetky obmedzenia a požiadavky uvedené v časti 3 zákona o ochrane údajov z roku 2018. Keďže sú príslušné orgány orgánmi verejnej moci v zmysle zákona o ľudských právach z roku 1998, musia okrem toho zabezpečiť, aby konali v súlade s právami dohovoru vrátane článku 8 EDĽP. Týmito obmedzeniami sa zabezpečuje, že každé poskytnutie údajov medzi orgánmi presadzovania práva a spravodajskými službami je v súlade s právnymi predpismi o ochrane údajov a EDĽP.

([208]) Pozri napríklad vec M/The Chief Constable of Sussex Police [2019] EWHC 975 (Admin), v ktorej bol Vrchný súd (High Court) požiadaný, aby posúdil výmenu údajov medzi políciou a Partnerstvo na znižovanie kriminality pri podnikaní (Business Crime Reduction Partnership – BCRP), organizáciou poverenou správou systémov oznámení o vylúčení z podnikateľských priestorov, ktorými sa zakazuje osobám vstupovať do takýchto priestorov jej členov. Súd preskúmal poskytovanie údajov, ktoré prebiehalo na základe dohody, ktorej cieľom je ochrana verejnosti a predchádzanie trestnej činnosti, a nakoniec dospel k záveru, že väčšina aspektov poskytovania údajov je zákonná, s výnimkou niektorých citlivých informácií, ktoré si vzájomne poskytovali polícia a BCRP. Ďalším príkladom je vec Cooper/NCA [2019] EWCA Civ 16, v ktorej odvolací súd potvrdil vzájomné poskytovanie údajov medzi políciou a Agentúrou pre závažnú organizovanú trestnú činnosť (Serious Organised Crime Agency – SOCA), orgánom presadzovania práva, ktorý je v súčasnosti súčasťou vnútroštátneho orgánu na ochranu hospodárskej súťaže.

([209]) § 36 ods. 4 zákona o ochrane údajov z roku 2018.

([210]) Zákon o boji proti terorizmu z roku 2008, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([211]) Zákon o spravodajských službách z roku 1994, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/1994/13/contents.

([212]) Zákon o bezpečnostných službách z roku 1989, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/1989/5/contents.

([213]) V § 2 ods. 2 zákona o spravodajských službách z roku 1994 sa stanovuje, že vedúci spravodajskej služby je zodpovedný za efektívnosť tejto služby a je povinný zabezpečiť – a) aby existovali opatrenia na zabezpečenie toho, aby spravodajská služba získala informácie, len ak sú nevyhnutné na riadne plnenie jej funkcií a že akákoľvek informácia bude poskytnutá, len ak je to nevyhnutné – i) na tento účel; ii) v záujme národnej bezpečnosti; iii) na účely predchádzania závažnej trestnej činnosti alebo jej odhaľovania, alebo iv) na účely akéhokoľvek trestného konania a b) že spravodajská služba nepodnikne žiadne kroky na podporu záujmov žiadnej politickej strany Spojeného kráľovstva; v § 2 ods. 2 zákona o bezpečnostných službách z roku 1989 sa stanovuje, že generálny riaditeľ je zodpovedný za efektívnosť tejto služby a je povinný zabezpečiť – a) aby existovali opatrenia na zabezpečenie toho, aby služba získala informácie, len ak sú nevyhnutné na riadne plnenie jej funkcií, resp. že akákoľvek informácia bude poskytnutá, len ak je to nevyhnutné na tento účel alebo na účel predchádzania závažnej trestnej činnosti alebo jej odhaľovania; a b) že služba nepodnikne žiadne kroky na podporu záujmov žiadnej politickej strany a zabezpečiť c) aby existovali opatrenia dohodnuté s generálnym riaditeľom Národnej kriminálnej agentúry, ktorých cieľom je koordinácia činností služby podľa § 1 ods. 4 tohto zákona s činnosťou policajných zložiek, Národnej kriminálnej agentúry a iných orgánov presadzovania práva.

(150) Ak príslušný orgán zamýšľa poskytnúť osobné údaje spracúvané podľa časti 3 zákona o ochrane údajov z roku 2018 orgánom presadzovania práva tretej krajiny, uplatňujú sa osobitné požiadavky ([214]). Takéto prenosy sa môžu uskutočniť konkrétne vtedy, keď sú založené na právnych predpisoch o primeranosti prijatých ministrom, alebo ak takéto právne predpisy neexistujú, je potrebné zabezpečiť primerané záruky. V § 75 zákona o ochrane údajov z roku 2018 sa stanovuje, že primerané záruky sú zavedené vtedy, ak ich tvorí právny nástroj, ktorý zamýšľaného príjemcu zaväzuje, alebo ak prevádzkovateľ po vyhodnotení všetkých okolností týkajúcich sa prenosov tohto druhu osobných údajov do tretej krajiny alebo medzinárodnej organizácii dospeje k záveru, že na ochranu údajov existujú primerané záruky.

(151) Ak sa prenos nezakladá na právnom predpise o primeranosti alebo primeraných zárukách, môže sa uskutočniť len za určitých osobitných okolností, ktoré sa označujú ako „osobitné okolnosti“ ([215]). Ide o prípad, keď je prenos nevyhnutný: a) na ochranu životne dôležitých záujmov dotknutej osoby či inej osoby; b) na zabezpečenie oprávnených záujmov dotknutej osoby; c) na zabránenie bezprostrednému a vážnemu ohrozeniu verejnej bezpečnosti tretej krajiny; d) v jednotlivých prípadoch na akékoľvek účely presadzovania práva, alebo e) v jednotlivých prípadoch na právne účely (napríklad v súvislosti so súdnym konaním alebo s cieľom získať právne poradenstvo). Možno poznamenať, že písmená d) a e) sa neuplatňujú, ak práva a slobody dotknutej osoby prevažujú nad verejným záujmom na prenose. Tento súbor okolností zodpovedá špecifickým situáciám a podmienkam kvalifikovaným ako „výnimky“ podľa článku 38 smernice (EÚ) 2016/680.

(152) Okrem toho, ak sa materiál získaný orgánmi presadzovania práva na základe príkazu, ktorým sa povoľuje použitie zachytávania alebo zasahovanie do zariadení, odovzdá tretej krajine, zákonom o vyšetrovacích právomociach z roku 2016 sa ukladajú dodatočné záruky. Takéto poskytnutie údajov, vymedzené ako „poskytovanie údajov do zahraničia“, je povolené konkrétne len vtedy, ak vydávajúci orgán usúdi, že sa zaviedli osobitné primerané opatrenia, ktorými sa obmedzuje počet osôb, ktorým sa údaje poskytujú, rozsah, v akom sa ktorýkoľvek materiál poskytuje alebo sprístupňuje, ako aj rozsah, v akom sa ktorýkoľvek materiál kopíruje, a počet zhotovených kópií. Okrem toho vydávajúci orgán môže usúdiť, že sú nevyhnutné primerané opatrenia na to, aby sa zabezpečilo, že sa každá zhotovená kópia ktorejkoľvek časti tohto materiálu zničí v okamihu, keď už nebudú existovať relevantné dôvody na jej uchovávanie (ak nebola zničená skôr) ([216]).

(153) A napokon v budúcnosti by sa mohli uskutočňovať osobitné formy následných prenosov zo Spojeného kráľovstva do Spojených štátov na základe „Dohody medzi vládou Spojeného kráľovstva Veľkej Británie a Severného Írska a vládou Spojených štátov amerických o prístupe k elektronickým údajom na účely boja proti závažnej trestnej činnosti“ (ďalej len „dohoda medzi Spojeným kráľovstvom a USA“) ([217]) uzavretej v októbri 2019 ([218]). Hoci dohoda medzi Spojeným kráľovstvom a USA ešte nenadobudla platnosť v čase prijatia tohto rozhodnutia, jej predpokladané nadobudnutie platnosti môže mať vplyv na následné prenosy údajov, ktoré sa najprv preniesli do Spojeného kráľovstva na základe tohto rozhodnutia, do USA. Konkrétnejšie by sa na údaje prenášané z EÚ poskytovateľom služieb v Spojenom kráľovstve podľa tejto dohody medzi Spojeným kráľovstvom a USA po nadobudnutí jej platnosti mohli vzťahovať príkazy na predloženie elektronických dôkazov vydávané príslušnými orgánmi presadzovania práva USA a uplatniteľné v Spojenom kráľovstve. Z týchto dôvodov je posúdenie podmienok a záruk, na základe ktorých sa takýto príkaz môže vydávať a vykonávať, pre toto rozhodnutie relevantné.

([214]) Pozri časť 3 kapitolu 5 zákona o ochrane údajov z roku 2018.

([215]) § 76 zákona o ochrane údajov z roku 2018.

([216]) § 54 a § 130 zákona o vyšetrovacích právomociach z roku 2016. Vydávajúce orgány musia uvážiť potrebu zaviesť osobitné záruky týkajúce sa materiálu odovzdaného zahraničným orgánom, aby sa zabezpečilo, že sa na údaje vzťahujú záruky, pokiaľ ide o uchovávanie, zničenie a poskytovanie údajov, podobné tým, ktoré sú zakotvené v § 53 a 129 zákona o vyšetrovacích právomociach z roku 2016.

([217]) Dohoda medzi vládou Spojeného kráľovstva Veľkej Británie a Severného Írska a vládou Spojených štátov amerických o prístupe k elektronickým údajom na účely boja proti závažnej trestnej činnosti, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

([218]) Ide o prvú dohodu dosiahnutú na základe zákona Spojených štátov o objasnení zákonného využívania údajov v zámorí (Clarifying Lawful Overseas Use of Data Act). Tento zákon Spojených štátov je federálny zákon USA, ktorý bol prijatý 23. marca 2018 a ktorým sa prostredníctvom novely zákona o uchovávaných komunikáciách z roku 1986 (Stored Communications Act) upresňuje, že poskytovatelia služieb v USA sú povinní dodržiavať príkazy Spojených štátov na poskytnutie obsahových a neobsahových údajov bez ohľadu na to, kde sa takéto údaje uchovávajú. Zákon o objasnení zákonného využívania údajov v zámorí ďalej umožňuje uzatváranie vykonávacích dohôd so zahraničnými vládami, na základe ktorých by poskytovatelia služieb Spojených štátov mohli doručovať obsahové údaje priamo týmto zahraničným vládam (znenie tohto zákona je k dispozícii na tomto odkaze: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

(154) V tejto súvislosti treba poznamenať, že po prvé, pokiaľ ide o vecnú pôsobnosť dohody medzi Spojeným kráľovstvom a USA, vzťahuje sa len na trestné činy, za ktoré možno uložiť trest odňatia slobody s hornou hranicou trestnej sadzby stanovenou najmenej na tri roky (vymedzené ako „závažný trestný čin“) ([219]) vrátane „teroristickej činnosti“. Po druhé údaje spracúvané v inej jurisdikcii možno získať podľa tejto dohody medzi Spojeným kráľovstvom a USA len na základe „príkazu [...], ktorý podlieha preskúmaniu alebo dohľadu podľa vnútroštátneho právneho poriadku vydávajúcej strany súdom, sudcom alebo iným nezávislým orgánom pred začiatkom konania alebo v konaní týkajúcom sa výkonu príkazu“ ([220]). Po tretie každý príkaz musí „vychádzať z požiadaviek primeraného odôvodnenia na základe konkrétnych a dôveryhodných skutočností, osobitosti, zákonnosti a závažnosti, pokiaľ ide o vyšetrovaný prípad“ ([221]), a „zameriavať na konkrétne účty, ako aj identifikovať konkrétnu osobu, účet, adresu, osobné zariadenie alebo akýkoľvek iný konkrétny identifikátor“ ([222]). Po štvrté na údaje získané na základe tejto dohody sa vzťahuje rovnocenná ochrana ako osobitné záruky stanovené takzvanou zastrešujúcou dohodou medzi EÚ a USA ([223]) – komplexnou dohodou o ochrane údajov uzavretou v decembri 2016 medzi EÚ a USA, v ktorej sa stanovujú záruky a práva uplatniteľné na prenosy údajov v oblasti spolupráce týkajúcej sa presadzovania práva – ktoré sú všetky začlenené *mutatis mutandis* do tejto dohody medzi Spojeným kráľovstvom a USA prostredníctvom odkazov, aby sa zohľadnila najmä osobitná povaha prenosov (t. j. ide skôr prenosy od súkromných subjektov orgánom presadzovania práva než o prenosy medzi orgánmi presadzovania práva) ([224]). V dohode medzi Spojeným kráľovstvom a USA sa konkrétne stanovuje, že ochrana, ktorá je rovnocenná ako ochrana stanovená v rámci zastrešujúcej dohody medzi EÚ a USA, sa bude vzťahovať „na všetky osobné údaje predkladané pri vykonávaní príkazov, na ktoré sa vzťahuje dohoda medzi Spojeným kráľovstvom a USA, s cieľom zabezpečiť rovnocennú ochranu“ ([225]).

(155) Na údaje prenášané orgánom USA na základe dohody medzi Spojeným kráľovstvom a USA by sa preto mala vzťahovať ochrana podľa nástroja práva EÚ, pričom by sa vykonali potrebné úpravy, ktoré by odzrkadlili povahu príslušných prenosov. Orgány Spojeného kráľovstva ďalej potvrdili, že ochrana zastrešujúcej dohody sa bude vzťahovať na všetky osobné údaje predkladané alebo uchovávané na základe dohody medzi Spojeným kráľovstvom a USA bez ohľadu na povahu alebo druh orgánu, ktorý podal žiadosť (napr. federálne orgány aj štátne orgány presadzovania práva v USA), takže rovnocenná ochrana sa musí zabezpečiť vo všetkých prípadoch. Orgány Spojeného kráľovstva však ďalej upresnili, že podrobnosti o konkrétnom vykonávaní záruk ochrany údajov sú stále predmetom diskusií medzi Spojeným kráľovstvom a USA. V súvislosti s rokovaniami s útvarmi Európskej komisie o tomto rozhodnutí orgány Spojeného kráľovstva potvrdili, že nechajú dohodu medzi Spojeným kráľovstvom a USA vstúpiť do platnosti až vtedy, keď sa presvedčia, že jej vykonávanie je v súlade s právnymi povinnosťami stanovenými v tejto dohode vrátane jednoznačnosti, pokiaľ ide o súlad s normami ochrany údajov pre všetky údaje požadované na základe tejto dohody medzi Spojeným kráľovstvom a USA. Keďže prípadné nadobudnutie platnosti dohody medzi Spojeným kráľovstvom a USA môže mať vplyv na úroveň ochrany posudzovanú v tomto rozhodnutí, akékoľvek informácie alebo budúce upresnenie spôsobu, akým budú USA plniť svoje záväzky vyplývajúce z dohody medzi Spojeným kráľovstvom a USA, by malo Spojené kráľovstvo oznámiť Európskej komisii hneď, ako bude k dispozícii, a v každom prípade pred nadobudnutím platnosti dohody medzi Spojeným kráľovstvom a USA, aby sa zabezpečilo riadne monitorovanie tohto rozhodnutia v súlade s článkom 45 ods. 4 nariadenia (EÚ) 2016/679. Osobitná pozornosť sa bude venovať uplatňovaniu ochrany zastrešujúcej dohody na konkrétny druh prevodov, na ktoré sa vzťahuje dohoda medzi Spojeným kráľovstvom a USA, a jej úprave.

(156) Všeobecnejšie povedané, akákoľvek relevantná zmena, pokiaľ ide o nadobudnutie platnosti a uplatňovanie dohody medzi Spojeným kráľovstvom a USA, sa náležite zohľadní v spojitosti s nepretržitým monitorovaním tohto rozhodnutia, a to aj pokiaľ ide o príslušné dôsledky, ktoré sa vyvodia v prípade akéhokoľvek náznaku, že už nie je zabezpečená v zásade rovnocenná úroveň ochrany.

3.2.3. *Dohľad*

(157) V závislosti od právomocí, ktoré príslušné orgány využívajú pri spracúvaní osobných údajov na účely presadzovania práva (či už podľa zákona o ochrane údajov z roku 2018, alebo zákona o vyšetrovacích právomociach z roku 2016), zabezpečujú dohľad nad využívaním týchto právomocí rôzne orgány. Komisár pre informácie konkrétne dozerá na spracúvanie osobných údajov, keď spracúvanie patrí do rozsahu pôsobnosti časti 3 zákona o ochrane údajov z roku

([219]) Článok 1 ods. 14 dohody medzi Spojeným kráľovstvom a USA.
([220]) Článok 5 ods. 2 dohody medzi Spojeným kráľovstvom a USA.
([221]) Článok 5 ods. 1 dohody medzi Spojeným kráľovstvom a USA.
([222]) Článok 4 ods. 5 dohody medzi Spojeným kráľovstvom a USA. Pokiaľ ide o zachytávanie v reálnom čase, uplatňuje sa dodatočná a prísnejšia norma: príkazy sa musia vydávať na obmedzené obdobie, ktoré nesmie byť dlhšie ako obdobie primerane nevyhnutné na splnenie účelov príkazu, a vydávajú sa len vtedy, ak by tie isté informácie nebolo možné primeraným spôsobom získať menej rušivým postupom (článok 5 ods. 3 dohody medzi Spojeným kráľovstvom a USA).
([223]) Dohoda medzi Spojenými štátmi americkými a Európskou úniou o ochrane osobných informácií v súvislosti s predchádzaním trestným činom, ich vyšetrovaním, odhaľovaním a stíhaním (Ú. v. EÚ L 336, 10.12.2016, s. 3 – 13), k dispozícii na tomto odkaze: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:22016A1210(01)&from=SK.
([224]) Článok 9 ods. 1 dohody medzi Spojeným kráľovstvom a USA.
([225]) Článok 9 ods. 1 dohody medzi Spojeným kráľovstvom a USA.

2018 ([226]). Nezávislý a súdny dohľad nad používaním vyšetrovacích právomocí podľa zákona o vyšetrovacích právomociach z roku 2016 zabezpečuje Úrad Komisára pre vyšetrovacie právomoci ([227]) (táto časť je predmetom odôvodnení 250 až 255). Okrem toho ďalší dohľad zabezpečuje parlament a ďalšie orgány.

3.2.3.1. Dohľad na základe ustanovení časti 3 zákona o ochrane údajov z roku 2018

(158) Všeobecné funkcie Komisára pre informácie – ktorého nezávislosť a organizácia sú vysvetlené v odôvodnení 87 – v súvislosti so spracúvaním osobných údajov, ktoré patrí do rozsahu pôsobnosti časti 3 zákona o ochrane údajov z roku 2018, sú stanovené v prílohe 13 k zákonu o ochrane údajov z roku 2018. Hlavnou úlohou Komisára pre informácie je monitorovať a presadzovať časť 3 zákona o ochrane údajov z roku 2018, ako aj zvyšovať povedomie verejnosti a poskytovať poradenstvo parlamentu, vláde a iným inštitúciám a orgánom. V záujme zachovania nezávislosti justície nie je Komisár pre informácie oprávnený vykonávať svoje funkcie v súvislosti so spracúvaním osobných údajov jednotlivcom konajúcim v rámci súdnej právomoci, resp. súdom či tribunálom konajúcim v rámci svojej súdnej právomoci. Za týchto okolností by funkcie dohľadu vykonávali iné orgány, ako sa uvádza v odôvodneniach 99 až 103.

(159) Komisár pre informácie má všeobecné vyšetrovacie, nápravné, povoľovacie a poradné právomoci v súvislosti so spracúvaním osobných údajov, na ktoré sa vzťahuje časť 3. Komisár pre informácie má predovšetkým právomoc oznamovať prevádzkovateľovi alebo sprostredkovateľovi údajné porušenie časti 3 zákona o ochrane údajov z roku 2018, vydávať varovania alebo napomenutia prevádzkovateľovi alebo sprostredkovateľovi, ktorý porušil ustanovenia časti 3 zákona, ako aj z vlastnej iniciatívy alebo na požiadanie vydávať stanoviská pre parlament, vládu alebo iné inštitúcie a orgány, ako aj pre verejnosť k akejkoľvek otázke týkajúcej sa ochrany osobných údajov ([228]).

(160) Okrem toho má Komisár pre informácie právomoc vydávať informačné oznámenia ([229]), oznámenia o posúdení ([230]) a presadzovacie oznámenia ([231]), ako aj právo na prístup k dokumentom prevádzkovateľov a sprostredkovateľov, na vstup do ich priestorov ([232]) a právo ukladať správne pokuty formou oznámenia o uložení sankcie. ([233]) Okolnosti, za ktorých Komisár pre informácie vydáva informačné oznámenie, oznámenie o posúdení, presadzovacie oznámenie a oznámenie o uložení sankcie ([234]) sa stanovujú v regulačnej politike Komisára pre informácie [pozri aj odôvodnenie 93 a odôvodnenia týkajúce sa rozhodnutia o primeranosti 101 – 102 smernice (EÚ) 2016/680].

(161) Podľa posledných výročných správ (2018 – 2019 ([235]), 2019 – 2020 ([236])) Komisár pre informácie uskutočnil niekoľko vyšetrovaní a prijal opatrenia na presadzovanie práva v súvislosti so spracúvaním údajov orgánmi presadzovania práva. Komisár napríklad viedol vyšetrovanie a v októbri 2019 uverejnil stanovisko týkajúce sa používania technológie rozpoznávania tváre na verejných miestach na účely presadzovania práva. Vyšetrovanie sa zameriavalo najmä na využívanie schopností rozpoznávania tváre v reálnom čase zo strany polície Južného Walesu a Metropolitnej policajnej služby (ďalej len „MPS“). Komisár pre informácie ďalej prešetroval matricu MPS na odhaľovanie gangov ([237]) a zistil celý rad závažných porušení právnych predpisov o ochrane údajov, ktoré by mohli narušiť dôveru verejnosti v matricu a v spôsob, akým sa údaje používali. V novembri 2018 Komisár pre informácie vydal presadzovacie oznámenie a následne MPS podnikla kroky potrebné na zvýšenie bezpečnosti a zodpovednosti a na zabezpečenie primeraného

([226]) § 116 zákona o ochrane údajov z roku 2018.
([227]) Pozri zákon o vyšetrovacích právomociach z roku 2016, najmä časť 8 kapitolu 1.
([228]) Bod 2 prílohy 13 k zákonu o ochrane údajov z roku 2018.
([229]) Nariaďujú prevádzkovateľovi a sprostredkovateľovi (a za určitých okolností akejkoľvek inej osobe), aby poskytli potrebné informácie (§ 142 zákona o ochrane údajov z roku 2018).
([230]) Umožňujú vykonávať vyšetrovanie a audit, pri ktorých možno vyžadovať, aby prevádzkovateľ alebo sprostredkovateľ povolil Komisárovi pre informácie vstúpiť do určených priestorov, skontrolovať alebo preskúmať dokumenty alebo zariadenia, vypočuť osoby, ktoré spracúvajú osobné údaje v mene prevádzkovateľa (§ 146 zákona o ochrane údajov z roku 2018).
([231]) Umožňujú vykonávať nápravné právomoci, pri ktorých sa vyžaduje, aby prevádzkovatelia/sprostredkovatelia prijali alebo sa zdržali prijatia konkrétnych krokov (§ 149 zákona o ochrane údajov z roku 2018).
([232]) § 154 zákona o ochrane údajov z roku 2018.
([233]) § 155 zákona o ochrane údajov z roku 2018.
([234]) Regulačná politika, pozri poznámku pod čiarou č. 96.
([235]) Výročná správa a finančné výkazy Komisára pre informácie za roky 2018 – 2019, pozri poznámku pod čiarou č. 101.
([236]) Výročná správa a finančné výkazy Komisára pre informácie za roky 2019 – 2020, pozri poznámku pod čiarou č. 82.
([237]) Databáza, ktorá zaznamenávala spravodajské informácie týkajúce sa údajných členov gangov a obetí trestných činov súvisiacich s gangmi.

využívania údajov. Ďalším príkladom presadzovacích opatrení v tejto oblasti je pokuta vo výške 325 000 GBP, ktorú Komisár pre informácie udelil v máji 2018 prokuratúre (Crown Prosecution Service) za stratu nezašifrovaných nosičov DVD obsahujúcich záznamy policajných výsluchov. Komisár pre informácie ďalej prešetroval širšie témy, napríklad v prvej polovici roka 2020 využívanie extrakcie mobilných telefónov na policajné účely a spracúvanie údajov o obetiach zo strany polície. Okrem toho Komisár pre informácie v súčasnosti vyšetruje prípad, ktorý sa týka prístupu orgánov presadzovania práva k údajom, ktorými disponuje subjekt v súkromnom sektore Clearview AI Inc ([238]).

(162) Okrem právomocí Komisára pre informácie v oblasti presadzovania práva uvedených v odôvodneniach 160 a 161 možno uviesť, že určité porušenia právnych predpisov o ochrane údajov predstavujú trestné činy, a preto môžu podliehať trestnoprávnym sankciám (§ 196 zákona o ochrane údajov z roku 2018). Ide napríklad o získanie, poskytnutie alebo uchovávanie osobných údajov bez súhlasu prevádzkovateľa a poskytnutie prístupu k osobným údajom inej osobe bez súhlasu prevádzkovateľa ([239]); opätovnú identifikáciu anonymizovaných osobných údajov bez súhlasu prevádzkovateľa zodpovedného za anonymizáciu týchto osobných údajov ([240]); úmyselné bránenie Komisárovi pre informácie pri výkone jeho právomocí v súvislosti s kontrolou osobných údajov v súlade s medzinárodnými záväzkami ([241]), nepravdivé vyhlásenia v reakcii na informačné oznámenie alebo zničenie informácií v súvislosti s informačným oznámením a oznámením o posúdení ([242]).

3.2.3.2. Ďalšie orgány dohľadu v oblasti presadzovania trestného práva

(163) Okrem Komisára pre informácie existuje v oblasti presadzovania trestného práva niekoľko orgánov dohľadu so špecifickými mandátmi súvisiacimi s otázkami ochrany údajov. Patrí medzi ne napríklad Komisár pre uchovávanie a používanie biometrického materiálu (ďalej len „Komisár pre biometriu“) ([243]) a Komisár pre sledovanie kamerovým systémom ([244]).

3.2.3.3. Parlamentný dohľad v oblasti presadzovania trestného práva

(164) Užší výbor pre vnútorné záležitosti zabezpečuje parlamentný dohľad v oblasti presadzovania práva. Tento výbor sa skladá z 11 poslancov parlamentu vybraných z troch najväčších politických strán. Úlohou výboru je kontrolovať výdavky, správu a postupy ministerstva vnútra a súvisiacich verejných orgánov vrátane polície a Národnej kriminálnej agentúry, ktorej činnosť môže výbor konkrétne kontrolovať ([245]).

([238]) Pozri vyhlásenie Komisára pre informácie, k dispozícii na tomto odkaze: 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]) § 170 zákona o ochrane údajov z roku 2018.

([240]) § 171 zákona o ochrane údajov z roku 2018.

([241]) § 119 ods. 6 zákona o ochrane údajov z roku 2018.

([242]) Počas rozpočtového roka pokrývajúceho obdobie od 1. apríla 2019 do 31. marca 2020 viedli vyšetrovania Komisára pre informácie k štyrom varovaniam a ôsmim trestným stíhaniam. Tieto prípady boli stíhané v súlade s § 55 zákona o ochrane údajov z roku 1998, § 77 zákona o slobodnom prístupe k informáciám z roku 2000 a § 170 zákona o ochrane údajov z roku 2018. V 75 % prípadoch obžalovaní priznali svoju vinu, čím odpadla potreba zdĺhavých konaní so súvisiacimi nákladmi. (Výročná správa a finančné výkazy Komisára pre informácie za roky 2019 – 2020, pozri poznámku pod čiarou č. 87, s. 40).

([243]) Úrad Komisára pre biometriu bol zriadený zákonom o ochrane slobôd z roku 2012 (pozri https://www.legislation.gov.uk/ukpga/2012/9/contents). Komisár pre biometriu okrem iného rozhoduje o tom, či polícia môže uchovávať záznamy o profiloch DNA a odtlačky prstov získané od osôb, ktoré boli zatknuté, ale neboli obvinené z kvalifikovaného trestného činu (§ 63G zákona o polícii a dôkazoch v trestných veciach z roku 1984). Tento komisár má okrem toho všeobecnú zodpovednosť za to, aby uchovávanie a používanie DNA a odtlačkov prstov a uchovávanie z dôvodov národnej bezpečnosti boli predmetom preskúmania (§ 20 ods. 2 zákona o ochrane slobody z roku 2012). Komisár pre biometriu sa vymenúva na základe kódexu riadenia verejných menovaní (tento kódex je k dispozícii na tomto odkaze: https://www.gov.uk/government/publications/governance-code-for-public-appointments) a v podmienkach jeho vymenovania sa jasne stanovuje, že ho z funkcie môže odvolať len minister vnútra, a to len na základe úzko vymedzeného súboru okolností, medzi ktoré patrí neplnenie si povinností počas troch mesiacov, odsúdenie za spáchanie trestného činu alebo neplnenie podmienok jeho vymenovania.

([244]) Úrad Komisára pre sledovanie kamerovým systémom bol zriadený zákonom o ochrane slobôd z roku 2012 a jeho úlohou je podporovať súlad s Kódexom postupov pre sledovanie kamerovým systémom, kontrolovať uplatňovanie tohto kódexu a poskytovať poradenstvo ministrom o prípadných potrebných zmenách tohto kódexu. Komisár sa vymenúva podľa rovnakých pravidiel ako Komisár pre biometriu a má podobné právomoci, zdroje a ochranu pred odvolaním z funkcie.

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

(165) Výbor si môže v rámci svojej právomoci zvoliť vlastný predmet vyšetrovania vrátane konkrétnych prípadov, pokiaľ vec práve nie je predmetom súdneho konania. Výbor takisto môže požiadať širokú škálu relevantných skupín a jednotlivcov o písomné a ústne dôkazy. Vypracúva správy o svojich zisteniach a vydáva odporúčania vláde ([246]). Od vlády sa očakáva, že zareaguje na každé odporúčanie v správe, a musí tak urobiť do 60 dní ([247]).

(166) V oblasti sledovania výbor takisto vypracoval správu týkajúcu sa zákona o regulácii vyšetrovacích právomocí z roku 2000 ([248]), z ktorej vyplynulo, že zákon o regulácii vyšetrovacích právomocí z roku 2000 neplní svoj účel. Táto správa sa zohľadňovala pri nahradení veľkých častí zákona o regulácii vyšetrovacích právomocí z roku 2000 zákonom o vyšetrovacích právomociach z roku 2016. Úplný zoznam vyšetrovaní sa nachádza na webovom sídle výboru ([249]).

(167) V Škótsku vykonáva úlohy užšieho výboru pre vnútorné záležitosti justičný podvýbor pre policajnú činnosť (Justice Subcommittee on Policing) a v Severnom Írsku výbor pre justíciu (Committee for Justice) ([250]).

3.2.4. *Náprava*

(168) Pokiaľ ide o spracúvanie údajov orgánmi presadzovania práva, mechanizmy nápravy sa stanovujú v časti 3 zákona o ochrane údajov z roku 2018 a v zákone o vyšetrovacích právomociach z roku 2016, ako aj v zákone o ľudských právach z roku 1998.

(169) Súbor mechanizmov poskytuje dotknutým osobám účinné správne a súdne prostriedky nápravy, ktoré im umožňujú najmä zaistiť svoje práva vrátane práva na prístup k svojim osobným údajom alebo práva dosiahnuť opravu alebo vymazanie týchto údajov.

(170) Po prvé podľa § 165 zákona o ochrane údajov z roku 2018 má dotknutá osoba právo podať sťažnosť Komisárovi pre informácie, ak sa dotknutá osoba domnieva, že v súvislosti s osobnými údajmi, ktoré sa jej týkajú, došlo k porušeniu časti 3 zákona o ochrane údajov z roku 2018 ([251]). Komisár pre informácie má právomoc posúdiť dodržiavanie zákona o ochrane údajov z roku 2018 zo strany prevádzkovateľa a sprostredkovateľa a požadovať od nich, aby v prípade nedodržiavania tohto zákona prijali potrebné kroky, a ukladať pokuty.

([246]) Užšie výbory vrátane užšieho výboru pre vnútorné záležitosti podliehajú rokovaciemu poriadku Dolnej snemovne. Rokovací poriadok predstavuje pravidlá odsúhlasené Dolnou snemovňou upravujúce spôsob činnosti parlamentu. Užšie výbory majú rozsiahlu právomoc, pričom v § 152 ods. 1 rokovacieho poriadku sa stanovuje, že „Užšie výbory sa volia na účely kontroly výdavkov, správy a postupov hlavných ministerstiev uvedených v odseku 2 tohto poriadku a súvisiacich verejných orgánov.“ To umožňuje užšiemu výboru pre vnútorné záležitosti preskúmať akýkoľvek postup ministerstva vnútra vrátane postupov (a súvisiacich právnych predpisov) v oblasti vyšetrovacích právomocí. Okrem toho sa v § 152 ods. 4 rokovacieho poriadku jasne uvádza, že výbory majú rôzne právomoci vrátane schopnosti požiadať jednotlivcov o vypovedanie alebo predloženie dokumentov ku konkrétnej otázke a schopnosti vypracúvať správy. Aktuálne a doterajšie vyšetrovania výboru sú k dispozícii na tomto odkaze: https://committees.parliament.uk/committee/83/home-affairs-committee/.

([247]) Právomoci užšieho výboru pre vnútorné záležitosti v Anglicku a vo Walese sa uvádzajú v rokovacom poriadku Dolnej snemovne a sú k dispozícii na tomto odkaze: https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

([248]) K dispozícii na tomto odkaze: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm.

([249]) K dispozícii na tomto odkaze: https://committees.parliament.uk/committee/83/home-affairs-committee.

([250]) Predpisy justičného podvýboru pre policajnú činnosť v Škótsku sa nachádzajú na tomto odkazehttps://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx a predpisy výboru pre justíciu v Severnom Írsku sa nachádzajú na tomto odkaze: http://www.niassembly.gov.uk/assembly-business/standing-orders/.

([251]) Posledná výročná správa Komisára pre informácie obsahuje prehľad povahy prijatých a uzavretých sťažností. Počet prijatých sťažností na „policajnú činnosť a záznamy vedené v registri trestov“ konkrétne predstavuje 6 % celkového počtu prijatých sťažností (nárast o 1 % v porovnaní s predchádzajúcim rozpočtovým rokom). Z výročnej správy takisto vyplýva, že sťažnosti týkajúce sa žiadostí dotknutých osôb o prístup k údajom tvoria najvyšší podiel (46 % celkového počtu sťažností, čo predstavuje nárast o 8 % v porovnaní s predchádzajúcim rozpočtovým rokom) (Výročná správa Komisára pre informácie za roky 2019 – 2020, s. 55, pozri poznámku pod čiarou č. 88).

(171) Po druhé v zákone o ochrane údajov z roku 2018 sa stanovuje právo na prostriedok nápravy voči Komisárovi pre informácie, ak sťažnosť podanú dotknutou osobou nerieši primerane. Konkrétne sa uvádza, že ak Komisár pre informácie „nepokročil“ ([252]) vo veci sťažnosti podanej dotknutou osobou, sťažovateľ má prístup k súdnemu prostriedku nápravy, pretože sa môže obrátiť na tribunál prvého stupňa ([253]) s cieľom nariadiť Komisárovi pre informácie, aby v reakcii na sťažnosť prijal vhodné opatrenia, alebo aby informoval sťažovateľa o pokroku v súvislosti so sťažnosťou ([254]). Okrem toho sa každá osoba, ktorá dostane od Komisára pre informácie akékoľvek z uvedených oznámení (informačné oznámenie, oznámenie o posúdení, presadzovacie oznámenie alebo oznámenie o uložení sankcie), môže odvolať na tribunál prvého stupňa. Ak sa tribunál domnieva, že rozhodnutie Komisára pre informácie nie je v súlade so zákonom alebo že Komisár pre informácie mal uplatniť svoju voľnú úvahu inak, tribunál musí odvolaniu vyhovieť, resp. musí vydať iné oznámenie alebo prijať iné rozhodnutie, ktoré mohol vydať alebo prijať Komisár pre informácie ([255]).

(172) Po tretie osoby môžu vymáhať súdne prostriedky nápravy voči prevádzkovateľom a sprostredkovateľom priamo pred súdom. Konkrétne podľa § 167 zákona o ochrane údajov z roku 2018 môže dotknutá osoba podať žalobu na súd pre porušenie jej práv vyplývajúcich z právnych predpisov o ochrane údajov a súd môže formou príkazu prevádzkovateľa požiadať, aby prijal (alebo neprijal) akékoľvek kroky súvisiace so spracúvaním s cieľom dosiahnuť dodržiavanie zákona o ochrane údajov z roku 2018. Okrem toho podľa § 169 zákona o ochrane údajov z roku 2018 akákoľvek osoba, ktorá utrpela škodu v dôsledku porušenia niektorej požiadavky právnych predpisov o ochrane údajov (vrátane časti 3 zákona o ochrane údajov z roku 2018) iných ako všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, má nárok na náhradu tejto škody od prevádzkovateľa alebo sprostredkovateľa s výnimkou prípadu, že prevádzkovateľ alebo sprostredkovateľ dokáže, že prevádzkovateľ alebo sprostredkovateľ nie je žiadnym spôsobom zodpovedný za udalosť, ktorá spôsobila škodu. Škoda zahŕňa tak finančnú ujmu, ako aj škodu, ktorá nezahŕňa finančnú ujmu, ako napríklad nemajetkovú ujmu.

(173) Napokon akákoľvek osoba, ktorá sa domnieva, že došlo k poškodeniu jej práv vrátane práva na súkromie a ochranu údajov zo strany orgánov verejnej moci, môže dosiahnuť nápravu pred súdmi Spojeného kráľovstva na základe zákona o ľudských právach z roku 1998 ([256]) a po vyčerpaní vnútroštátnych prostriedkov nápravy môže osoba, mimovládna organizácia a skupina osôb vymôcť nápravu pred Európskym súdom pre ľudské práva za porušenia práv zaručených v Európskom dohovore o ľudských právach ([257]) (pozri odôvodnenie 111).

3.2.4.1. Mechanizmy nápravy dostupné podľa zákona o vyšetrovacích právomociach z roku 2016

(174) Osoby môžu dosiahnuť nápravu za porušenie zákona o vyšetrovacích právomociach z roku 2016 pred tribunálom pre kontrolu vyšetrovacích právomocí (Investigatory Powers Tribunal). Možnosti získania nápravy dostupné podľa zákona o vyšetrovacích právomociach z roku 2016 sú opísané v odôvodneniach 263 až 269.

([252]) V § 166 zákona o ochrane údajov z roku 2018 sa konkrétne uvádzajú tieto situácie: a) Komisár pre informácie nepodnikne primerané kroky v reakcii na sťažnosť, b) Komisár pre informácie neposkytne sťažovateľovi informácie o pokroku v súvislosti so sťažnosťou alebo o jej výsledku pred uplynutím 3-mesačnej lehoty, ktorá začína plynúť od prijatia sťažnosti týmto komisárom, alebo c) v prípade, že posúdenie sťažnosti Komisárom pre informácie počas tohto obdobia ešte nie je ukončené, ak neposkytne sťažovateľovi takéto informácie počas nasledujúcich 3 mesiacov.

([253]) Tribunál prvého stupňa je súd príslušný na rozhodovanie o odvolaniach proti rozhodnutiam vládnych regulačných orgánov. V prípade rozhodnutia Komisára pre informácie je príslušnou komorou „Všeobecná regulačná komora“, ktorá má právomoc nad celým Spojeným kráľovstvom.

([254]) § 166 zákona o ochrane údajov z roku 2018. Jedným z príkladov úspešných žalôb proti Komisárovi pre informácie pred tribunálom je prípad, v ktorom Komisár pre informácie potvrdil prijatie sťažnosti od dotknutej osoby, ale neuviedol, aké kroky plánuje podniknúť, a preto mu bolo nariadené do 21 kalendárnych dní potvrdiť, či sťažnosti vyšetrí, a ak áno, informovať sťažovateľa o pokroku vo vyšetrovaní najmenej každých 21 kalendárnych dní po potvrdení (rozsudok ešte nebol zverejnený). Takisto aj prípad, v ktorom tribunál prvého stupňa rozhodol, že nie je jasné, či odpoveď Komisára pre informácie sťažovateľovi predstavovala náležitý „výsledok“ sťažnosti (pozri vec Susan Milne/The Information Commissioner [2020], rozsudok k dispozícii na tomto odkaze: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220 %20Section%20166 %20DPA%20-DECISION.pdf).

([255]) § 162 a § 163 zákona o ochrane údajov z roku 2018.

([256]) Pozri napríklad vec Brown/Commissioner of Police of the Metropolis & Anor [2019] EWCA Civ 1724, v ktorej bola na základe zákona o ochrane údajov z roku 1998 a zákona o ľudských právach z roku 1998 prisúdená náhrada škody vo výške 9 000 GBP za nezákonné získanie a zneužitie osobných údajov, a vec R (on the application of Bridges/The Chief Constable of South Wales [2020] EWCA Civ 1058, v ktorej odvolací súd vyhlásil používanie systému na rozpoznávanie tváre waleskou políciou za nezákonné, keďže predstavovalo porušenie článku 8 EDĽP a posúdenie vplyvu na ochranu údajov vypracované prevádzkovateľom nebolo v súlade so zákonom o ochrane údajov z roku 2018.

([257]) V článku 34 Európskeho dohovoru o ľudských právach sa stanovuje, že „Súd môže prijať žaloby od akejkoľvek osoby, mimovládnej organizácie alebo skupiny osôb, ktorá tvrdí, že je obeťou porušenia práv stanovených v dohovore alebo v protokoloch k dohovoru zo strany jednej z vysokých zmluvných strán. Vysoké zmluvné strany sa zaväzujú, že žiadnym spôsobom nebudú brániť účinnému vykonávaniu tohto práva“.

3.3. **Prístup k osobným údajom a ich používanie zo strany orgánov verejnej moci Spojeného kráľovstva na účely národnej bezpečnosti**

(175) V rámci právneho poriadku Spojeného kráľovstva sú spravodajskými službami s právomocou získavať elektronické údaje, ktoré majú v držbe prevádzkovatelia alebo sprostredkovatelia, z dôvodu národnej bezpečnosti a v situáciách súvisiacich so scenárom primeranosti Bezpečnostná služba (MI5) ([258]), Tajná spravodajská služba (SIS) ([259]) a Vládne komunikačné ústredie ([260]) (GCHQ) ([261]).

3.3.1. *Právne základy, obmedzenia a záruky*

(176) V Spojenom kráľovstve sú právomoci spravodajských služieb stanovené v zákone o vyšetrovacích právomociach z roku 2016 a v zákone o regulácii vyšetrovacích právomocí z roku 2000, ktoré spolu so zákonom o ochrane údajov z roku 2018 vymedzujú materiálny a osobný rozsah uplatňovania týchto právomocí, ako aj obmedzenia a záruky na ich používanie. Tieto právomoci, ako aj obmedzenia a záruky, ktoré sa na ne vzťahujú, sa podrobne posudzujú v nasledujúcich častiach.

3.3.1.1. Vyšetrovacie právomoci uplatňované v kontexte národnej bezpečnosti

(177) Zákonom o vyšetrovacích právomociach z roku 2016 sa ustanovuje právny rámec pre využívanie vyšetrovacích právomocí, t. j. právomoc zachytávať údaje z komunikácie, získavať k nim prístup a vykonávať zasahovanie do zariadení. V zákone o vyšetrovacích právomociach z roku 2016 sa zavádza všeobecný zákaz používania techník, ktoré umožňujú prístup k obsahu komunikácie, prístup k údajom o komunikácii alebo zasahovanie do zariadení bez zákonnej právomoci, a stanovuje sa, že ich používanie je trestným činom ([262]). Premieta sa to v skutočnosti, že využívanie týchto vyšetrovacích právomocí je zákonné len vtedy, keď sa uskutočňuje na základe príkazu alebo povolenia ([263]).

(178) V zákone o vyšetrovacích právomociach z roku 2016 sú stanovené podrobné pravidlá, ktoré riadia rozsah a uplatňovanie každej vyšetrovacej právomoci, ako aj ich osobitné obmedzenia a záruky. Uplatňujú sa odlišné pravidlá v závislosti od druhu vyšetrovacej právomoci (zachytávanie komunikácie, získavanie a uchovávanie

([258]) MI5 je v pôsobnosti ministerstva vnútra. V zákone o bezpečnostných službách z roku 1989 sa stanovujú funkcie MI5: ochrana národnej bezpečnosti (vrátane ochrany pred hrozbami špionáže, terorizmu a sabotáže, pred činnosťami agentov zahraničných veľmocí a pred činmi, ktorých cieľom je zvrhnúť alebo oslabiť parlamentnú demokraciu politickými, priemyselnými alebo násilnými prostriedkami), ochrana hospodárskeho blahobytu Spojeného kráľovstva pred vonkajšími hrozbami a podpora policajných zložiek a iných orgánov presadzovania práva pri predchádzaní závažným trestným činom a ich odhaľovaní.

([259]) Tajná spravodajská služba (SIS) je v pôsobnosti ministra zahraničných vecí a jej funkcie sú stanovené v zákone o spravodajských službách z roku 1994. Jej funkcie sú získavať a poskytovať informácie týkajúce sa činností alebo zámerov osôb mimo Britských ostrovov a plniť iné úlohy týkajúce sa činností alebo zámerov týchto osôb. Tieto funkcie možno vykonávať len v záujme národnej bezpečnosti, hospodárskeho blahobytu Spojeného kráľovstva alebo na podporu pri predchádzaní závažným trestným činom a ich odhaľovaní.

([260]) Vládne komunikačné ústredie je v pôsobnosti ministra zahraničných vecí a jeho funkcie sú stanovené v zákone o spravodajských službách z roku 1994. konkrétne a) monitorovanie, využívanie alebo zasahovanie do elektromagnetických a iných emisií a zariadení, ktoré vysielajú tieto emisie, získavanie a poskytovanie informácií vyplývajúcich z týchto emisií alebo zariadení a zo šifrovaného materiálu; b) poskytovanie poradenstva a pomoci ozbrojeným silám, vláde alebo iným príslušným organizáciám alebo osobám v oblasti jazykov vrátane terminológie používanej v technických záležitostiach a kryptografii a iných záležitostiach týkajúcich sa ochrany údajov. Tieto funkcie možno vykonávať len v záujme národnej bezpečnosti, hospodárskeho blahobytu Spojeného kráľovstva v súvislosti s činmi alebo zámermi osôb mimo Britských ostrovov alebo na podporu pri predchádzaní závažným trestným činom a ich odhaľovaní.

([261]) Ďalšími verejnými orgánmi vykonávajúcimi funkcie relevantné pre národnú bezpečnosť sú Obranná spravodajská služba, Rada a sekretariát pre národnú bezpečnosť (National Security Council and Secretariat), Spoločná spravodajská organizácia (Joint Intelligence Organisation) a Spoločný spravodajský výbor (Joint Intelligence Committee). Spoločný spravodajský výbor ani Spoločná spravodajská organizácia však nemôžu uplatňovať vyšetrovacie právomoci podľa zákona o vyšetrovacích právomociach z roku 2016, zatiaľ čo Obranná spravodajská služba má obmedzený rozsah uplatňovania svojich právomocí.

([262]) Tento zákaz sa vzťahuje na verejné aj súkromné komunikačné siete, ako aj na verejnú poštovú službu, keď sa zachytávanie vykonáva v Spojenom kráľovstve. Zákaz sa nevzťahuje na prevádzkovateľa súkromnej siete, ak prevádzkovateľ dal výslovný alebo nepriamo vyjadrený súhlas na výkon zachytávania (§ 3 zákona o vyšetrovacích právomociach z roku 2016).

([263]) V konkrétnych obmedzených prípadoch je možné zákonné zachytávanie bez príkazu, t. j. pri zachytávaní so súhlasom odosielateľa alebo prijímateľa (§ 44 zákona o vyšetrovacích právomociach z roku 2016), v prípade obmedzených administratívnych účelov alebo účelov presadzovania práva (§ 45 až § 48 zákona o vyšetrovacích právomociach z roku 2016), v určitých osobitných inštitúciách (§ 49 až § 51 zákona o vyšetrovacích právomociach z roku 2016) a v súlade so zahraničnými žiadosťami (§ 52 zákona o vyšetrovacích právomociach z roku 2016).

údajov o komunikácii a zasahovanie do zariadení) ([264]), ako aj od toho, či sa právomoc uplatňuje na konkrétny cieľ, alebo hromadne. Podrobnosti o rozsahu, zárukách a obmedzeniach každého opatrenia, ktoré je stanovené v zákone o vyšetrovacích právomociach z roku 2016, sú opísané ďalej v osobitných oddieloch.

(179) Zákon o vyšetrovacích právomociach z roku 2016 navyše dopĺňajú viaceré zákonné kódexy postupov vydané ministrom, schválené obidvomi snemovňami parlamentu ([265]) a platné v celej krajine, pričom tieto kódexy poskytujú usmernenia k využívaniu týchto právomocí ([266]). Zatiaľ čo sa dotknuté osoby môžu spoľahnúť priamo na ustanovenia uvedené v zákone o vyšetrovacích právomociach z roku 2016, v bode 5 prílohy 7 k zákonu o vyšetrovacích právomociach z roku 2016 stanovuje, že kódexy postupov sú prípustné ako dôkaz v občianskych a trestných konaniach a súd, tribunál alebo dozorný orgán môže zohľadniť prípadné nedodržiavanie kódexov pri stanovovaní relevantnej otázky v súdnom konaní ([267]). Veľká komora Európskeho súdu pre ľudské práva v rámci svojho posúdenia „kvality práva“ predchádzajúcich právnych predpisov Spojeného kráľovstva v oblasti sledovania, zákona o regulácii vyšetrovacích právomocí z roku 2000, výslovne uznala relevantnosť kódexov postupov Spojeného kráľovstva a uznala, že ich ustanovenia by mohli byť zohľadnené pri posudzovaní predvídateľnosti právnych predpisov umožňujúcich sledovanie ([268]).

(180) Takisto je potrebné poznamenať, že cielené právomoci (cielené zachytávanie ([269]), získavanie údajov o komunikácii ([270]), uchovávanie údajov o komunikácii ([271]) a cielené zasahovanie do zariadení ([272])) sú k dispozícii národným bezpečnostným službám a určitým orgánom presadzovania práva ([273]), zatiaľ čo len spravodajské služby môžu využívať hromadné právomoci (t. j. hromadné zachytávanie ([274]), hromadné získavanie údajov o komunikácii ([275]), hromadné zasahovanie do zariadení ([276]) a súbory hromadných osobných údajov ([277])).

(181) Pri rozhodovaní o tom, ktorá vyšetrovacia právomoc sa má využiť, musí spravodajská služba dodržiavať „všeobecné povinnosti týkajúce sa súkromia“ uvedené v § 2 ods. 2 písm. a) zákona o vyšetrovacích právomociach z roku 2016, ktoré zahŕňajú overenie kritéria nevyhnutnosti a proporcionality. Presnejšie povedané, podľa tohto ustanovenia musí orgán verejnej moci zamýšľajúci využiť vyšetrovaciu právomoc zvážiť i) či by sa to, čo sa má dosiahnuť príkazom, povolením alebo oznámením, mohlo primerane dosiahnuť inými menej rušivými prostriedkami; ii) či úroveň ochrany, ktorá sa má uplatňovať v súvislosti s akýmkoľvek získavaním údajov na základe príkazu, povolenia

([264]) Pokiaľ ide napríklad o rozsah takých opatrení, podľa časti 3 a časti 4 (uchovávanie a získavanie údajov o komunikácii) je rozsah opatrenia úzko spojený s vymedzením pojmu „telekomunikační operátori“, na ktorých používateľské údaje sa vzťahuje opatrenie. Ďalší príklad môže byť uvedený v súvislosti s používaním „hromadných“ právomocí. V tomto prípade je rozsah uplatňovania týchto právomocí obmedzený na „komunikáciu odoslanú alebo prijatú jednotlivcami mimo Britských ostrovov“.

([265]) V prílohe 7 zákona o vyšetrovacích právomociach z roku 2016 sa stanovuje rozsah kódexov, postup, ktorý sa má dodržiavať pri ich vydávaní, pravidlá ich revízie a ich účinok.

([266]) Kódexy postupov podľa zákona o vyšetrovacích právomociach z roku 2016 sú k dispozícii na tomto odkaze: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice.

([267]) Súdy a tribunály používajú kódexy postupov na posúdenie zákonnosti konania orgánov. Pozri napríklad vec Dias/Cleveland Police, [2017] UKIPTrib15_586-CH, v ktorej sa tribunál pre kontrolu vyšetrovacích právomocí odvolával na konkrétne časti Kódexu postupov pre údaje o komunikácii, pokiaľ ide o chápanie vymedzenia dôvodu „predchádzať trestnému činu alebo ho odhaliť alebo zabrániť rušeniu verejného poriadku“ používaného na podanie žiadosti o získanie údajov o komunikácii. Kódex bol zahrnutý do odôvodnenia s cieľom zistiť, či sa tento dôvod použil nesprávne. Súd následne dospel k záveru, že napadnuté konanie bolo nezákonné. Súdy takisto hodnotili úroveň záruk dostupných v kódexoch, pozri napr. vec Just for Law Kids/Secretary of State for the Home Department [2019] EWHC 1772 (Admin), v ktorej Vrchný súd zistil, že primárne a sekundárne právne predpisy spolu s vnútornými usmerneniami poskytovali dostatočné záruky, alebo vec R (National Council for Civil Liberties)/Secretary of State for the Home Department & Others [2019] EWHC 2057 (Admin), v ktorej zistil, že zákon o vyšetrovacích právomociach z roku 2016 a Kódex postupov pre zasahovanie do zariadení obsahoval dostatočné ustanovenia, pokiaľ ide o potrebu konkrétnosti príkazov.

([268]) Vo veci Big Brother Watch veľká komora Európskeho súdu pre ľudské práva uviedla, že „Kódex postupov pre zachytávanie komunikácie je verejným dokumentom schváleným obidvomi snemovňami parlamentu, ktorý vláda uverejňuje online aj v tlačenej podobe a ktorý musí byť zohľadnený tak osobami vykonávajúcimi úlohy v oblasti zachytávania, ako aj súdmi (pozri body 93 – 94). V dôsledku toho súd pripustil, že jeho ustanovenia by sa mohli zohľadňovať pri posudzovaní predvídateľnosti zákona o regulácii vyšetrovacích právomocí (pozri Kennedy, citované v predchádzajúcom texte, § 157). Súd by preto pripustil, že vnútroštátne právo bolo primerane „dostupné“; [pozri Európsky súd pre ľudské práva (veľká komora), vec Big Brother Watch and others/United Kingdom, žaloby č. 58170/13, 62322/14 a 24960/15 z 25. mája 2021, bod 366].

([269]) Časť 2 zákona o vyšetrovacích právomociach z roku 2016.

([270]) Časť 3 zákona o vyšetrovacích právomociach z roku 2016.

([271]) Časť 4 zákona o vyšetrovacích právomociach z roku 2016.

([272]) Časť 5 zákona o vyšetrovacích právomociach z roku 2016.

([273]) Zoznam príslušných orgánov presadzovania práva, ktoré môžu uplatňovať cielené vyšetrovacie právomoci podľa zákona o vyšetrovacích právomociach z roku 2016, sa nachádzajú v predchádzajúcej poznámke pod čiarou č. 139.

([274]) § 136 zákona o vyšetrovacích právomociach z roku 2016.

([275]) § 158 zákona o vyšetrovacích právomociach z roku 2016.

([276]) § 176 zákona o vyšetrovacích právomociach z roku 2016.

([277]) § 199 zákona o vyšetrovacích právomociach z roku 2016.

alebo oznámenia, je vyššia z dôvodu osobitnej citlivosti týchto údajov; iii) verejný záujem na integrite a bezpečnosti telekomunikačných systémov a poštových služieb a iv) akékoľvek iné aspekty verejného záujmu na ochrane súkromia ([278]).

(182) Spôsob, akým by sa mali uplatňovať tieto kritériá, a spôsob posudzovania ich dodržiavania v rámci povolenia na využitie týchto právomocí vydaného ministrom a nezávislými Komisármi pre justíciu sa podrobnejšie uvádzajú v príslušných kódexoch postupov. Využitie ktorejkoľvek z týchto vyšetrovacích právomocí musí byť vždy „primerané tomu, čo sa má dosiahnuť, [čo] so sebou prináša vyváženie závažnosti narušenia súkromia (a iné posúdenia stanovené v § 2 ods. 2) úmerne k nevyhnutnosti tejto činnosti z vyšetrovacieho alebo operačného hľadiska, prípadne hľadiska spôsobilosti“. Znamená to, že „by malo poskytovať realistické vyhliadky na dosiahnutie očakávaného prínosu a nemalo by byť neprimerané ani svojvoľné“ a „[ž]iadne zasahovanie do súkromia by sa nemalo považovať za primerané, ak by sa žiadané informácie mohli primerane získať inými menej rušivými prostriedkami“ ([279]). Dodržiavanie zásady proporcionality sa konkrétne musí posúdiť vzhľadom na tieto kritériá: „i) rozsah navrhovaného zasahovania do súkromia oproti tomu, čo sa má dosiahnuť; ii) ako a prečo spôsobia metódy, ktoré sa majú použiť, čo najmenšie zasiahnutie vo vzťahu k danej osobe a k iným; iii) či táto činnosť predstavuje náležité uplatnenie zákona a primeraný spôsob dosiahnutia toho, čo sa má dosiahnuť, po zvážení všetkých primeraných alternatív; iv) ktoré iné vhodné metódy sa buď neuplatnili, alebo sa použili a zhodnotili sa ako nedostatočné na splnenie operačných cieľov bez použitia navrhovanej vyšetrovacej právomoci“ ([280]).

(183) Ako vysvetľujú orgány Spojeného kráľovstva, v praxi sa tým zabezpečuje, že spravodajská služba najskôr stanoví operatívny cieľ (čím sa vymedzí získavanie, napr. na účely medzinárodného boja proti terorizmu v konkrétnej zemepisnej oblasti) a následne na základe operačného cieľa bude musieť zvážiť, ktorá technická možnosť (napr. cielené alebo hromadné zachytávanie, zasahovanie do zariadení, získavanie údajov o komunikácii) je najprimeranejšia (t. j. najmenej narúšajúca súkromie – pozri § 2 ods. 2 zákona o vyšetrovacích právomociach) tomu, čo sa má dosiahnuť, a preto sa môže povoliť v rámci jedného z dostupných zákonných rámcov.

(184) Je potrebné poznamenať, že takéto opieranie sa o normy nevyhnutnosti a proporcionality takisto zobral na vedomie a uvítal osobitný spravodajca OSN pre právo na súkromie Joseph Cannataci, ktorý sa v súvislosti so systémom zriadeným zákonom o vyšetrovacích právomociach z roku 2016 vyjadril, že „sa zdá, že postupy zavedené v spravodajských službách, ako aj v orgánoch presadzovania práva si systematicky vyžadujú posúdenie nevyhnutnosti a proporcionality opatrenia alebo operácie v oblasti sledovania pred tým, ako sa odporučí na schválenie, ako aj jeho preskúmanie z rovnakého dôvodu“ ([281]). Takisto poznamenal, že na tomto stretnutí so zástupcami orgánov presadzovania práva a národných bezpečnostných služieb „nadobudol jednoznačný dojem, že pri akomkoľvek rozhodnutí týkajúcom sa opatrení v oblasti sledovania sa musí v prvom rade zohľadňovať právo na súkromie. Všetci pochopili a uvedomovali si nevyhnutnosť a proporcionalitu ako hlavné zásady, ktoré sa majú zohľadňovať“.

([278]) V Kódexe postupov pre zachytávanie komunikácie sa stanovuje, že ďalšími prvkami kritéria proporcionality sú: „i) rozsah navrhovaného zasahovania do súkromia oproti tomu, čo sa má dosiahnuť; ii) ako a prečo spôsobia metódy, ktoré sa majú použiť, čo najmenšie zasiahnutie vo vzťahu k danej osobe a k iným; iii) či táto činnosť predstavuje náležité uplatnenie zákona a primeraný spôsob dosiahnutia toho, čo sa má dosiahnuť, po zvážení všetkých primeraných alternatív; iv) ktoré iné vhodné metódy sa buď neuplatnili, alebo sa použili a zhodnotili sa ako nedostatočné na splnenie operačných cieľov bez použitia navrhovanej vyšetrovacej právomoci“. Kódex postupov pre zachytávanie komunikácie, bod 4.16, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([279]) Pozri Kódex postupov pre zachytávanie komunikácie, body 4.12 a 4.15, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([280]) Pozri Kódex postupov pre zachytávanie komunikácie, bod 4.16.

([281]) Záverečná správa z misie osobitného spravodajcu OSN pre právo na súkromie na záver jeho misie v Spojenom kráľovstve Veľkej Británie a Severného Írska, k dispozícii na tomto odkaze: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, bod 1 písm. a).

(185) Osobitné kritériá na vydanie rôznych príkazov, ako aj obmedzenia a záruky zavedené zákonom o vyšetrovacích právomociach z roku 2016 týkajúce sa každej vyšetrovacej právomoci sa podrobne uvádzajú v odôvodneniach 186 až 243.

3.3.1.1.1. Cielené zachytávanie a preskúmanie

(186) Pre cielené zachytávanie existujú tri druhy príkazov: príkaz na cielené zachytávanie ([282]), príkaz na cielené preskúmanie a príkaz na vzájomnú pomoc ([283]). Podmienky na získanie takých príkazov, ako aj príslušné záruky sú stanovené v časti 2 kapitole 1 zákona o vyšetrovacích právomociach z roku 2016.

(187) Príkazom na cielené zachytávanie sa povoľuje zachytávanie komunikácie opísanej v príkaze počas ich prenosu a získavanie ďalších údajov relevantných pre túto komunikáciu ([284]) vrátane sekundárnych údajov ([285]). Príkaz na cielené preskúmanie povoľuje osobe uskutočniť výber na preskúmanie zachyteného obsahu získaného na základe príkazu na hromadné zachytávanie ([286]).

(188) Akýkoľvek príkaz podľa časti 2 zákona o vyšetrovacích právomociach z roku 2016 môže byť vydaný ministrom ([287]) a schválený Komisárom pre justíciu ([288]). Vo všetkých prípadoch je trvanie akéhokoľvek druhu cieleného príkazu obmedzené na šesť mesiacov ([289]) a na jeho zmenu ([290]) a obnovenie ([291]) sa vzťahujú osobitné pravidlá.

(189) Pred vydaním príkazu musí minister vykonať posúdenie nevyhnutnosti a proporcionality ([292]). V prípade príkazu na cielené zachytávanie a príkazu na cielené preskúmanie by minister mal konkrétne overiť, či je opatrenie nevyhnutné z jedného z týchto dôvodov: v záujme národnej bezpečnosti; predchádzanie alebo odhaľovanie závažnej trestnej činnosti; v záujme hospodárskeho blahobytu Spojeného kráľovstva ([293]), pokiaľ tento záujem súvisí aj so záujmami národnej bezpečnosti ([294]). Na druhej strane možno príkaz na vzájomnú pomoc (pozri odôvodnenie 139) vydať len vtedy, keď sa minister domnieva, že existujú okolnosti zodpovedajúce okolnostiam, v ktorej by vydal príkaz na účel predchádzania alebo odhalenia závažnej trestnej činnosti ([295]).

(190) Okrem toho by minister mal posúdiť, či je opatrenie primerané tomu, čo sa má dosiahnuť ([296]). Posúdenie proporcionality žiadaných opatrení musí zohľadňovať všeobecné povinnosti súvisiace so súkromím uvedené v § 2 ods. 2 zákona o vyšetrovacích právomociach z roku 2016, najmä potrebu posúdiť, či to, čo sa má dosiahnuť

([282]) § 15 ods. 2 zákona o vyšetrovacích právomociach z roku 2016.
([283]) § 15 ods. 4 zákona o vyšetrovacích právomociach z roku 2016.
([284]) § 15 ods. 2 zákona o vyšetrovacích právomociach z roku 2016.
([285]) Sekundárne údaje sú údaje pripojené alebo logicky súvisiace so zachytenou komunikáciou, možno ich od nej logicky oddeliť a keby sa takto oddelili, neodhalili by nič, čo by sa mohlo opodstatnene považovať za zmysel komunikácie (ak ho má). Medzi príklady sekundárnych údajov patria konfigurácie smerovačov alebo firewall, alebo čas, počas ktorého bol smerovač aktívny na sieti, keď je súčasťou zachytávania komunikácie, je ku komunikácii pripojený alebo s ňou logicky súvisí. Viac podrobností sa nachádza v § 16 zákona o vyšetrovacích právomociach z roku 2016 a Kódexe postupov pre zachytávanie komunikácie, bod 2.19, pozri poznámku pod čiarou č. 278.
([286]) Toto preskúmanie sa vykonáva ako výnimka z § 152 ods. 4 zákona o vyšetrovacích právomociach z roku 2016, v ktorom sa stanovuje zákaz pokusov o identifikáciu komunikácie osôb, ktoré sa nachádzajú na Britských ostrovoch. Pozri odôvodnenie 229.
([287]) Škótsky minister schvaľuje príkaz, keď sa týka závažnej trestnej činnosti v Škótsku (pozri § 21 a 22 zákona o vyšetrovacích právomociach z roku 2016), zatiaľ čo minister môže určiť vyššieho úradníka, ktorý vydá príkaz na vzájomnú pomoc, keď sa zdá, že zachytávanie sa bude týkať osoby alebo priestorov nachádzajúcich sa mimo Spojeného kráľovstva (§ 40 zákona o vyšetrovacích právomociach z roku 2016).
([288]) § 19 a § 23 zákona o vyšetrovacích právomociach z roku 2016.
([289]) § 32 zákona o vyšetrovacích právomociach z roku 2016.
([290]) § 39 zákona o vyšetrovacích právomociach z roku 2016. Stanovené osoby môžu uskutočniť obmedzené zmeny príkazov za podmienok uvedených v zákone o vyšetrovacích právomociach z roku 2016. Osoba, ktorá príkaz vydala, ho môže kedykoľvek zrušiť. Musí to urobiť, ak už príkaz nie je nevyhnutný zo žiadneho relevantného dôvodu alebo konanie povolené na základe príkazu už nie je primerané tomu, čo sa má dosiahnuť.
([291]) § 33 zákona o vyšetrovacích právomociach z roku 2016. Rozhodnutie o obnovení príkazu musí schváliť Komisár pre justíciu.
([292]) § 19 zákona o vyšetrovacích právomociach z roku 2016.
([293]) Pokiaľ ide o „záujem hospodárskeho blahobytu Spojeného kráľovstva, ak tento záujem priamo súvisí aj s národnou bezpečnosťou“, pozri vec Big Brother Watch and others/United Kingdom (pozri poznámku pod čiarou č. 268, bod 371), v ktorej veľká komora Európskeho súdu pre ľudské práva konštatovala, že táto koncepcia je dostatočne zameraná na národnú bezpečnosť. Kým v tomto prípade sa konštatovanie súdu týkalo používania koncepcie v zákone o regulácii vyšetrovacích právomocí z roku 2000, rovnaká koncepcia je použitá v zákone o vyšetrovacích právomociach z roku 2016.
([294]) § 20 ods. 2 zákona o vyšetrovacích právomociach z roku 2016.
([295]) § 20 ods. 3 zákona o vyšetrovacích právomociach z roku 2016.
([296]) § 19 ods. 1 písm. b), § 19 ods. 2 písm. b) a § 19 ods. 3 písm. b) zákona o vyšetrovacích právomociach z roku 2016.

príkazom, povolením alebo oznámením, by bolo možné primerane dosiahnuť inými menej rušivými prostriedkami, a či úroveň ochrany, ktorá sa má uplatňovať v súvislosti s akýmkoľvek získavaním údajov na základe príkazu, je vyššia z dôvodu osobitnej citlivosti týchto údajov (pozri odôvodnenie 181).

(191) S týmto cieľom musí minister zohľadniť všetky prvky žiadosti uvedené orgánom predkladajúcim žiadosť, najmä prvky týkajúce sa osôb, ktorých komunikácia sa má zachytávať, a dôležitosť opatrenia pre vyšetrovanie. Tieto prvky sa podrobne uvádzajú v Kódexe postupov pre zachytávanie komunikácie a musia byť opísané s určitou mierou konkrétnosti ([297]). Okrem toho sa v § 17 zákona o vyšetrovacích právomociach z roku 2016 vyžaduje, aby sa v každom príkaze vydanom na základe jeho kapitoly 2 menovite uvádzala alebo opisovala konkrétna osoba alebo skupina osôb, organizácia alebo priestory, v súvislosti s ktorými sa má zachytávať komunikácia („cieľ"). Pokiaľ ide o príkaz na cielené zachytávanie alebo príkaz na cielené preskúmanie, môžu sa týkať skupiny osôb, viac ako jednej osoby alebo organizácie alebo viac ako jedného priestoru (takisto tzv. tematický príkaz) ([298]). V týchto prípadoch by sa v príkaze mal opisovať spoločný účel alebo činnosť, ktorá sa spoločne týka skupiny osôb alebo operácie/vyšetrovania, a mal by sa v ňom menovite uvádzať alebo opisovať taký počet týchto osôb/organizácií alebo priestorov, aký je primerane možný ([299]). Napokon sa vo všetkých príkazoch vydaných na základe časti 2 zákona o vyšetrovacích právomociach z roku 2016 musia uvádzať adresy, čísla, zariadenia, faktory alebo kombinácie faktorov, ktoré sa majú použiť na identifikáciu komunikácie ([300]). V tejto súvislosti sa v Kódexe postupov pre zachytávanie komunikácie stanovuje, že v prípade príkazu na cielené zachytávanie a príkazu na cielené preskúmanie „sa v príkaze musia uvádzať (alebo opisovať) faktory alebo kombinácia faktorov, ktoré sa majú používať na identifikáciu komunikácie. Ak sa komunikácia má identifikovať (napríklad) na základe odkazu na telefónne číslo, číslo musí byť špecifikované uvedením celej podoby. Ak sa však na identifikáciu komunikácie majú použiť veľmi zložité alebo neustále sa meniace internetové selektory, tieto selektory by mali byť opísané v čo najväčšej miere" ([301]).

(192) Dôležitou zárukou v tejto súvislosti je to, že posúdenie vykonané ministrom na účely vydania príkazu musí schváliť nezávislý Komisár pre justíciu ([302]), ktorý najmä preverí, či je rozhodnutie vydať príkaz v súlade so zásadami nevyhnutnosti a proporcionality ([303]) (viac informácií o postavení a úlohe Komisárov pre justíciu sa nachádza v odôvodneniach 251 až 256). V zákone o vyšetrovacích právomociach z roku 2016 sa takisto vysvetľuje, že pri tomto preverovaní musí Komisár pre justíciu uplatňovať rovnaké zásady, ako by uplatňoval súd pri žiadosti o súdne preskúmanie ([304]). Tým sa zabezpečí, že v každom prípade a pred získaním prístupu k údajom nezávislý orgán systematicky kontroluje zásadu nevyhnutnosti a proporcionality.

(193) V zákone o vyšetrovacích právomociach z roku 2016 sa stanovuje niekoľko konkrétnych a úzko vymedzených výnimiek na vykonanie cieleného zachytávania bez príkazu. Obmedzené prípady sú podrobne uvedené v zákone ([305]) a okrem jedného založeného na „súhlase" odosielateľa/prijímateľa ich vykonávajú osoby (súkromné alebo verejné orgány) iné ako národné bezpečnostné služby. Tento druh zachytávania sa vykonáva na účely iné ako zhromažďovanie „spravodajských informácií" ([306]) a pre niektoré z nich je veľmi nepravdepodobné, že získavanie sa

([297]) Medzi požadované informácie patria podrobnosti o kontexte (opis osôb/organizácií/priestorov, komunikácia, ktorá sa má zachytávať) a prínos, ktorý bude mať získanie týchto informácií pre vyšetrovanie, ako aj opis konania, ktoré sa má schváliť. V prípade, že nemožno opísať osoby/organizácie/priestory, je potrebné zahrnúť vysvetlenie, prečo to nie je možné alebo prečo je opis len všeobecný (Kódex postupov pre zachytávanie komunikácie, body 5.32 a 5.34, pozri poznámku pod čiarou č. 278).

([298]) § 17 ods. 2 zákona o vyšetrovacích právomociach z roku 2016. Pozri takisto Kódex postupov pre zachytávanie komunikácie, bod 5.11 a nasl., pozri poznámku pod čiarou č. 278.

([299]) § 31 ods. 4 a 5 zákona o vyšetrovacích právomociach z roku 2016.

([300]) § 31 ods. 8 zákona o vyšetrovacích právomociach z roku 2016.

([301]) Kódex postupov pre zachytávanie komunikácie, body 5.37 a 5.38, pozri poznámku pod čiarou č. 278.

([302]) Schválenie Komisárom pre justíciu sa nevyžaduje, keď sa minister domnieva, že existuje naliehavá potreba vydať príkaz (§ 19 ods. 1 zákona o vyšetrovacích právomociach). Komisára pre justíciu je však v krátkom čase potrebné informovať a musí sa rozhodnúť, či príkaz schváli. Ak tak neurobí, príkaz stráca účinnosť (§ 24 a § 25 zákona o vyšetrovacích právomociach z roku 2016).

([303]) § 23 ods. 1 zákona o vyšetrovacích právomociach z roku 2016.

([304]) § 23 ods. 2 zákona o vyšetrovacích právomociach z roku 2016.

([305]) Pozri § 44 – § 51 zákona o vyšetrovacích právomociach z roku 2016 a bod 12 Kódexu postupov pre zachytávanie komunikácie (pozri poznámku pod čiarou č. 278).

([306]) To platí napríklad vtedy, keď sa vyžaduje zachytávanie vo väznici alebo v psychiatrickej liečebni (na kontrolu správania zaistenej osoby alebo pacienta), alebo ak ho vykonáva telekomunikačný operátor napríklad na odhalenie hanlivého obsahu.

môže uskutočniť v rámci scenára „prenosu“ (napríklad v prípade zachytávania v psychiatrických liečebniach alebo vo väzniciach). Vzhľadom na charakter orgánu, na ktorý sa tieto konkrétne prípady vzťahujú (iné ako národné bezpečnostné služby), sa budú uplatňovať všetky záruky uvedené v časti 2 zákona o ochrane údajov z roku 2018 a vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov vrátane dohľadu Komisára pre informácie a dostupných mechanizmov nápravy. Okrem záruk, ktoré sú stanovené v zákone o ochrane údajov z roku 2018, sa v zákone o vyšetrovacích právomociach z roku 2016 pre isté prípady stanovuje dohľad *ex post* úradu Komisára pre vyšetrovacie právomoci ([307]).

(194) Keď sa vykonáva zachytávanie, vzhľadom na osobitné postavenie osoby (osôb), ktorých komunikácia sa zachytáva ([308]), sa uplatňujú dodatočné obmedzenia a záruky. Napríklad zachytávanie položiek podliehajúcich povinnosti advokáta zachovávať mlčanlivosť sa povoľuje len v prípade výnimočných a závažných okolností, pričom osoba vydávajúca príkaz musí zohľadňovať verejný záujem na dôvernosti položiek podliehajúcich povinnosti advokáta zachovávať mlčanlivosť a skutočnosť, že pre zaobchádzanie s takýmto materiálom, jeho uchovávanie a poskytovanie platia osobitné požiadavky ([309]).

(195) Okrem toho sa v zákone o vyšetrovacích právomociach z roku 2016 stanovujú osobitné záruky týkajúce sa bezpečnosti, uchovávania a poskytovania, ktoré by mal minister zohľadňovať pri vydávaní cieleného príkazu ([310]). Najmä v § 53 ods. 5 zákona o vyšetrovacích právomociach z roku 2016 sa vyžaduje, aby sa každá vytvorená kópia tohto materiálu bezpečne uchovávala a zničila v okamihu, keď už neexistujú relevantné dôvody na jej uchovávanie, pričom sa na základe ustanovení v § 53 ods. 2 zákona o vyšetrovacích právomociach z roku 2016 vyžaduje, aby sa počet osôb, ktorým sa materiál poskytuje, a rozsah jeho poskytnutia, sprístupnenia alebo kopírovania obmedzili na úplné minimum, ktoré je nevyhnutné na zákonné účely.

(196) Napokon, ak sa má materiál zachytený na základe príkazu na cielené zachytávanie alebo príkazu na vzájomnú pomoc odovzdať tretej krajine (ďalej len „poskytovanie údajov do zahraničia“), v zákone o vyšetrovacích právomociach z roku 2016 sa stanovuje, že minister musí zabezpečiť zavedenie primeraných opatrení, ktorými sa v danej tretej krajine zabezpečí existencia podobných záruk týkajúcich sa bezpečnosti, uchovávania a poskytovania ([311]). Navyše v § 109 ods. 2 zákona o ochrane údajov z roku 2018 sa uvádza, že spravodajské služby môžu prenášať údaje mimo územia Spojeného kráľovstva len vtedy, keď je prenos nevyhnutným a primeraným opatrením vykonávaným na účely plnenia zákonných funkcií prevádzkovateľa alebo na ďalšie účely stanovené v § 2 ods. 2 písm. a) zákona o bezpečnostných službách z roku 1989 alebo § 2 ods. 2 písm. a) a § 4 ods. 2 písm. a) zákona o spravodajských službách z roku 1994 ([312]). Je dôležité, že tieto požiadavky sa vzťahujú aj na prípady, keď sa podľa § 110 zákona o ochrane údajov z roku 2018 uplatní výnimka týkajúca sa národnej bezpečnosti, keďže v § 110 zákona o ochrane údajov z roku 2018 sa § 109 zákona o ochrane údajov z roku 2018 neuvádza ako jedno z ustanovení, ktoré sa môže prestať uplatňovať, ak sa na účely ochrany národnej bezpečnosti vyžaduje výnimka z istých ustanovení.

3.3.1.1.2. Cielené získavanie a uchovávanie údajov o komunikácii

(197) Zákonom o vyšetrovacích právomociach z roku 2016 sa ministrovi povoľuje, aby od telekomunikačných operátorov vyžadoval uchovávanie údajov o komunikácii na účely cieleného prístupu zo strany širokej škály orgánov verejnej moci vrátane orgánov presadzovania práva a spravodajských služieb. V časti 4 zákona o vyšetrovacích právomociach z roku 2016 sa stanovuje uchovávanie údajov o komunikácii, zatiaľ čo v časti 3 sa stanovuje cielené získavanie údajov o komunikácii. V častiach 3 a 4 zákona o vyšetrovacích právomociach z roku 2016 sa takisto uvádzajú osobitné obmedzenia uplatňovania týchto právomocí a stanovujú sa osobitné záruky.

([307]) Pozri a *contrario* § 229 ods. 4 zákona o vyšetrovacích právomociach.

([308]) V § 26 – § 29 zákona o vyšetrovacích právomociach z roku 2016 sa zavádzajú obmedzenia týkajúce sa získania príkazov na cielené zachytávanie a preskúmanie vo vzťahu k zachytávaniu komunikácie odoslanej osobou, ktorá je poslancom parlamentu (ktoréhokoľvek parlamentu Spojeného kráľovstva), alebo komunikácie jej určenej, zachytávaniu položiek podliehajúcich povinnosti advokáta zachovávať mlčanlivosť, zachytávaniu komunikácie, o ktorej sa orgán vykonávajúci zachytávanie domnieva, že obsahuje dôverný žurnalistický materiál a vtedy, keď je účelom príkazu identifikovať alebo potvrdiť zdroj žurnalistických informácií.

([309]) § 26 zákona o vyšetrovacích právomociach z roku 2016.

([310]) § 19 ods. 1 zákona o vyšetrovacích právomociach z roku 2016.

([311]) § 54 zákona o vyšetrovacích právomociach z roku 2016. Záruky týkajúce sa poskytovania materiálu zahraničným orgánom sú bližšie špecifikované v kódexoch postupov: pozri najmä body 9.26 a nasl. a bod 9.87 Kódexu postupov pre zachytávanie komunikácie a body 9.33 a nasl. a bod 9.41 Kódexu postupov pre zasahovanie do zariadení (pozri poznámku pod čiarou č. 278).

([312]) Týmito účelmi sú: predchádzanie závažným trestným činom alebo ich odhaľovanie alebo akékoľvek trestné konanie v prípade bezpečnostných služieb [§ 2 ods. 2 písm. a) zákona o bezpečnostných službách z roku 1989], záujmy národnej bezpečnosti, predchádzanie závažným trestným činom alebo ich odhaľovanie alebo akékoľvek trestné konanie v prípade spravodajských služieb [§ 2 ods. 2 písm. a) zákona o spravodajských službách z roku 1994] a akékoľvek trestné konanie v prípade Vládneho komunikačného ústredia [§ 4 ods. 2 písm. a) zákona o spravodajských službách z roku 1994]. Pozri aj vysvetlivky k zákonu o ochrane údajov z roku 2018, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(198) Pojem „údaje o komunikácii“ zahŕňa otázky „kto“, „kedy“, „kde“ a „ako“ týkajúce sa komunikácie, ale nie obsah, t. j. to, čo sa povedalo alebo napísalo. Na rozdiel od zachytávania nie je získavanie a uchovávanie údajov o komunikácii zamerané na získavanie obsahu komunikácie, ale na získavanie informácií, ako je predplatiteľ telefónnej služby alebo účet s rozpísanými položkami. Mohlo by to zahŕňať čas a trvanie komunikácie, číslo alebo e-mailovú adresu odosielateľa a príjemcu a niekedy polohu zariadení, z ktorých sa telekomunikácia uskutočňovala ([313]).

(199) Je potrebné poznamenať, že uchovávanie a získavanie údajov o komunikácii sa zvyčajne nebude týkať osobných údajov dotknutých osôb z EÚ prenesených do Spojeného kráľovstva na základe tohto rozhodnutia. Povinnosť uchovávať alebo poskytnúť údaje o komunikácii podľa časti 3 a 4 zákona o vyšetrovacích právomociach z roku 2016 sa vzťahuje na údaje, ktoré sú získavané telekomunikačnými operátormi v Spojenom kráľovstve priamo od používateľov telekomunikačných služieb ([314]). Takýto druh spracúvania „orientovaný na zákazníka“ nezahŕňa prenos na základe tohto rozhodnutia, t. j. prenos od prevádzkovateľa/sprostredkovateľa v EÚ k prevádzkovateľovi/sprostredkovateľovi v Spojenom kráľovstve.

(200) V záujme úplnosti sú však v nasledujúcich odôvodneniach zanalyzované podmienky a záruky, ktoré upravujú tieto režimy získavania a uchovávania.

(201) V rámci predpokladu však treba podotknúť, že uchovávanie a cielené získavanie údajov o komunikácii sú dostupné tak národným bezpečnostným službám, ako aj istým orgánom presadzovania práva ([315]). Podmienky na požadovanie uchovávania a/alebo získavania údajov o komunikácii sa môžu líšiť v závislosti od dôvodu žiadosti o opatrenie, konkrétne podľa toho, či ide o účely národnej bezpečnosti, alebo presadzovania práva.

(202) Hoci sa týmto novým režimom zaviedla najmä všeobecná požiadavka povolenia *ex ante* od nezávislého orgánu, ktorá sa uplatní vo všetkých prípadoch, keď sa údaje o komunikácii zachovávajú a/alebo získavajú (buď na účely presadzovania práva, alebo národnej bezpečnosti), v nadväznosti na rozsudok Súdneho dvora ([316]) vo veci Tele2/Watson boli zavedené konkrétne záruky, keď sa opatrenie vyžaduje na účely presadzovania práva. Keď sa uchovávanie alebo získavanie údajov o komunikácii vyžaduje na účely presadzovania práva, povolenie *ex ante* musí vždy udeliť Komisár pre vyšetrovanie právomoci. Neplatí to však, keď sa opatrenie vyžaduje na účely národnej bezpečnosti, pretože, ako sa uvádza ďalej v texte, v niektorých prípadoch môže byť taký druh opatrení povolený iným „jednotlivcom, ktorý udeľuje povolenie“. Nový režim stanovil pre „závažné trestné činy“ prahovú hodnotu, do ktorej môže byť uchovávanie a získavanie údajov o komunikácii povolené ([317]).

([313]) Údaje o komunikácii sa vymedzujú v § 261 ods. 5 zákona o vyšetrovacích právomociach z roku 2016. Údaje o komunikácii sa rozdeľujú na „údaje o udalostiach“ (akékoľvek údaje, ktoré identifikujú alebo opisujú udalosť, či už odkazom na jej polohu, alebo bez odkazu na ňu, v telekomunikačnom systéme alebo pomocou neho, v prípade, že udalosť spočíva v tom, že jeden alebo viaceré subjekty sa zapájajú do konkrétnej činnosti v konkrétnom čase) a „údaje o subjekte“ [akékoľvek údaje, ktoré a) sa týkajú i) subjektu; ii) vzťahu medzi telekomunikačnou službou a subjektom alebo iii) vzťahu medzi akoukoľvek časťou telekomunikačného systému a subjektom; b) sa skladajú z údajov alebo zahŕňajú údaje, ktoré identifikujú alebo opisujú subjekt (či už odkazom na polohu subjektu, alebo bez odkazu na ňu) a c) nepredstavujú údaje o udalosti].

([314]) Vyplýva to z vymedzenia údajov o komunikácii stanoveného v § 261 ods. 5 zákona o vyšetrovacích právomociach z roku 2016, podľa ktorého údaje o komunikácii sú údaje získané telekomunikačným operátorom, ktoré sú buď o používateľovi telekomunikačných služieb a týkajú sa poskytovania týchto služieb, alebo sú obsiahnuté v rámci komunikácie ako jej súčasť, sú k nej pripojené alebo logicky s ňou súvisia (pozri aj Kódex postupov pre údaje o komunikácii, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, body 2.22 až 2.33). Okrem toho sa podľa vymedzenia pojmu telekomunikačný operátor, ktoré je stanovené v § 261 ods. 10 zákona o vyšetrovacích právomociach z roku 2016, vyžaduje, aby bol telekomunikačný operátor osoba, ktorá ponúka alebo poskytuje telekomunikačné služby osobám v Spojenom kráľovstve alebo ktorá poskytuje telekomunikačný systém, ktorý sa (úplne alebo čiastočne) nachádza v Spojenom kráľovstve, alebo ho prevádzkuje. Z uvedených vymedzení jasne vyplýva, že povinnosti podľa zákona o vyšetrovacích právomociach z roku 2016 sa nemôžu uložiť telekomunikačným operátorom, ktorých zariadenia sa nenachádzajú v Spojenom kráľovstve alebo nie sú prevádzkované zo Spojeného kráľovstva a neponúkajú alebo neposkytujú služby osobám v Spojenom kráľovstve (pozri aj Kódex postupov pre údaje o komunikácii, bod 2.1). Ak predplatitelia z EÚ (či už sa nachádzajú v EÚ, alebo Spojenom kráľovstve) využili služby v Spojenom kráľovstve, akúkoľvek komunikáciu v súvislosti s poskytovaním týchto služieb by priamo získal poskytovateľ služieb v Spojenom kráľovstve namiesto toho, aby podliehala prenosu z EÚ.

([315]) Príslušné orgány sa uvádzajú v prílohe 4 k zákonu o vyšetrovacích právomociach z roku 2016 a zahŕňajú policajné zložky, spravodajské služby, niektoré ministerstvá a vládne orgány, Národnú kriminálnu agentúru, daňové a colné orgány jej veličenstva, Úrad pre hospodársku súťaž a trhy, Komisára pre informácie, ambulančné, požiarne a záchranné služby a napríklad orgány v oblasti zdravotníctva a bezpečnosti potravín.

([316]) Spojené veci C-203/15 a C-698/15, Tele2/Watson, ECLI:EU:C:2016:970).

([317]) Pre získavanie údajov o komunikácii pozri § 61 ods. 7 písm. b) a pre uchovávanie údajov o komunikácii pozri § 87 ods. 10A.

i) *Povolenie na získanie údajov o komunikácii*

(203) Podľa časti 3 zákona o vyšetrovacích právomociach z roku 2016 majú príslušné orgány verejnej moci povolené získavať údaje o komunikácii od telekomunikačného operátora alebo akejkoľvek osoby schopnej získať a poskytnúť tieto údaje. Povolením sa nemusí umožňovať zachytávanie obsahu komunikácie ([318]) a povolenie prestáva byť účinné po uplynutí lehoty jedného mesiaca ([319]) s možnosťou obnovenia v závislosti od dodatočného povolenia ([320]). Získavanie údajov o komunikácii si vyžaduje povolenie od Komisára pre vyšetrovacie právomoci ([321]) (viac informácií o postavení a právomociach Komisára pre vyšetrovacie právomoci sa nachádza v odôvodneniach 250 až 251). Je to tak vždy, keď si získanie údajov o komunikácii vyžiada príslušný orgán presadzovania práva. V § 61 zákona o vyšetrovacích právomociach z roku 2016 sa však uvádza, že keď sa údaje získavajú na účely národnej bezpečnosti alebo hospodárskeho blahobytu Spojeného kráľovstva, pokiaľ súvisia s národnou bezpečnosťou alebo keď o ne požiada člen spravodajskej služby na základe § 61 ods. 7 písm. b) ([322]), získavanie môže takisto ([323]) povoliť Komisár pre vyšetrovacie právomoci alebo určený vyšší úradník ([324]). Určený úradník musí byť nezávislý od daného vyšetrovania alebo operácie a musí mať praktické znalosti o zásadách a právnych predpisoch v oblasti ľudských práv, najmä o zásadách nevyhnutnosti a primeranosti ([325]). Rozhodnutie prijaté určeným úradníkom podlieha dohľadu ex post vykonávaného Kominárom pre vyšetrovacie právomoci (informácie o funkciách dohľadu ex post Komisára pre vyšetrovacie právomoci sa nachádza v odôvodnení 254).

(204) Povolenie získavať údaje o komunikácii sa zakladá na posúdení nevyhnutnosti a proporcionality opatrenia. Konkrétnejšie, nevyhnutnosť opatrenia sa posudzuje vzhľadom na dôvody uvedené v právnych predpisoch ([326]). Vzhľadom na cielený charakter tohto opatrenia, musí byť takisto nevyhnutné pre konkrétne vyšetrovanie alebo operáciu ([327]). Ďalšie požiadavky týkajúce sa posudzovania nevyhnutnosti opatrení sú stanovené v Kódexe postupov pre údaje o komunikácii ([328]). Kódex stanovuje najmä to, že žiadosť, ktorú podáva žiadajúci orgán, by mala obsahovať tri základné prvky, ktoré odôvodňujú nevyhnutnosť takejto žiadosti: i) udalosť, ktorá je predmetom vyšetrovania, ako trestný čin alebo poloha zraniteľnej nezvestnej osoby; ii) osoba, o ktorej sa žiadajú údaje, ako podozrivý, svedok alebo nezvestná osoba a ako sa táto osoba spája s udalosťou; a iii) žiadané údaje o komunikácii, ako je telefónne číslo alebo IP adresa, a ako sa tieto údaje vzťahujú na osobu a udalosť ([329]).

(205) Získavanie údajov o komunikácii musí byť navyše primerané tomu, čo sa má dosiahnuť ([330]). V Kódexe postupov pre údaje o komunikácii sa objasňuje, že jednotlivec, ktorý udeľuje povolenie, musí pri uskutočnení takéhoto posúdenia zvážiť „rozsah zásahu do práv a slobôd jednotlivca a konkrétny prínos pre vyšetrovanie alebo operáciu, ktorú vykonáva príslušný orgán verejnej moci v záujme verejnosti“, a že berúc na vedomie všetky aspekty daného prípadu

([318]) § 60 A ods. 6 zákona o vyšetrovacích právomociach z roku 2016.

([319]) Toto obdobie sa skracuje na tri dni, keď sa povolenie vydá z dôvodu naliehavosti [§ 65 ods. 3A zákona o vyšetrovacích právomociach z roku 2016].

([320]) Podľa § 65 zákona o vyšetrovacích právomociach z roku 2016 obnovené povolenie trvá jeden mesiac od dátumu uplynutia platnosti súčasného povolenia. Osoba, ktorá udelila povolenie, môže povolenie kedykoľvek zrušiť, ak sa domnieva, že už nie sú splnené požiadavky.

([321]) § 60 A ods. 1 zákona o vyšetrovacích právomociach z roku 2016. Úrad pre schvaľovanie získavania údajov o komunikácii (Office for Communications Data Authorisations) vykonáva túto úlohu v mene Komisára pre vyšetrovacie právomoci (pozri Kódex postupov pre údaje o komunikácii, bod 5.6).

([322]) Žiadosť na základe § 61 ods. 7 písm. b) zákona o vyšetrovacích právomociach z roku 2016 sa podáva na „príslušné trestné účely“, čo podľa § 61 ods. 7A zákona o vyšetrovacích právomociach z roku 2016 znamená: „v prípade, keď údaje o komunikácii predstavujú úplne alebo čiastočne údaje o udalostiach na účely predchádzania alebo odhaľovania závažnej trestnej činnosti; vo všetkých ostatných prípadoch na účely predchádzania alebo odhaľovania závažnej trestnej činnosti alebo zabraňovania rušeniu verejného poriadku“.

([323]) V Kódexe postupov pre údaje o komunikácii sa uvádza, že „Ak žiadosť týkajúcu sa národnej bezpečnosti možno podať buď na základe § 60A, alebo § 61, rozhodnutie o tom, ktorá možnosť povolenia je v danom prípade najvhodnejšia, prináleží jednotlivým orgánom verejnej moci. Orgány verejnej moci, ktoré chcú využiť možnosť prostredníctvom určeného vyššieho úradníka, by mali mať zavedené jasné usmernenia o tom, kedy je táto možnosť povolenia vhodná.“ (Kódex postupov pre údaje o komunikácii, bod 5. 19, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

([324]) V § 70 ods. 3 zákona o vyšetrovacích právomociach z roku 2016 sa uvádza vymedzenie pojmu „určený úradník“, ktorý sa líši v závislosti od príslušného orgánu verejnej moci (ako sa stanovuje v prílohe 4 k zákonu o vyšetrovacích právomociach z roku 2016).

([325]) Ďalšie podrobnosti o nezávislosti určeného vyššieho úradníka sú uvedené v Kódexe postupov pre údaje o komunikácii (Kódex postupov pre údaje o komunikácii, body 4.12 – 4.17, pozri poznámku pod čiarou č. 323).

([326]) Dôvody: i) národná bezpečnosť; ii) predchádzanie trestnej činnosti alebo jej odhaľovanie alebo zabraňovanie rušeniu verejného poriadku (v prípade „údajov o udalostiach“ len ak ide o závažnú trestnú činnosť); iii) je to v záujme hospodárskeho blahobytu Spojeného kráľovstva, ak však tento záujem súvisí aj so záujmami národnej bezpečnosti; iv) je to v záujme verejnej bezpečnosti; v) ich účelom je zabrániť smrti alebo zraneniu, alebo inému poškodeniu fyzického či duševného zdravia osoby, prípadne zmierniť zranenie alebo poškodenie fyzického či duševného zdravia osoby; vi) pomoc pri vyšetrovaní údajných justičných omylov alebo vii) identifikácia mŕtvej osoby alebo osoby, ktorá sa nedokáže sama identifikovať v dôsledku jej stavu (§ 61 ods. 7 zákona o vyšetrovacích právomociach z roku 2016).

([327]) § 60A ods. 1 písm. b) zákona o vyšetrovacích právomociach z roku 2016.

([328]) Kódex postupov pre údaje o komunikácii, bod 3.3 a ďalšie, pozri poznámku pod čiarou č. 323.

([329]) Kódex postupov pre údaje o komunikácii, bod 3.13, pozri poznámku pod čiarou č. 323.

([330]) § 60 ods. 1 písm. c) zákona o vyšetrovacích právomociach z roku 2016.

„zásah do práv jednotlivca stále nemusí byť odôvodnený, pretože nepriaznivý vplyv na práva iného jednotlivca alebo skupiny jednotlivcov je príliš veľký“. Na konkrétne posúdenie proporcionality opatrenia, kódex navyše uvádza niekoľko prvkov, ktoré by mali byť zahrnuté v žiadosti žiadajúceho orgánu ([331]). Okrem toho treba osobitne posúdiť druh údajov o komunikácii (údaje o „subjekte“ alebo „udalosti“ ([332])), ktoré sa majú získať, pričom treba uprednostniť použitie menej rušivých kategórií údajov ([333]). Kódex postupov pre údaje o komunikácii obsahuje aj pokyny pre povolenia, ktoré zahŕňajú údaje o komunikácii osôb s osobitným povolaním (ako lekári, právnici, novinári, parlamentní poslanci alebo duchovní) ([334]), na ktoré sa vzťahujú dodatočné záruky ([335]).

ii) *Príkaz vyžadujúci uchovávanie údajov o komunikácii*

(206) V časti 4 zákona o vyšetrovacích právomociach z roku 2016 sa stanovujú pravidlá o uchovávaní údajov o komunikácii, a to obzvlášť kritériá, na základe ktorých môže minister vydať príkaz na uchovávanie údajov ([336]). Záruky zavedené v zákone o vyšetrovacích právomociach sú rovnaké, keď sa údaje uchovávajú na účely presadzovania práva alebo v záujme národnej bezpečnosti.

(207) Cieľom vydávania takýchto príkazov je zabezpečiť, aby telekomunikační operátori uchovali počas najviac 12 mesiacov príslušné údaje o komunikácii, ktoré by boli inak vymazané hneď, ako sa stanú nepotrebnými na obchodné účely ([337]). Uchovávané údaje zostanú počas tohto vyžiadaného obdobia prístupné pre prípad, že by ich orgán verejnej moci potreboval získať, a to s povolením na cielené získavanie údajov o komunikácii uvedeným v časti 3 zákona o vyšetrovacích právomociach z roku 2016 a opísaným v odôvodneniach 203 až 205.

(208) Uplatňovanie právomoci, ktorou sa vyžaduje uchovávanie istých údajov, podlieha viacerým obmedzeniam a zárukám. Minister môže vydať príkaz na uchovávanie údajov jednému alebo viacerým operátorom ([338]) iba vtedy, keď sa domnieva, že žiadosť o uchovanie údajov je nevyhnutná na jeden zo zákonných účelov ([339]) a je primeraná tomu, čo sa má dosiahnuť ([340]). Ako sa objasňuje v zákone

([331]) Zahrnuté informácie musia obsahovať: i) opis toho, ako získanie údajov pomôže vyšetrovaniu alebo operácii; ii) vysvetlenie významu žiadaných časových období vrátane toho, ako sú tieto obdobia primerané vyšetrovanej udalosti; iii) vysvetlenie, ako sa odôvodňuje rozsah narušenia súkromia, a to pri zvážení výhod, ktoré tieto údaje prinesú vyšetrovaniu (toto odôvodnenie by malo zahŕňať úvahu nad tým, či by sa na dosiahnutie cieľa nedalo uskutočniť menej rušivé vyšetrovanie); iv) posúdenie práv (najmä v oblasti súkromia a v náležitých prípadoch v oblasti slobody prejavu) jednotlivca a vyváženie týchto práv s výhodami pre vyšetrovanie; v) podrobnosti o tom, aké vedľajšie narušenie súkromia môže nastať a aké môžu mať žiadané časové obdobia vplyv na vedľajšie narušenie súkromia (Kódex postupov pre údaje o komunikácii, body 3.22 – 3.26, pozri poznámku pod čiarou č. 323).

([332]) Pozri poznámku pod čiarou č. 313.

([333]) Pri žiadaní viacej rušivých údajov o komunikácii (t. J. údajov o udalostiach) sa v kódexe špecifikuje, že vhodnejším postupom je najprv získať údaje o subjekte alebo získať priamo údaje o udalosti v niektorých prípadoch s určitou naliehavosťou (Kódex postupov pre údaje o komunikácii, body 6.10 – 6.14, pozri poznámku pod čiarou č. 323).

([334]) Kódex postupov pre údaje o komunikácii, body 8.8 – 8.44, pozri poznámku pod čiarou č. 323.

([335]) V kódexe postupov sa špecifikuje, že „jednotlivec, ktorý udeľuje povolenie, musí dávať obzvlášť pozor pri posudzovaní takýchto žiadostí vrátane dodatočného uváženia, či tieto žiadosti nemôžu mať neúmyselné následky a či žiadosť slúži najlepším záujmom verejnosti“ (Kódex postupov pre údaje o komunikácii, bod 8.8). Okrem toho treba viesť o takomto druhu žiadostí záznamy a pri najbližšej kontrole by takéto žiadosti mali byť označené, aby im Komisár pre vyšetrovacie právomoci venoval pozornosť (Kódex postupov pre údaje o komunikácii, bod 8.10, pozri poznámku pod čiarou č. 323).

([336]) § 87 až § 89 zákona o vyšetrovacích právomociach z roku 2016.

([337]) Podľa § 90 zákona o vyšetrovacích právomociach z roku 2016 telekomunikačný operátor, ktorý dostal príkaz na uchovávanie údajov, môže požiadať o preskúmanie ministrom, ktorý príkaz vydal.

([338]) Podľa § 87 ods. 2 písm. a) zákona o vyšetrovacích právomociach z roku 2016 sa príkaz na uchovávanie údajov môže vzťahovať „na konkrétny operátor alebo akýkoľvek opis operátorov“.

([339]) Účely: i) záujem národnej bezpečnosti; ii) príslušný trestný účel (podľa vymedzenia v § 87 ods. 10A zákona o vyšetrovacích právomociach z roku 2016); iii) je to v záujme hospodárskeho blahobytu Spojeného kráľovstva, ak však tento záujem súvisí aj so záujmami národnej bezpečnosti; iv) je to v záujme verejnej bezpečnosti; v) účelom je zabrániť smrti alebo zraneniu, alebo inému poškodeniu fyzického či duševného zdravia osoby, prípadne zmierniť zranenie alebo poškodenie fyzického či duševného zdravia osoby; alebo vi) účelom je pomáhať pri vyšetrovaní údajných justičných omylov (§ 87 zákona o vyšetrovacích právomociach z roku 2016).

([340]) § 87 zákona o vyšetrovacích právomociach z roku 2016. Podľa príslušného kódexu postupov na posúdenie proporcionality príkazu na uchovávanie údajov sa vzťahujú navyše kritériá uvedené v § 2 ods. 2 zákona a vyšetrovacích právomociach z roku 2016, a to obzvlášť požiadavka na posúdenie, či cieľ príkazu nemožno dosiahnuť menej rušivými prostriedkami. Podobne ako pri posudzovaní proporcionality pri získavaní údajov o komunikácii, v Kódexe postupov pre údaje o komunikácii sa objasňuje, že takéto posudzovanie zahŕňa „zváženie rozsahu zásahu do práv jednotlivca na rešpektovanie súkromného života a konkrétneho prínosu pre vyšetrovanie“ (Kódex postupov pre údaje o komunikácii, bod 16.3, pozri poznámku pod čiarou č. 323).

o vyšetrovacích právomociach z roku 2016 ([341]), minister musí pred vydaním príkazu na uchovávanie údajov zohľadniť: možné výhody príkazu ([342]); opis telekomunikačných služieb; či je vhodné obmedziť údaje, ktoré sa majú uchovávať, podľa odkazu na polohu alebo opis osôb, ktorým sa poskytujú telekomunikačné služby ([343]); možný počet používateľov (ak je známy) akejkoľvek telekomunikačnej služby, na ktorú sa príkaz vzťahuje ([344]); technickú uskutočniteľnosť splnenia príkazu; možné náklady za splnenie príkazu a akýkoľvek iný následok príkazu pre telekomunikačného operátora (alebo opis operátorov), na ktorého sa príkaz vzťahuje ([345]). Ako sa ďalej podrobne uvádza v kapitole 17 Kódexu postupov pre údaje o komunikácii, všetky príkazy na uchovávanie údajov musia špecifikovať každý typ údajov, ktorý sa má uchovávať, a ako každý typ údajov spĺňa potrebné podmienky pre uchovávanie.

(209) Vo všetkých prípadoch (tak na účely národnej bezpečnosti, ako aj presadzovania práva) musí rozhodnutie ministra vydať príkaz na uchovávanie údajov schváliť nezávislý Komisár pre justíciu v rámci takzvaného postupu dvojitého zabezpečenia, ktorý musí preskúmať najmä to, či je príkaz na uchovávanie príslušných údajov o komunikácii nevyhnutný a primeraný jednému alebo viacerým zákonným účelom ([346]).

3.3.1.1.3. Zasahovanie do zariadení

(210) Zasahovanie do zariadení je súbor techník, ktoré sa využívajú na získanie rôznych údajov zo zariadení ([347]), ako sú počítače, tablety a smartfóny, ako aj káble, elektrické rozvody a pamäťové zariadenia ([348]). Zasahovanie do zariadení umožňuje získať obsah komunikácie, ako aj údaje zo zariadení ([349]).

(211) V súlade s § 13 ods. 1 zákona o vyšetrovacích právomociach z roku 2016 je na použitie zasahovania do zariadení spravodajskou službou potrebné povolenie prostredníctvom príkazu v rámci postupu „dvojitého zabezpečenia“ podľa zákona o vyšetrovacích právomociach z roku 2016, a to za predpokladu, že existuje „prepojenie s Britskými ostrovmi“, ([350]). Podľa vysvetlení poskytnutých orgánmi Spojeného kráľovstva v situáciách, keď sa údaje prenášajú

([341]) Pozri § 88 zákona o vyšetrovacích právomociach z roku 2016.

([342]) Výhody môžu už existovať alebo môžu byť očakávané a musia sa vzťahovať na zákonné účely, na ktoré možno uchovávať údaje (Kódex postupov pre údaje o komunikácii, bod 17.17, pozri poznámku pod čiarou č. 323).

([343]) Pri zohľadňovaní sa stanovuje, či je nevyhnutný a primeraný plný zemepisný dosah príkazu na uchovávanie údajov a či je nevyhnutné a primerané zahrnúť alebo vylúčiť akékoľvek konkrétne opisy osôb (Kódex postupov pre údaje o komunikácii, bod 17.17, pozri poznámku pod čiarou č. 323).

([344]) Pomôže to ministrovi zohľadniť rozsah narušenia súkromia zákazníkov, ako aj možné výhody získania údajov, ktoré sa majú uchovávať (Kódex postupov pre údaje o komunikácii, bod 17.17, pozri poznámku pod čiarou č. 323).

([345]) § 88 zákona o vyšetrovacích právomociach z roku 2016.

([346]) § 89 zákona o vyšetrovacích právomociach z roku 2016.

([347]) Podľa § 135 ods. 1 a § 198 ods. 1 zákona o vyšetrovacích právomociach z roku 2016 pojem „zariadenie“ zahŕňa zariadenia, ktoré vydávajú elektromagnetické, akustické alebo iné emisie, a akýkoľvek nástroj, ktorý možno použiť v spojení s takýmto zariadením.

([348]) Kódex postupov pre zasahovanie do zariadení, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, bod 2.2.

([349]) Údaje zo zariadení sa vymedzujú v § 100 zákona o vyšetrovacích právomociach z roku 2016 ako systémové údaje a údaje, ktoré a) sú súčasťou komunikácie (buď zo strany odosielateľa, alebo naopak) alebo akejkoľvek inej informácie, sú v nej zahrnuté, k nej pripojené alebo logicky s ňou súvisia; b) sa môžu logicky oddeliť od ostatnej komunikácie alebo informácie a c) ak by sa takto oddelili, neodhalili by nič, čo možno odôvodnene považovať za zmysel (ak nejaký existuje) komunikácie alebo informácie.

([350]) Na to, aby bola požiadavka na príkaz povinná, v § 13 ods. 1 zákona o vyšetrovacích právomociach z roku 2016 sa vyžaduje aj to, aby konanie spravodajskej služby predstavovalo jeden alebo viacero trestných činov podľa § 1 až 3A zákona o zneužívaní počítačov z roku 1990 (Computer Misuse Act), čo by bolo pravdou v prevažnej väčšine okolností (pozri Kódex postupov pre zasahovanie do zariadení, body 3.32 a 3.6 – 3.9). Podľa § 13 ods. 2 zákona o vyšetrovacích právomociach z roku 2016 „prepojenie s Britskými ostrovmi“ existuje, ak a) sa ktorékoľvek konanie odohralo na Britských ostrovoch (bez ohľadu na polohu zariadenia, do ktorého by sa malo alebo sa môže zasahovať); b) sa spravodajská služba domnieva, že ktorékoľvek zariadenie, do ktorého by sa malo alebo sa môže zasahovať, niekedy v čase zasahovania by sa mohlo alebo môže nachádzať na Britských ostrovoch; alebo c) cieľom zasahovania je získať i) komunikáciu zaslanú osobou alebo osobe, ktorá sa v tom čase nachádza alebo o ktorej sa spravodajské služby domnievajú, že sa v tom čase nachádza na Britských ostrovoch; ii) súkromné informácie vzťahujúce sa na jednotlivca, ktorý sa v tom čase nachádza alebo o ktorom sa spravodajské služby domnievajú, že sa v tom čase nachádza na Britských ostrovoch; alebo iii) údaje zo zariadení, ktoré sú súčasťou komunikácie či súkromnej informácie, ktoré patria do pododsekov i) a ii), alebo sú s takou komunikáciou či informáciou spojené.

z Európskej únie do Spojeného kráľovstva v zmysle tohto rozhodnutia, bude vždy existovať „prepojenie s Britskými ostrovmi“ a akékoľvek zasahovanie do zariadení týkajúce sa takýchto údajov bude preto podliehať povinnej požiadavke na príkaz podľa § 13 ods. 1 zákona o vyšetrovacích právomociach z roku 2016 ([351]).

(212) Pravidlá vzťahujúce sa na príkazy na cielené zasahovanie do zariadení sú stanovené v časti 5 zákona o vyšetrovacích právomociach z roku 2016. Cielené zasahovanie do zariadení sa podobne ako cielené zachytávanie musí vzťahovať na konkrétny „cieľ“, ktorý musí byť uvedený v príkaze ([352]). Podrobnosti o tom, ako treba určiť „cieľ“, závisia od záležitosti a typu zariadenia, do ktorého sa má zasahovať. Konkrétne v § 115 ods. 3 zákona o vyšetrovacích právomociach z roku 2016 sa špecifikujú prvky, ktoré by mali byť zahrnuté v príkaze (napr. meno osoby alebo organizácie, opis polohy) napríklad v závislosti od toho, či sa zasahovanie týka zariadenia, ktoré patrí určitej osobe, organizácii alebo skupine osôb, alebo či ho táto osoba, organizácia alebo skupina osôb používa alebo má v držbe, či sa zariadenie nachádza na určitom mieste atď ([353]). To, na aké ciele možno vydať príkaz na cielené zasahovanie do zariadenia, závisí od žiadajúceho orgánu verejnej moci ([354]).

(213) Vydávajúci orgán je povinný podobne ako v prípade cieleného zachytávania posúdiť, či je opatrenie nevyhnutné na dosiahnutie konkrétneho účelu a či je primerané tomu, čo sa má dosiahnuť ([355]). Okrem toho by mal zvážiť aj to, či existujú záruky týkajúce sa bezpečnosti, uchovávania a poskytovania, ako aj „poskytovania údajov do zahraničia“ ([356]) (pozri odôvodnenie 196).

(214) Príkaz musí schváliť Komisár pre justíciu s výnimkou naliehavých prípadov ([357]). V poslednom uvedenom prípade sa musí Komisár pre justíciu informovať o tom, že sa príkaz vydal, a musí ho schváliť do troch pracovných dní. Ak Komisár pre justíciu odmietne príkaz schváliť, príkaz stráca účinnosť a nemôže sa obnoviť ([358]). Komisár pre justíciu má navyše právomoc vyžadovať vymazanie akýchkoľvek údajov, ktoré boli získané na základe príkazu ([359]). Skutočnosť, že došlo k naliehavému vydaniu príkazu, neovplyvní dohľad *ex post* (pozri odôvodnenia 244 až 255) ani možnosti jednotlivcov žiadať o nápravu (pozri odôvodnenia 260 až 270). Jednotlivci môžu podať sťažnosť Komisárovi pre informácie alebo bežným postupom podať žiadosť tribunálu pre kontrolu vyšetrovacích právomocí, ktorá sa týka akéhokoľvek údajného konania. Komisár pre justíciu pri rozhodovaní sa, či schváliť príkaz, vo všetkých prípadoch overuje kritérium nevyhnutnosti a proporcionality, ktoré sa uplatňuje v prípade žiadostí o cielené zachytávanie ([360]) (pozri odôvodnenie 192).

([351]) Pre úplnosť treba poznamenať, že aj v prípadoch, keď neexistuje „prepojenie s Britskými ostrovmi“ a použitie zasahovania do zariadení teda nepodlieha povinnej požiadavke na príkaz podľa § 13 ods. 1 zákona o vyšetrovacích právomociach z roku 2016, spravodajská služba, ktorá plánuje vykonať činnosť, na ktorú môže získať príkaz na hromadné zasahovanie do zariadení, by mala podľa pravidla (pozri Kódex postupov pre zasahovanie do zariadení, bod 3.24) takýto príkaz získať. Aj keď sa podľa zákona o vyšetrovacích právomociach z roku 2016 príkaz na zasahovanie do zariadení právne nevyžaduje a ani sa podľa pravidla nezíska, činnosti spravodajských služieb podliehajú viacerým podmienkam a obmedzeniam podľa § 7 zákona o spravodajských službách z roku 1994. Patrí sem najmä požiadavka na povolenie ministrom, ktorý sa musí uistiť, že žiadna činnosť nepresiahne hranice toho, čo je nevyhnutné na riadne plnenie funkcií spravodajskej služby.

([352]) § 115 zákona o vyšetrovacích právomociach z roku 2016 upravuje obsah príkazu, pričom špecifikuje, že musí obsahovať meno alebo opis osôb, organizácií, polohy alebo skupiny osôb, ktoré predstavujú „cieľ“, opis podstaty vyšetrovania a opis činností, na ktoré sa zariadenie využíva. Takisto musí opísať druh zariadenia a konanie, ktoré má povolenie vykonať osoba, ktorej je príkaz adresovaný.

([353]) Pozri aj Kódex postupov pre zasahovanie do zariadení, bod 5.7, pozri poznámku pod čiarou č. 348.

([354]) Národné bezpečnostné služby môžu požiadať o príkaz na zasahovanie do zariadení, ak je to nevyhnutné na účely národnej bezpečnosti, na účel odhaľovania závažných trestných činov a/alebo v záujme hospodárskeho blahobytu Spojeného kráľovstva, pokiaľ je tento záujem relevantný aj pre záujmy národnej bezpečnosti (§ 102 až 103 zákona o vyšetrovacích právomociach z roku 2016). V závislosti od dotknutej služby možno o príkaz na zasahovanie do zariadení požiadať na účel presadzovania práva, ak je to nevyhnutné na odhaľovanie závažných trestných činov alebo predchádzanie takýmto činom alebo na účel zabránenia smrti alebo akémukoľvek zraneniu, alebo poškodeniu fyzického či duševného zdravia osoby, prípadne zmiernenia akéhokoľvek zranenia alebo poškodenia fyzického či duševného zdravia osoby (pozri § 106 ods. 1 a 3 zákona o vyšetrovacích právomociach z roku 2016).

([355]) § 102 ods. 1 zákona o vyšetrovacích právomociach z roku 2016.

([356]) § 129 až § 131 zákona o vyšetrovacích právomociach z roku 2016.

([357]) § 109 zákona o vyšetrovacích právomociach z roku 2016.

([358]) § 109 ods. 4 zákona o vyšetrovacích právomociach z roku 2016.

([359]) § 110 ods. 3 písm. b) zákona o vyšetrovacích právomociach z roku 2016. Podľa bodu 5.67 Kódexu postupov pre zasahovanie do zariadení sa naliehavosť určuje podľa toho, či by bolo prakticky možné žiadať Komisára pre justíciu o schválenie vydania príkazu v lehote, ktorá je k dispozícii na splnenie operačnej potreby alebo potreby z hľadiska vyšetrovania. Naliehavé príkazy by mali patriť do jednej alebo oboch z týchto kategórií: i) bezprostredné ohrozenie života alebo ťažká ujma na zdraví – napríklad ak bol jedinec unesený a usudzuje sa, že jeho život je v bezprostrednom ohrození alebo ii) zhromažďovanie spravodajských informácií alebo možnosť vyšetrovania s obmedzeným časom na konanie – napríklad zásielka s drogami triedy A práve vstupuje do Spojeného kráľovstva a orgány presadzovania práva chcú mať informácie o páchateľoch závažnej trestnej činnosti, aby ich mohli zatknúť. Pozri poznámku pod čiarou č. 348.

([360]) § 108 zákona o vyšetrovacích právomociach z roku 2016.

(215) Nakoniec konkrétne záruky uplatniteľné na cielené zachytávanie sa vzťahujú aj na zasahovanie do zariadení v súvislosti s trvaním, obnovou a zmenou príkazu, ako aj na zachytávanie komunikácie poslancov parlamentu, položiek, ktoré podliehajú povinnosti advokáta zachovávať mlčanlivosť, a novinárskeho materiálu (pozri ďalšie podrobnosti v odôvodnení 193).

3.3.1.1.4. Výkon hromadných právomocí

(216) Hromadné právomoci upravuje časť 6 zákona o vyšetrovacích právomociach z roku 2016. Kódexy postupov poskytujú ďalšie podrobnosti o použití hromadných právomocí. Napriek tomu, že v právnych predpisoch Spojeného kráľovstva neexistuje vymedzenie pojmu „hromadná právomoc“, v kontexte zákona o vyšetrovacích právomociach z roku 2016 sa opisuje ako získavanie a uchovávanie veľkého množstva údajov, ktoré vláda získala rôznymi prostriedkami (t. j. právomoc hromadného zachytávania, hromadného získavania, hromadného zasahovania a právomoc týkajúca sa súborov hromadných osobných údajov) a ku ktorým majú následne orgány prístup. Tento opis je objasnený v kontraste s tým, čo nie je „hromadná právomoc“: nejde o tzv. masové sledovanie bez obmedzení alebo záruk. Naopak, ako je vysvetlené v nasledujúcom texte, hromadná právomoc zahŕňa obmedzenia a záruky navrhnuté s cieľom zabezpečiť, aby sa prístup k údajom neposkytoval neuvážene alebo bezdôvodne ([361]). Hromadné právomoci sa konkrétne môžu využiť, len ak existuje prepojenie medzi technickým opatrením, ktoré národná spravodajská služba plánuje použiť, a operačným cieľom, na ktorý sa požaduje.

(217) Okrem toho sú hromadné právomoci dostupné len pre spravodajské služby a vždy sa na ne vzťahuje príkaz, ktorý vydáva minister a schvaľuje Komisár pre justíciu. Pri výbere spôsobu získavania spravodajských informácií sa musí zohľadniť, či daný cieľ možno dosiahnuť „menej rušivými prostriedkami“ ([362]). Tento prístup vychádza z legislatívneho rámca zakladajúceho sa na zásade proporcionality, a preto uprednostňuje cielené získavanie pred hromadným získavaním údajov.

3.3.1.1.4.1. Hromadné zachytávanie a hromadné zasahovanie do zariadení

(218) Systém pre hromadné zachytávanie sa stanovuje v časti 6 kapitole 1 zákona o vyšetrovacích právomociach z roku 2016, pričom sa v kapitole 3 rovnakej časti upravuje hromadné zasahovanie do zariadení. Uvedené systémy sú vo svojej podstate rovnaké, a preto sa podmienky a dodatočné záruky uplatniteľné na tieto príkazy analyzujú spoločne.

i) *Podmienky a kritériá na vydanie príkazu*

(219) Príkaz na hromadné zachytávanie sa obmedzuje na zachytávanie komunikácie počas jej prenosu, ktorú odoslali alebo prijali jednotlivci na území mimo Britských ostrovov ([363]), tzv. zahraničná komunikácia ([364]), ako aj na iné

([361]) V Správe o hromadných právomociach, ktorú predložil lord David Anderson, nezávislý revízor právnych predpisov v oblasti boja proti terorizmu, pred schválením zákona o vyšetrovacích právomociach z roku 2016 sa uvádza, že *“by malo byť jasné, že hromadné získavanie a uchovávanie údajov nepredstavuje tzv. masové sledovanie. Každý právny systém hodný svojho mena bude zahŕňať obmedzenia a záruky navrhnuté s cieľom zabezpečiť, aby sa prístup k citlivým údajom [...] neposkytoval neuvážene alebo bezdôvodne. Tieto obmedzenia a záruky rozhodne figurujú v návrhu zákona*”. Lord David Anderson, Správa o preskúmaní hromadných právomocí, august 2016, bod 1.9 (zvýraznenie bolo doplnené), k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF.

([362]) § 2 ods. 2 zákona o vyšetrovacích právomociach z roku 2016. Pozri napríklad Kódex postupov pre hromadné získavanie údajov o komunikácii, bod 4.11, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf.

([363]) „Britské ostrovy“ pozostávajú zo Spojeného kráľovstva, Normanských ostrovov a Ostrova Man a vymedzujú sa v prílohe 1 k zákonu o výklade z roku 1978 (Interpretation Act), ktorý je k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

([364]) Podľa § 136 zákona o vyšetrovacích právomociach z roku 2016 „zahraničná komunikácia“ je: i) komunikácia odosielaná jednotlivcami, ktorí sa nachádzajú mimo územia Britských ostrovov; alebo ii) komunikácia prijímaná jednotlivcami, ktorí sa nachádzajú mimo územia Britských ostrovov. Systém sa podľa potvrdenia orgánov Spojeného kráľovstva vzťahuje aj na komunikáciu medzi dvoma osobami, ktoré sa nachádzajú mimo územia Britských ostrovov. Veľká komora Európskeho súdu pre ľudské práva konštatovala vo veci Big Brother Watch and others/United Kingdom (pozri poznámku pod čiarou č. 279), bod 376, že pokiaľ ide o podobné obmedzenie (v súvislosti s „externou komunikáciou“) komunikácie, ktorú možno podľa zákona o regulácii vyšetrovacích právomocí z roku 2000 zachytiť prostredníctvom hromadného zachytávania, bolo dostatočne vymedzené a predvídateľné.

relevantné údaje a následný výber zachyteného materiálu na preskúmanie ([365]). Príkazom na hromadné zasahovanie do zariadení ([366]) sa adresátovi povoľuje zaistiť zasahovanie do akéhokoľvek zariadenia na účely získania zahraničnej komunikácie (vrátane čohokoľvek, čo obsahuje reč, hudbu, zvuky, vizuálne obrazy alebo údaje akéhokoľvek druhu), údajov zo zariadení (údaje, ktoré umožňujú alebo uľahčujú fungovanie poštovej služby, telekomunikačného systému, telekomunikačnej služby) alebo akýchkoľvek ďalších informácií ([367]).

(220) Minister môže vydať hromadný príkaz len na základe žiadosti vedúceho spravodajskej služby ([368]). Príkaz, ktorým sa povoľuje hromadné zachytávanie alebo hromadné zasahovanie do zariadení sa musí vydať, len ak je to v záujme národnej bezpečnosti a na ďalší účel predchádzania závažným trestným činom a ich odhaľovania alebo v záujme hospodárskeho blahobytu Spojeného kráľovstva, ak je to relevantné pre národnú bezpečnosť ([369]). Okrem toho § 142 ods. 7 zákona o vyšetrovacích právomociach z roku 2016 vyžaduje, že príkaz na hromadné zachytávanie musí byť špecifikovaný podrobnejšie ako len jednoduchým odkazom na „záujmy národnej bezpečnosti“, „hospodársky blahobyt Spojeného kráľovstva“ a „predchádzanie závažným trestným činom a boj proti nim“, pričom sa v príkaze musí stanoviť prepojenie medzi opatrením, ktoré sa má dosiahnuť, a jedným alebo viacerými operačnými účelmi.

(221) Výber operačného účelu je výsledkom viacvrstvového postupu. Podľa § 142 ods. 4 zákona o vyšetrovacích právomociach z roku 2016 operačné účely uvedené v príkaze musia byť uvedené v zozname udržiavanom vedúcimi spravodajských služieb ako účely, ktoré považujú za operačné účely, na ktoré sa môže zachytený obsah alebo sekundárne údaje získané prostredníctvom príkazov na hromadné zachytávanie vybrať na preskúmanie. Zoznam operačných účelov musí schváliť minister. Minister môže udeliť takéto schválenie iba vtedy, ak je presvedčený, že operačný účel je špecifikovaný podrobnejšie, ako sú všeobecné dôvody na povolenie príkazu (národná bezpečnosť alebo národná bezpečnosť a hospodársky blahobyt, alebo predchádzanie závažným trestným činom) ([370]). Na konci každého príslušného trojmesačného obdobia je minister povinný parlamentnému výboru pre spravodajstvo a bezpečnosť predložiť kópiu zoznamu operačných účelov. Nakoniec predseda vlády musí aspoň raz ročne preskúmať zoznam operačných účelov ([371]). Ako poznamenal Vrchný súd, „[t]ieto sa nemajú bagatelizovať ako bezvýznamné záruky, keďže spoločne vytvárajú spletitý súbor druhov zodpovednosti, ktoré sa dotýkajú parlamentu, ako aj najvyššie postavených členov vlády“ ([372]).

(222) Takýmito operačnými účelmi sa zároveň obmedzuje rozsah výberu zachyteného materiálu pre fázu preskúmania. Výber na preskúmanie akéhokoľvek materiálu získaného na základe hromadného príkazu musí byť odôvodnený so zreteľom na operačné účely. Podľa vysvetlení orgánov Spojeného kráľovstva to znamená, že praktické opatrenia na preskúmanie musí minister posúdiť už vo fáze príkazu, poskytujúc dostatočné podrobnosti na splnenie zákonných povinností podľa § 152 a 193 zákona o vyšetrovacích právomociach z roku 2016 ([373]). Podrobnosti poskytnuté ministrom týkajúce sa týchto opatrení by museli napríklad zahŕňať informácie (ak je to uplatniteľné) o tom, ako sa môžu opatrenia týkajúce sa filtrovania líšiť počas obdobia, na ktoré sa príkaz vzťahuje ([374]). Podrobnejšie informácie o postupe a zárukách, ktoré sa vzťahujú na fázu filtrovania a preskúmania sú uvedené v odôvodnení 229.

([365]) § 136 ods. 4 zákona o vyšetrovacích právomociach z roku 2016. Podľa vysvetlení vlády Spojeného kráľovstva sa môže hromadné zachytávanie použiť napríklad na identifikáciu predtým neznámych hrozieb pre národnú bezpečnosť Spojeného kráľovstva prostredníctvom filtrovania a analýzy zachyteného materiálu s cieľom identifikovať komunikáciu, ktorá má spravodajskú hodnotu (Vysvetľujúci rámec Spojeného kráľovstva, oddiel H s názvom „Národná bezpečnosť“ s. 27 – 28, pozri poznámku pod čiarou č. 29). Podľa vysvetlení orgánov Spojeného kráľovstva sa takéto nástroje môžu použiť na stanovenie prepojení medzi známymi záujmovými osobami, na hľadanie stôp činností jednotlivcov, ktorí ešte nemusia byť známi, ale ktorí sa počas vyšetrovania odhalia, ako aj na identifikáciu vzorcov činnosti, ktorá môže poukazovať na hrozbu pre Spojené kráľovstvo.

([366]) V súlade s § 13 ods. 1 zákona o vyšetrovacích právomociach z roku 2016 je na použitie zasahovania do zariadení spravodajskou službou potrebné povolenie prostredníctvom príkazu podľa zákona o vyšetrovacích právomociach z roku 2016, a to za predpokladu, že existuje „prepojenie s Britskými ostrovmi“, pozri odôvodnenie 211.

([367]) § 176 zákona o vyšetrovacích právomociach z roku 2016. Príkazom na hromadné zasahovanie do zariadení sa nemôže povoliť výkon činnosti, ktorá by predstavovala (ak nie je vykonávaná zo zákonnej právomoci) nezákonné zachytávanie (s výnimkou uchovávanej komunikácie). Získané informácie by mohli byť podľa vysvetľujúceho rámca Spojeného kráľovstva nevyhnutné na identifikáciu záujmových osôb a zvyčajne by boli vhodné pre rozsiahle operácie (Vysvetľujúci rámec Spojeného kráľovstva, oddiel H s názvom „Národná bezpečnosť“ s. 28, pozri poznámku pod čiarou č. 29).

([368]) § 138 ods. 1 a § 178 ods. 1 zákona o vyšetrovacích právomociach z roku 2016.

([369]) § 138 ods. 2 a § 178 ods. 2 zákona o vyšetrovacích právomociach z roku 2016.

([370]) Podľa vysvetlení poskytnutých orgánmi Spojeného kráľovstva sa môže operačným účelom napríklad obmedzovať rozsah opatrenia na prítomnosť hrozby v konkrétnej zemepisnej oblasti.

([371]) § 142 ods. 4 až 10 zákona o vyšetrovacích právomociach z roku 2016.

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

([373]) Ustanovenia § 152 a § 193 zákona o vyšetrovacích právomociach z roku 2016 si vyžadujú, aby: a) výber na preskúmanie bol vykonávaný len na operačné účely uvedené v príkaze, b) výber na preskúmanie bol za každých okolností nevyhnutný a primeraný a c) výber na preskúmanie neporušoval zákaz výberu materiálu a identifikácie komunikácie, ktorá bola odoslaná alebo určená jednotlivcom, ktorí sa v tom čase nachádzajú na Britských ostrovoch.

([374]) Pozri Kódex postupov pre zachytávanie komunikácie, bod 6.6, pozri poznámku pod čiarou č. 278.

(223) Hromadná právomoc sa môže povoliť, len ak je primeraná tomu, čo sa má dosiahnuť ([375]). Ako sa uvádza v Kódexe postupov pre zachytávanie komunikácie, každé posúdenie proporcionality zahŕňa „vyváženie závažnosti narušenia súkromia (a ďalšie posúdenia stanovené v § 2 ods. 2) úmerne k nevyhnutnosti tejto činnosti z vyšetrovacieho alebo operačného hľadiska, prípadne hľadiska spôsobilosti. Povolené konanie by malo ponúknuť realistickú perspektívu týkajúcu sa dosahovania očakávaného prínosu a nemalo by byť neprimerané ani svojvoľné“ ([376]). Ako už bolo uvedené, v praxi to znamená, že overenie kritéria proporcionality vychádza z overenia vyváženosti medzi tým, čo sa má dosiahnuť („operačné účely“), a dostupnými technickými možnosťami (napr. cielené alebo hromadné zachytávanie, zasahovanie do zariadení, získavanie údajov o komunikácií), pričom sa uprednostní najmenej rušivý prostriedok (pozri odôvodnenie 181 a 182). Ak sú na dosahovaný cieľ primerané viaceré opatrenia, musí sa uprednostniť menej rušivý prostriedok.

(224) Dodatočnou zárukou týkajúcou sa posúdenia proporcionality požadovaného opatrenia sa zabezpečuje skutočnosť, že sa na riadny výkon posúdenia musia ministrovi predložiť potrebné príslušné informácie. Konkrétne sa v Kódexe postupov pre zachytávanie komunikácie a Kódexe postupov pre zasahovanie do zariadení vyžaduje, aby žiadosť predložená príslušným orgánom obsahovala podklady žiadosti, opis komunikácie, ktorá sa má zachytávať, a telekomunikačných operátorov, od ktorých sa požaduje spolupráca, opis činnosti, ktorá sa má povoliť, operačné účely, ako aj vysvetlenie, prečo je konanie nevyhnutné a primerané ([377]).

(225) Čo je napokon dôležité, rozhodnutie ministra o vydaní príkazu musí schváliť nezávislý Komisár pre justíciu, ktorý posudzuje hodnotenie nevyhnutnosti a proporcionality navrhovaného opatrenia, pričom využíva rovnaké zásady, ktoré by sa použili na súde pri žiadosti o súdne preskúmanie ([378]). Konkrétnejšie, Komisár pre justíciu preskúma závery ministra o tom, či je príkaz nevyhnutný a či je konanie primerané so zreteľom na zásady stanovené v § 2 ods. 2 zákona o vyšetrovacích právomociach z roku 2016 (všeobecné povinnosti týkajúce sa súkromia). Komisár pre justíciu zároveň preskúma závery ministra o tom, či každý z operačných účelov uvedených v príkaze predstavuje účel, na ktorý je alebo môže byť výber nevyhnutný. Ak Komisár pre justíciu odmietne schváliť rozhodnutie o vydaní príkazu, minister môže: i) akceptovať rozhodnutie a príkaz nevydať alebo ii) vec postúpiť na rozhodnutie Komisárovi pre vyšetrovacie právomoci (pokiaľ pôvodné rozhodnutie nevykonal Komisár pre vyšetrovacie právomoci) ([379]).

ii) *Dodatočné záruky*

(226) Zákonom o vyšetrovacích právomociach z roku 2016 sa zaviedli ďalšie obmedzenia týkajúce sa trvania, obnovy a zmeny hromadného príkazu. Príkaz musí trvať najviac šesť mesiacov a každé rozhodnutie o obnovení alebo zmene (okrem malých zmien) príkazu musí rovnako schváliť Komisár pre justíciu ([380]). V Kódexe postupov pre zachytávanie komunikácie a Kódexe postupov pre zasahovanie do zariadení sa stanovuje, že zmena operačných účelov príkazu sa považuje za zásadnú zmenu príkazu ([381]).

([375]) § 138 ods. 1 písm. b) a c) a § 178 písm. b) a c) zákona o vyšetrovacích právomociach z roku 2016.

([376]) Kódex postupov pre zachytávanie komunikácie, bod 4.10, pozri poznámku pod čiarou č. 278.

([377]) Kódex postupov pre zachytávanie komunikácie, bod 6.20, pozri poznámku pod čiarou č. 278, a Kódex postupov pre zasahovanie do zariadení, bod 6.13, pozri poznámku pod čiarou č. 348.

([378]) § 138 ods. 1 písm. g) a § 178 ods. 1 písm. f) zákona o vyšetrovacích právomociach z roku 2016. Predchádzajúce povolenie od nezávislého orgánu bolo identifikované najmä Európskym súdom pre ľudské práva ako dôležitá záruka proti zneužívaniu v rámci hromadného zachytávania. Európsky súd pre ľudské práva (veľká komora), vec Big Brother Watch and others/United Kingdom, (pozri poznámku pod čiarkou č. 269), body 351 a 352. Je dôležité pripomenúť, že tento rozsudok sa týkal predchádzajúceho právneho rámca (zákona o regulácii vyšetrovacích právomocí z roku 2000), ktorý neobsahoval niektoré záruky (vrátane predchádzajúceho povolenia od nezávislého Komisára pre justíciu), ktoré boli zavedené zákonom o vyšetrovacích právomociach z roku 2016.

([379]) § 159 ods. 3 a 4 zákona o vyšetrovacích právomociach z roku 2016.

([380]) § 143 až § 146 a § 184 až § 188 zákona o vyšetrovacích právomociach z roku 2016. Minister môže v prípade naliehavej zmeny vykonať zmenu bez schválenia, musí však na to upozorniť Komisára, ktorý musí následne rozhodnúť o tom, či zmenu schváli alebo zamietne (§ 147 zákona o vyšetrovacích právomociach z roku 2016). Príkazy musia byť zrušené vtedy, ak už nie sú nevyhnutné alebo primerané alebo ak preskúmanie zachyteného obsahu, metaúdajov alebo iných údajov získaných na základe príkazu už nie je nevyhnutné na ktorýkoľvek z operačných účelov stanovených v príkaze (§ 148 a 189 zákona o vyšetrovacích právomociach z roku 2016).

([381]) Kódex postupov pre zachytávanie komunikácie, body 6.44 až 6.47, pozri poznámku pod čiarou č. 278a Kódex postupov pre zasahovanie do zariadení, bod 6.48, pozri poznámku pod čiarou č. 348.

(227) V časti 6 zákona o vyšetrovacích právomociach z roku 2016 sa podobne ako v prípade cieleného zachytávania stanovuje, že minister musí zabezpečiť zavedenie opatrení, ktorými sa poskytujú záruky týkajúce sa uchovávania a poskytovania materiálu získaného prostredníctvom príkazu ([382]), ako aj v prípade poskytovania údajov do zahraničia ([383]). Konkrétne sa v § 150 ods. 5 a § 191 ods. 5 zákona o vyšetrovacích právomociach z roku 2016 vyžaduje, aby sa každá vytvorená kópia tohto materiálu bezpečne uchovávala a zničila v okamihu, keď už neexistujú relevantné dôvody na jej uchovávanie, pričom sa na základe ustanovení v § 150 ods. 2 a § 191 ods. 2 vyžaduje, aby sa počet osôb, ktorým sa materiál poskytuje, a rozsah jeho poskytnutia, sprístupnenia alebo kopírovania obmedzili na úplné minimum, ktoré je nevyhnutné na zákonné účely ([384]).

(228) Napokon, ak sa má materiál zachytený prostredníctvom hromadného zachytávania alebo hromadného zasahovania do zariadení odovzdať tretej krajine (ďalej len „poskytovanie údajov do zahraničia“), v zákone o vyšetrovacích právomociach z roku 2016 sa stanovuje, že minister musí zabezpečiť zavedenie primeraných opatrení, ktorými sa v danej tretej krajine zabezpečí existencia podobných záruk týkajúcich sa bezpečnosti, uchovávania a poskytovania ([385]). Navyše v § 109 zákona o ochrane údajov z roku 2018 sa stanovujú osobitné požiadavky na medzinárodné prenosy osobných údajov spravodajskými službami do tretích krajín alebo medzinárodným organizáciám, pričom v ňom nie je povolený prenos údajov do krajiny ani na územie mimo Spojeného kráľovstva, ani medzinárodnej organizácii, pokiaľ prenos nie je nevyhnutný a primeraný na účely plnenia zákonných funkcií prevádzkovateľa alebo na ďalšie účely stanovené v § 2 ods. 2 písm. a) zákona o bezpečnostných službách z roku 1989 alebo § 2 ods. 2 písm. a) a § 4 ods. 2 písm. a) zákona o spravodajských službách z roku 1994 ([386]). Je dôležité, že tieto požiadavky sa vzťahujú aj na prípady, keď sa podľa § 110 zákona o ochrane údajov z roku 2018 uplatní výnimka týkajúca sa národnej bezpečnosti, keďže v § 110 zákona o ochrane údajov z roku 2018 sa § 109 zákona o ochrane údajov z roku 2018 neuvádza ako jedno z ustanovení, ktoré sa môže prestať uplatňovať, ak sa na účely ochrany národnej bezpečnosti vyžaduje výnimka z istých ustanovení.

(229) Po schválení príkazu a hromadnom získaní údajov budú údaje pred preskúmaním predmetom výberu. Na fázu výberu a preskúmania sa vzťahuje dodatočné overenie kritéria proporcionality vykonávané analytikom, ktorý na základe operačných účelov obsiahnutých v príkaze (a možných existujúcich opatrení týkajúcich sa filtrovania) vymedzuje kritéria výberu. Ako sa stanovuje v § 152 a 193 zákona o vyšetrovacích právomociach z roku 2016, minister musí pri vydávaní príkazu zabezpečiť, že sú zavedené opatrenia, ktorými sa zaručuje, že výber materiálu sa vykonáva len na stanovené operačné účely a že je za každých okolností primeraný a nevyhnutný. V tejto súvislosti orgány Spojeného kráľovstva vysvetlili, že hromadne zachytený materiál sa v prvom rade vyberá prostredníctvom automatizovaného filtrovania s cieľom odstrániť údaje, v ktorých prípade je nepravdepodobné, že budú predmetom záujmu národnej bezpečnosti. Filtre sa budú z času na čas líšiť (so zmenou vzorcov, druhov a protokolov internetovej komunikácie) a budú závisieť od technológií a operačného kontextu. Po skončení tejto fázy môžu byť údaje vybrané na preskúmanie, len ak sú relevantné pre operačné účely uvedené v príkaze ([387]). Záruky uvedené v zákone o vyšetrovacích právomociach z roku 2016 na preskúmanie získaného materiálu sa uplatňujú na akýkoľvek druh údajov (tak zachyteného obsahu, ako aj sekundárnych údajov) ([388]). V § 152 a 193 zákona o vyšetrovacích právomociach z roku 2016 sa zároveň stanovuje všeobecný zákaz výberu materiálu na preskúmanie, ktorý sa vzťahuje na konverzácie odoslané alebo určené jednotlivcom, ktorí sa nachádzajú na Britských ostrovoch. Ak orgány chcú preskúmať takýto materiál, musia predložiť žiadosť o príkaz na cielené preskúmanie podľa časti 2 a časti 4 zákona o vyšetrovacích právomociach z roku 2016, ktorý vydáva minister a schvaľuje Komisár pre justíciu ([389]). Ak osoba úmyselne vyberie zachytený obsah na preskúmanie v rozpore s požiadavkami stanovenými v právnych predpisoch, ([390]) pácha tak trestný čin ([391]).

([382]) § 156 zákona o vyšetrovacích právomociach z roku 2016.

([383]) § 150 a § 191 zákona o vyšetrovacích právomociach z roku 2016.

([384]) Veľká komora Európskeho súdu pre ľudské práva vo veci Big Brother Watch and others/United Kingdom (pozri poznámku pod čiarou č. 268) potvrdila systém dodatočných záruk na uchovávanie, prístup a poskytovanie, ktorý bol stanovený v rámci zákona o regulácii vyšetrovacích právomocí z roku 2000, pozri body 392 – 394 a 402 – 405. Rovnaký systém záruk je stanovený v zákone o vyšetrovacích právomociach z roku 2016.

([385]) § 151 a § 192 zákona o vyšetrovacích právomociach z roku 2016.

([386]) Viac informácií o týchto účeloch sa nachádza v poznámke pod čiarou č. 312.

([387]) V Kódexe postupov pre zachytávanie komunikácie sa v tejto súvislosti stanovuje, že „Tieto spracovateľské systémy spracúvajú údaje z komunikačných prepojení alebo signálov, ktoré si orgány vykonávajúce zachytávanie vybrali na zachytenie. Stupeň filtrovania sa následne uplatní na komunikáciu v rámci týchto prepojení a signálov, ktoré je navrhnuté na výber komunikácie s potenciálnou spravodajskou hodnotou, pričom sa odstráni tá komunikácia, v ktorej prípade je najmenej pravdepodobné, že má spravodajskú hodnotu. Výsledkom tohto filtrovania, ktoré sa bude líšiť podľa spracovateľských systémov, je automatické odstránenie významnej časti komunikácie na týchto prepojeniach a signáloch. Následne sa môžu vykonať ďalšie komplexné vyhľadávania s cieľom vybrať konkrétne komunikáciu, ktorá má s najväčšou pravdepodobnosťou spravodajskú hodnotu a ktorá sa týka zákonom stanovených funkcií služby. Určená komunikácia sa následne môže vybrať na preskúmanie na jeden alebo viacero operačných účelov uvedených v príkaze za predpokladu, že sú splnené podmienky nevyhnutnosti a proporcionality. Na preskúmanie poverenými osobami sa potenciálne môžu vybrať iba položky, ktoré neboli odfiltrované“ (Kódex postupov pre zachytávanie komunikácie, bod 6.6, pozri poznámku pod čiarou č. 278).

([388]) Pozri § 152 ods. 1 písm. a) a b) zákona o vyšetrovacích právomociach z roku 2016, podľa ktorého sa preskúmanie oboch druhov údajov (zachyteného obsahu a sekundárnych údajov) musí vykonať len na určený účel a za každých okolností musí byť nevyhnutné a primerané.

([389]) Tento druh príkazu sa nepožaduje, ak sú údaje týkajúce sa jednotlivcov, ktorí sa nachádzajú na Britských ostrovoch, „sekundárne údaje“ [pozri § 152 ods. 1 písm. c) zákona o vyšetrovacích právomociach z roku 2016].

([390]) § 152 a § 193 zákona o vyšetrovacích právomociach z roku 2016.

([391]) § 155 a § 196 zákona o vyšetrovacích právomociach z roku 2016.

(230) Na posúdenie vykonávané analytikom v súvislosti s výberom materiálu sa vzťahuje dohľad *ex post* Komisára pre vyšetrovacie právomoci, ktorý hodnotí súlad s konkrétnymi zárukami, ktoré sa pre fázu preskúmania stanovujú v zákone o vyšetrovacích právomociach z roku 2016 ([392]) (pozri aj odôvodnenie 229). Komisár pre vyšetrovacie právomoci musí (a to aj prostredníctvom auditu, kontroly a vyšetrovania) kontrolovať, ako orgány verejnej moci vykonávajú vyšetrovacie právomoci, ktoré sú uvedené v zákone o vyšetrovacích právomociach z roku 2016 ([393]). V tejto súvislosti sa v Kódexe postupov pre zachytávanie komunikácie a Kódexe postupov pre zasahovanie do zariadení objasňuje, že služba musí uchovávať záznamy na účely následného preskúmania a auditu, pričom sa v záznamoch musia opísať dôvody, prečo bol prístup poverených osôb k materiálu nevyhnutný a primeraný, ako aj príslušné operačné účely ([394]). Úrad Komisára pre vyšetrovacie právomoci ([395]) vo svojej výročnej správe za rok 2018 napríklad dospel k záveru, že odôvodnenia na preskúmanie určitého hromadne získaného materiálu zaznamenané analytikmi spĺňali požadovanú normu proporcionality, a to poskytnutím dostatočných podrobností o dôvodoch ich „vyhľadávaní“ vo vzťahu k účelu, ktorý sa mal dosiahnuť ([396]). Úrad Komisára pre vyšetrovacie právomoci vo svojej správe za rok 2019 v súvislosti s hromadnými právomocami jasne vyjadril svoj zámer pokračovať v kontrolách hromadného zachytávania vrátane podrobného preskúmania selektorov a kritérií vyhľadávania ([397]). Bude pokračovať aj v dôkladnom preskúmaní jednotlivých prípadov výberu opatrení sledovania (cielených/hromadných) tak pri skúmaní žiadostí o príkaz na základe dvojitého zabezpečenia, ako aj pri kontrolách ([398]). Toto ďalšie monitorovanie Komisia riadne zohľadní v rámci monitorovania tohto rozhodnutia uvedeného v odôvodneniach 281 – 284.

3.3.1.1.4.2. Hromadné získavanie údajov o komunikácii

(231) Ustanovenia časti 6 kapitoly 2 zákona o vyšetrovacích právomociach z roku 2016 upravujú príkazy na hromadné získavanie, ktorými sa adresátom udeľuje povolenie od telekomunikačných operátorov vyžadovať, aby poskytli alebo získali všetky údaje o komunikácií v ich vlastníctve. Tieto príkazy zároveň oprávňujú žiadajúci orgán na výber údajov pre ďalšiu fázu preskúmania. Rovnako ako v prípade cieleného uchovávania a získavania údajov o komunikácii (pozri odôvodnenie 199) ani hromadné získavanie údajov o komunikácii sa zvyčajne nevzťahuje na osobné údaje dotknutých osôb v EÚ prenesených na základe tohto rozhodnutia do Spojeného kráľovstva. Povinnosť poskytnúť údaje o komunikácii podľa časti 6 kapitoly 2 zákona o vyšetrovacích právomociach z roku 2016 sa vzťahuje na údaje, ktoré získavajú telekomunikační operátori v Spojenom kráľovstve priamo od používateľov telekomunikačných služieb ([399]). Takýto druh spracúvania „orientovaný na zákazníka“ nezahŕňa prenos na základe tohto rozhodnutia, t. j. prenos od prevádzkovateľa/sprostredkovateľa v EÚ k prevádzkovateľovi/sprostredkovateľovi v Spojenom kráľovstve.

(232) V záujme úplnosti sú ďalej opísané podmienky a záruky, ktoré upravujú získavanie hromadných údajov o komunikácii.

([392]) § 152 a § 193 zákona o vyšetrovacích právomociach z roku 2016.

([393]) § 229 zákona o vyšetrovacích právomociach z roku 2016.

([394]) Kódex postupov pre zachytávanie komunikácie, bod 6.74, pozri poznámku pod čiarou č. 278 a Kódex postupov pre zasahovanie do zariadení, bod 6.78, pozri poznámku pod čiarou č. 348.

([395]) Úrad Komisára pre vyšetrovacie právomoci je zriadený na základe § 238 zákona o vyšetrovacích právomociach z roku 2016 s cieľom poskytovať personál, ubytovanie, vybavenie a ďalšie zariadenia a služby potrebné na výkon ich funkcií (pozri odôvodnenie 251).

([396]) Vo výročnej správe Úradu Komisára pre vyšetrovacie právomoci za rok 2018 sa uvádza, že odôvodnenia na preskúmanie určitého hromadne získaného materiálu zaznamenané analytikmi Vládneho komunikačného ústredia „spĺňali požadovanú normu a analytici pri svojich vyhľadávaniach v hromadných údajoch v dostatočnej miere zohľadňovali proporcionalitu“. Výročná správa Komisára pre vyšetrovacie právomoci za rok 2018, bod 6.22, pozri poznámku pod čiarou č. 464.

([397]) Výročná správa Komisára pre vyšetrovacie právomoci za rok 2019, bod 7.6, pozri poznámku pod čiarou č. 463.

([398]) Výročná správa Komisára pre vyšetrovacie právomoci za rok 2019, bod 10.22, pozri poznámku pod čiarou č. 463.

([399]) Vyplýva to z vymedzenia údajov o komunikácii stanoveného v § 261 ods. 5 zákona o vyšetrovacích právomociach z roku 2016, podľa ktorého údaje o komunikácii sú údaje získané telekomunikačným operátorom, ktoré sú buď o používateľovi telekomunikačných služieb a týkajú sa poskytovania týchto služieb, alebo sú obsiahnuté v rámci komunikácie ako jej súčasť, sú k nej pripojené alebo logicky s ňou súvisia (pozri aj Kódex postupov pre hromadné získavanie údajov o komunikácii, ktorý je k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf body 2.15 až 2.22). Okrem toho sa podľa vymedzenia pojmu telekomunikačný operátor, ktoré je stanovené v § 261 ods. 10 zákona o vyšetrovacích právomociach z roku 2016, vyžaduje, aby bol telekomunikačný operátor osoba, ktorá ponúka alebo poskytuje telekomunikačné služby osobám v Spojenom kráľovstve alebo ktorá poskytuje telekomunikačný systém, ktorý sa (úplne alebo čiastočne) nachádza v Spojenom kráľovstve, alebo ho prevádzkuje. Z uvedených vymedzení jasne vyplýva, že povinnosti podľa zákona o vyšetrovacích právomociach z roku 2016 sa nemôžu uložiť telekomunikačným operátorom, ktorých zariadenia sa nenachádzajú v Spojenom kráľovstve alebo nie sú prevádzkované zo Spojeného kráľovstva a neponúkajú alebo neposkytujú služby osobám v Spojenom kráľovstve (pozri aj Kódex postupov pre hromadné získavanie údajov o komunikácii, bod 2.2). Ak predplatitelia z EÚ (či už sa nachádzajú v EÚ, alebo Spojenom kráľovstve) využili služby v Spojenom kráľovstve, akúkoľvek komunikáciu v súvislosti s poskytovaním týchto služieb by priamo získal poskytovateľ služieb v Spojenom kráľovstve namiesto toho, aby podliehala prenosu z EÚ.

(233) Zákonom o vyšetrovacích právomociach z roku 2016 sa nahrádzajú právne predpisy vzťahujúce sa na získavanie hromadných údajov o komunikácii, ktoré podliehali rozsudku Súdneho dvora Európskej únie vo veci Privacy International. Právne predpisy, ktoré boli predmetom v danej veci, boli zrušené a nový systém poskytuje konkrétne podmienky a záruky, podľa ktorých môže byť takého opatrenie povolené.

(234) Na rozdiel od predchádzajúceho systému, v rámci ktorého minister mal úplnú diskrečnú právomoc pri povoľovaní opatrenia ([400]), sa na základe ustanovení zákona o vyšetrovacích právomociach z roku 2016 vyžaduje, aby minister vydal príkaz, len ak je opatrenie nevyhnutné a primerané. V praxi to znamená, že by malo existovať prepojenie medzi prístupom k údajom a sledovaným cieľom ([401]). Konkrétnejšie, minister bude povinný posúdiť prítomnosť prepojenia medzi požadovaným opatrením a jedným alebo viacerými „operačnými účelmi" stanovenými v príkaze (pozri odôvodnenie 219). S ohľadom na posúdenie proporcionality sa v príslušnom kódexe postupov stanovuje, že „minister musí zohľadniť, či to, čo sa má dosiahnuť prostredníctvom príkazu, by sa mohlo primerane dosiahnuť inými menej rušivými prostriedkami [§ 2 ods. 2 písm. a) zákona], napríklad získavaním požadovaných informácií prostredníctvom menej rušivých právomocí, ako je cielené získavanie údajov o komunikácii" ([402]).

(235) Pri vykonávaní takého posúdenia sa minister bude spoliehať na informácie, ktoré sú vedúci spravodajských služieb ([403]) povinní predložiť vo svojej žiadosti, ako sú dôvody, prečo sa opatrenie považuje za nevyhnutné podľa zákonom stanovených odôvodnení a dôvody, prečo by to, čo sa má dosiahnuť prostredníctvom príkazu, nebolo možné primerane dosiahnuť inými menej rušivými prostriedkami ([404]). Operačné účely navyše obmedzujú rozsah, na ktorý sa môžu údaje získané prostredníctvom príkazu vybrať na preskúmanie ([405]). Ako sa uvádza v príslušnom kódexe postupov, operačné účely musia opisovať jasnú požiadavku a obsahovať dostatočné podrobnosti, ktorými sa minister uisťuje o tom, že sa získavané údaje môžu vybrať na preskúmanie len z konkrétnych dôvodov ([406]). Minister bude musieť pred povolením príkazu skutočne zabezpečiť zavedenie opatrení na zabezpečenie toho, aby sa na preskúmanie, ktoré by malo byť za každých okolností primerané a nevyhnutné, vybral iba materiál, ktorého preskúmanie sa považuje za nevyhnutné na operačné a zákonné účely. Táto konkrétna požiadavka, ktorá sa uvádza v § 158 a 172 ([407]) zákona o vyšetrovacích právomociach z roku 2016 a ktorá sa vzťahuje na predchádzajúce posúdenie nevyhnutnosti a proporcionality kritérií použitých na účely výberu, predstavuje v porovnaní s predchádzajúcim systémom ďalší významný nový prvok systému zavedeného na základe ustanovení zákona o vyšetrovacích právomociach z roku 2016.

(236) Zákonom o vyšetrovacích právomociach z roku 2016 sa zároveň zaviedla povinnosť ministra pred vydaním príkazu na hromadné získavanie údajov o komunikácii zabezpečiť zavedenie konkrétnych obmedzení v súvislosti s bezpečnosťou, uchovávaním a poskytovaním získaných osobných údajov ([408]). V prípade poskytovania údajov do zahraničia sa záruky opísané v odôvodnení 227 pre činnosti hromadného zachytávania a hromadného zasahovania do zariadení uplatňujú aj v tejto súvislosti ([409]). V právnych predpisoch sú stanovené ďalšie obmedzenia týkajúce sa trvania ([410]), obnovy ([411]) a zmeny hromadných príkazov ([412]).

(237) Čo je dôležité, podobne ako v prípade iných hromadných právomocí, minister musí pred vydaním príkazu získať súhlas od Komisára pre justíciu ([413]). Ide o kľúčový prvok systému, ktorý sa zaviedol podľa zákona o vyšetrovacích právomociach z roku 2016.

([400]) V § 94 ods. 1 zákona o telekomunikáciách z roku 1984 (Telecommunication Act) sa stanovilo, že minister mohol vydávať „rozhodnutia všeobecnej povahy tak, ako sa ministrovi javili nevyhnutné alebo účelné pre záujmy národnej bezpečnosti (…)" (pozri poznámku pod čiarou č. 451).

([401]) Pozri vec Privacy International, bod 78.

([402]) Pozri Kódex postupov pre hromadné získavanie údajov o komunikácii, bod 4.11 (pozri poznámku pod čiarou č. 399414).

([403]) O príkaz na hromadné získavanie môžu požiadať len vedúci spravodajských služieb, ktorými sú: i) generálny riaditeľ Bezpečnostnej služby, ii) šéf Tajnej spravodajskej služby alebo iii) riaditeľ Vládneho komunikačného ústredia (pozri § 158 a 263 zákona o vyšetrovacích právomociach z roku 2016).

([404]) Kódex postupov pre hromadné získavanie údajov o komunikácií, bod 4.5 (pozri poznámku pod čiarou č. 399).

([405]) Podľa ustanovení § 161 zákona o vyšetrovacích právomociach z roku 2016 operačné účely uvedené v príkaze musia byť uvedené v zozname udržiavanom vedúcimi spravodajských služieb (ďalej len „zoznam operačných účelov") ako účely, ktoré považujú za operačné účely, na ktoré sa môžu vybrať na preskúmanie údaje o komunikácii získané prostredníctvom príkazu na hromadné získavanie.

([406]) Kódex postupov pre hromadné získavanie údajov o komunikácii, bod 6.6 (pozri poznámku pod čiarou č. 399).

([407]) V § 172 zákona o vyšetrovacích právomociach z roku 2016 sa vyžaduje, aby boli zavedené konkrétne záruky týkajúce sa fázy filtrovania hromadne získanej komunikácie a jej výberu na preskúmanie. Navyše úmyselné preskúmanie v rozpore s týmito zárukami je trestným činom (pozri § 173 zákona o vyšetrovacích právomociach z roku 2016).

([408]) § 171 zákona o vyšetrovacích právomociach z roku 2016.

([409]) § 171 ods. 9 zákona o vyšetrovacích právomociach z roku 2016.

([410]) § 162 zákona o vyšetrovacích právomociach z roku 2016.

([411]) § 163 zákona o vyšetrovacích právomociach z roku 2016.

([412]) § 164 – § 166 zákona o vyšetrovacích právomociach z roku 2016.

([413]) § 159 zákona o vyšetrovacích právomociach z roku 2016.

(238) Komisár pre vyšetrovacie právomoci vykonáva dohľad *ex post* nad postupom preskúmania hromadne získaného materiálu (údajov o komunikácii), pozri odôvodnenie 254. V tejto súvislosti sa zákonom o vyšetrovacích právomociach z roku 2016 zaviedla požiadavka, podľa ktorej musí spravodajský analytik vykonávajúci preskúmanie pred výberom údajov na preskúmanie zaznamenať dôvod o tom, prečo je navrhované preskúmanie nevyhnutné a primerané na určený operačný účel ([414]). Vo výročnej správe Úradu Komisára pre vyšetrovacie právomoci za rok 2019 sa v súvislosti s praktikami Vládneho komunikačného ústredia a Bezpečnostnej služby (MI5) uvádza zistenie, že „kľúčová úloha hromadných údajov o komunikácii pre rozsah činností vykonávaných Vládnym komunikačným ústredím bola vo vyšetrovaných prípadoch jasne formulovaná. Posúdili sme povahu požadovaných údajov a uvedených spravodajských požiadaviek, pričom sme boli spokojní s tým, že z dokumentácie vyplýva, že ich prístup bol nevyhnutný a primeraný“ ([415]). Zaznamenané odôvodnenia Bezpečnostnej služby (MI5) vykazovali dobrú úroveň a spĺňali zásady nevyhnutnosti a proporcionality. ([416])

3.3.1.1.4.3. Uchovávanie a preskúmanie súborov hromadných osobných údajov

(239) Príkazom týkajúcim sa súboru hromadných osobných údajov (bulk personal dataset) sa ([417]) spravodajským službám povoľuje uchovávať a preskúmať súbory údajov, ktoré obsahujú osobné údaje o viacerých jednotlivcoch. Podľa vysvetlení poskytnutých orgánmi Spojeného kráľovstva môže analýza takýchto súborov údajov predstavovať „jediný nástroj, ktorý môžu spravodajské služby Spojeného kráľovstva využiť na dosiahnutie pokroku pri vyšetrovaní a na identifikáciu teroristov na základe veľmi obmedzených spravodajských informácií, prípadne ak úmyselne skrývajú svoje komunikácie ([418])." Existujú dva druhy príkazov: „príkazy týkajúce sa skupinového súboru hromadných osobných údajov“ ([419]), ktoré sa vzťahujú na konkrétnu kategóriu súborov údajov, t. j. súbory údajov, ktoré sú si podobné obsahom a navrhovaným použitím a vzbudzujú podobné úvahy, čo sa týka napríklad miery narušenia a citlivosti, ako aj proporcionality použitia údajov, umožňujúc tak ministrovi naraz zvážiť nevyhnutnosť a proporcionalitu získavania všetkých údajov v rámci príslušnej skupiny. Príkaz týkajúci sa skupinového súboru hromadných osobných údajov sa môže napríklad vzťahovať na súbory údajov o cestách, ktoré súvisia s podobnými trasami ([420]). „Príkazy týkajúce sa konkrétneho súboru hromadných osobných údajov“ ([421]) sa oproti tomu vzťahujú na jeden konkrétny súbor údajov, napríklad na súbor údajov nového alebo nezvyčajného druhu informácií, ktoré nepatria do rozsahu existujúceho príkazu týkajúceho sa skupinového súboru hromadných osobných údajov, alebo súbor údajov, ktorý obsahuje konkrétne druhy osobných údajov ([422]), a preto si vyžaduje dodatočné záruky ([423]). Na základe ustanovení zákona o vyšetrovacích právomociach z roku 2016, pokiaľ ide o súbory hromadných osobných údajov, umožňuje sa preskúmavanie a uchovávanie takýchto súborov údajov iba vtedy, ak je to nevyhnutné a primerané ([424]), a to v súlade s všeobecnými povinnosťami týkajúcimi sa ochrany súkromia ([425]).

(240) Právomoc vydávať príkazy týkajúce sa súborov hromadných osobných údajov podlieha postupu „dvojitého zabezpečenia“: posúdenie nevyhnutnosti a proporcionality opatrenia najskôr vykoná minister a následne Komisár pre justíciu ([426]). Minister je povinný posúdiť povahu a rozsah pôsobnosti druhu požadovaného príkazu, kategóriu dotknutých údajov a počet samostatných súborov hromadných osobných údajov, na ktoré sa bude pravdepodobne vzťahovať konkrétny druh príkazu ([427]). Podľa Kódexu postupov pre uchovávanie a používanie súborov hromadných osobných údajov spravodajskými službami sa majú viesť podrobné záznamy, ktoré podliehajú auditu Komisára pre vyšetrovacie právomoci ([428]). Uchovávanie a preskúmavanie súborov hromadných osobných údajov, ktoré prekračujú hranice stanovené v zákone o vyšetrovacích právomociach z roku 2016, sú trestným činom ([429]).

([414]) Výročná správa Úradu Komisára pre vyšetrovacie právomoci za rok 2019, bod 8.6, pozri poznámku pod čiarou č. 463.
([415]) Výročná správa Úradu Komisára pre vyšetrovacie právomoci za rok 2019, bod 10.4, pozri poznámku pod čiarou č. 463.
([416]) Výročná správa Úradu Komisára pre vyšetrovacie právomoci za rok 2019, bod 8.37, pozri poznámku pod čiarou č. 463.
([417]) § 200 zákona o vyšetrovacích právomociach z roku 2016.
([418]) Vysvetľujúci rámec Spojeného kráľovstva pre diskusiu o primeranosti, oddiel H s názvom „Národná bezpečnosť“, strana 34, pozri poznámku pod čiarou č. 29.
([419]) § 204 zákona o vyšetrovacích právomociach z roku 2016.
([420]) Kódex postupov pre uchovávanie a používanie súborov hromadných osobných údajov spravodajskými službami, bod 4.7, k dispozícii na tejto adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf.
([421]) § 205 zákona o vyšetrovacích právomociach z roku 2016.
([422]) Napríklad citlivé osobné údaje, pozri § 202 zákona o vyšetrovacích právomociach z roku 2016 a Kódex postupov pre uchovávanie a používanie hromadných osobných údajov spravodajskými službami, body 4.21 a 4.12, pozri poznámku pod čiarou č. 469.
([423]) Uplatňovanie príkazu týkajúceho sa konkrétneho súboru hromadných osobných údajov musí jednotlivo posúdiť minister, t. j. so zreteľom na jeden konkrétny súbor údajov. Spravodajské služby sú povinné podľa ustanovení v § 205 do svojej žiadosti o príkaz týkajúci sa konkrétnych súborov hromadných osobných údajov zahrnúť podrobné vysvetlenie povahy a rozsahu daného materiálu a zoznam „operačných účelov“, na ktoré chce príslušná spravodajská služba preskúmať súbor hromadných osobných údajov (v prípade, že spravodajské služby žiadajú o príkaz na uchovávanie a preskúmanie, nie výlučne na uchovávanie). Pri vydávaní príkazu týkajúceho sa skupinového súboru hromadných osobných údajov minister namiesto toho naraz posúdi celú kategóriu súborov údajov.
([424]) § 204 a § 205 zákona o vyšetrovacích právomociach z roku 2016.
([425]) § 2 zákona o vyšetrovacích právomociach z roku 2016.
([426]) § 204 a § 205 zákona o vyšetrovacích právomociach z roku 2016.
([427]) Kódex postupov pre uchovávanie a používanie súborov hromadných osobných údajov spravodajskými službami, bod 5.2, pozri poznámku pod čiarou č. 420.
([428]) Kódex postupov pre uchovávanie a používanie súborov hromadných osobných údajov spravodajskými službami, body 8.1 až 8.15, pozri poznámku pod čiarou č. 420.
([429]) Vysvetľujúci rámec Spojeného kráľovstva pre diskusiu o primeranosti, oddiel H s názvom „Národná bezpečnosť“, strana 34, pozri poznámku pod čiarou č. 29.

3.3.2. *Ďalšie používanie získaných informácií*

(241) Spracúvané osobné údaje sa podľa ustanovení v časti 4 zákona o ochrane údajov z roku 2018 nesmú spracúvať spôsobom, ktorý je nezlučiteľný s účelom, na ktorý boli získané ([430]). V zákone o ochrane údajov z roku 2018 sa stanovuje, že prevádzkovateľ môže spracúvať údaje na účel odlišný od toho, na ktorý boli údaje získané, v prípade, že je tento účel v súlade s pôvodným účelom, a za predpokladu, že prevádzkovateľ je na toto spracúvanie oprávnený zákonom a že spracúvanie je nevyhnutné a primerané ([431]). Okrem toho sa v zákone o bezpečnostných službách z roku 1989 a v zákone o spravodajských službách z roku 1994 stanovuje, že vedúci spravodajských služieb majú povinnosť zabezpečiť, že nie sú získané alebo poskytnuté žiadne informácie s výnimkou prípadov, keď to je nevyhnutné na riadne plnenie funkcii služieb alebo na ďalšie obmedzené a konkrétne účely uvedené v príslušných ustanoveniach ([432]).

(242) Okrem toho sa v § 109 zákona o ochrane údajov z roku 2018 stanovujú osobitné požiadavky na medzinárodné prenosy osobných údajov spravodajskými službami do tretích krajín alebo medzinárodným organizáciám. Podľa týchto ustanovení nie je povolený prenos osobných údajov do krajiny alebo na územie mimo Spojeného kráľovstva alebo medzinárodnej organizácii, pokiaľ prenos nie je nevyhnutný a primeraný na účely plnenia zákonných funkcií prevádzkovateľa alebo na ďalšie účely stanovené v § 2 ods. 2 písm. a) zákona o bezpečnostných službách z roku 1989 alebo § 2 ods. 2 písm. a) a § 4 ods. 2 písm. a) zákona o spravodajských službách z roku 1994 ([433]). Je dôležité, že tieto požiadavky sa uplatňujú vzťahujú aj na prípady, keď sa podľa § 110 zákona o ochrane údajov z roku 2018 uplatní výnimka týkajúca sa národnej bezpečnosti, keďže v § 110 zákona o ochrane údajov z roku 2018 sa § 109 zákona o ochrane údajov z roku 2018 neuvádza ako jedno z ustanovení, ktoré sa môže prestať uplatňovať, ak sa na účely ochrany národnej bezpečnosti vyžaduje výnimka z istých ustanovení.

(243) Navyše, ako to Komisár pre informácie zdôraznil vo svojom usmernení o spracúvaní údajov spravodajskými službami, okrem záruk uvedených v časti 4 zákona o ochrane údajov z roku 2018, sa na spravodajskú službu pri poskytovaní údajov spravodajskej službe tretej krajiny vzťahujú aj záruky stanovené v iných legislatívnych opatreniach, ktoré sa na ne uplatňujú s cieľom zabezpečiť, že získanie a poskytovanie osobných údajov a zaobchádzanie s nimi sa uskutočňuje zákonným a zodpovedným spôsobom ([434]). V zákone o vyšetrovacích právomociach z roku 2016 sa napr. stanovujú ďalšie záruky v súvislosti s presunmi materiálu do tretích krajín, ktorý bol získaný prostredníctvom cieleného zachytávania ([435]), cieleného zasahovania do zariadení ([436]), hromadného zachytávania ([437]), hromadného získavania údajov o komunikácii ([438]) a hromadného zasahovania do zariadení ([439]) (tzv. poskytovanie údajov do zahraničia). Konkrétne musí orgán vydávajúci príkaz zabezpečiť, že sú v platnosti opatrenia, ktorými sa tretie krajiny prijímajúce údaje zaväzujú k tomu, že obmedzia počet osôb, ktoré majú prístup k materiálu, rozsah poskytovania informácií a počet kópií materiálu na nevyhnutné minimum, a to na povolené účely stanovené v zákone o vyšetrovacích právomociach z roku 2016 ([440]).

3.3.3. *Dohľad*

(244) Dohľad nad prístupom vlády v záujme národnej bezpečnosti vykonáva viacero rozličných orgánov. Komisár pre informácie vykonáva dohľad nad spracúvaním osobných údajov so zreteľom na zákon o ochrane údajov z roku 2018 (pre ďalšie informácie o nezávislosti, vymenovaní a právomociach Komisára pozri odôvodnenia 85 až 98), zatiaľ čo nezávislý a súdny dohľad nad použitím vyšetrovacích právomocí podľa zákona o vyšetrovacích

([430]) § 87 ods. 1 zákona o ochrane údajov z roku 2018.

([431]) § 87 ods. 3 zákona o ochrane údajov z roku 2018. Napriek tomu, že prevádzkovatelia môžu byť oslobodení z pôsobnosti tejto zásady na základe § 110 zákona o ochrane údajov z roku 2018 v takom rozsahu, ako sa vyžaduje v záujme ochrany národnej bezpečnosti, musia sa takéto oslobodenia jednotlivo posúdiť a môžu sa uplatniť len vtedy, ak by uplatňovanie konkrétneho ustanovenia malo negatívne dôsledky na národnú bezpečnosť (pozri odôvodnenie 132). Osvedčenia o záujme národnej bezpečnosti pre spravodajské služby Spojeného kráľovstva (k dispozícii na tomto odkaze: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) sa nevzťahujú na § 87 ods. 3 zákona o ochrane údajov z roku 2018. Keďže každé spracúvanie osobných údajov na iný účel musí byť povolené v súlade so zákonom, spravodajské služby musia mať aj jasný právny základ na ďalšie spracúvanie.

([432]) Viac informácií o týchto účeloch sa nachádza v poznámke pod čiarou č. 312.

([433]) Pozri poznámku pod čiarou č. 312.

([434]) Usmernenie Komisára pre informácie o spracúvaní údajov spravodajskými službami (pozri poznámku pod čiarou č. 161).

([435]) § 54 zákona o vyšetrovacích právomociach z roku 2016.

([436]) § 130 zákona o vyšetrovacích právomociach z roku 2016.

([437]) § 151 zákona o vyšetrovacích právomociach z roku 2016.

([438]) § 171 ods. 9 zákona o vyšetrovacích právomociach z roku 2016.

([439]) § 192 zákona o vyšetrovacích právomociach z roku 2016.

([440]) Súčasťou opatrení musia byť opatrenia, ktorými sa zaisťuje bezpečné uchovávanie všetkých vytvorených kópií materiálu počas celého obdobia uchovávania. Materiál získaný na základe príkazu a každá vytvorená kópia takého materiálu musí byť zničená v okamihu, keď už neexistujú relevantné dôvody na ich uchovávanie (pozri § 150 ods. 2, § 150 ods. 5 a §151 ods. 2 zákona o vyšetrovacích právomociach z roku 2016). Je potrebné poznamenať, že v prípade podobných záruk stanovených v predchádzajúcom právnom rámci (zákon o regulácii vyšetrovacích právomocí z roku 2000), sa konštatoval súlad s požiadavkami stanovenými Európskym súdom pre ľudské práva týkajúcimi sa poskytovania materiálu získaného hromadným zachytávaním zahraničným štátom alebo medzinárodným organizáciám [Európsky súd pre ľudské práva (veľká komora), vec Big Brother Watch and others/United Kingdom, (pozri poznámku pod čiarou č. 279), body 362 a 399].

právomociach z roku 2016 vykonáva Komisár pre vyšetrovacie právomoci. Komisár pre vyšetrovacie právomoci vykonáva dohľad nad použitím vyšetrovacích právomocí podľa zákona o vyšetrovacích právomociach z roku 2016 v prípade orgánov presadzovania práva aj národných bezpečnostných orgánov. Politický dohľad poskytuje parlamentný výbor pre spravodajské služby.

3.3.3.1. Dohľad na základe ustanovení časti 4 zákona o ochrane údajov

(245) Na spracúvanie osobných údajov spravodajskými službami podľa časti 4 zákona o ochrane údajov z roku 2018 dozerá Komisár pre informácie ([441]).

(246) Všeobecné funkcie Komisára pre informácie v súvislosti so spracúvaním osobných údajov zo strany spravodajských služieb, ktoré patrí do rozsahu pôsobnosti časti 4 zákona o ochrane údajov z roku 2018, sú stanovené v prílohe 13 k zákonu o ochrane údajov z roku 2018. Medzi úlohy okrem iných patrí monitorovanie a presadzovanie ustanovení časti 4 zákona o ochrane údajov z roku 2018, podpora informovanosti verejnosti, poskytovanie poradenstva parlamentu, vláde a ďalším inštitúciám v oblasti legislatívnych a administratívnych opatrení, podpora informovanosti prevádzkovateľov a sprostredkovateľov o ich povinnostiach, poskytovanie informácií dotknutým osobám, ktoré sa týkajú uplatňovania ich práv, vedenie vyšetrovaní atď.

(247) Komisár má, podobne ako v časti 3 zákona o ochrane údajov z roku 2018, právomoc informovať prevádzkovateľov o údajnom porušení a vydávať varovania o tom, že spracúvaním môže porušovať pravidlá, ako aj vydávať napomenutia v prípade, že sa porušenie potvrdí. Môže vydávať aj presadzovacie oznámenia a oznámenia o uložení sankcie za porušenie určitých ustanovení tohto zákona ([442]). Na rozdiel od ostatných častí zákona o ochrane údajov z roku 2018 však Komisár nemôže národnému bezpečnostnému orgánu predložiť oznámenie o posúdení ([443]).

(248) Okrem toho sa v § 110 ods. 6 zákona o ochrane údajov z roku 2018 stanovuje výnimka z využívania určitých právomocí Komisára, ak je to potrebné na účely ochrany národnej bezpečnosti. Patrí sem právomoc Komisára vydávať (akýkoľvek druh) oznámení podľa zákona o ochrane údajov (informačné oznámenie, oznámenie o posúdení, presadzovacie oznámenie a oznámenie o uložení sankcie), právomoc vykonávať inšpekcie v súlade s medzinárodnými záväzkami, právomoci na vstup a inšpekciu a pravidlá týkajúce sa trestných činov ([444]). Ako sa vysvetľuje v odôvodnení 126, tieto výnimky sa budú uplatňovať len vtedy, ak sú potrebné a primerané, a od prípadu k prípadu.

(249) Komisár pre informácie a spravodajské služby Spojeného kráľovstva podpísali memorandum o porozumení ([445]), ktorým sa stanovuje rámec pre spoluprácu vo viacerých otázkach vrátane oznámení o porušení ochrany údajov a vybavovania sťažností dotknutých osôb. Konkrétne sa v ňom stanovuje, že po prijatí sťažnosti Komisár pre informácie posúdi, či sa primerane uplatnila akákoľvek výnimka v záujme národnej bezpečnosti. V súvislosti s preskúmaním jednotlivých sťažností sa musí dotknutej spravodajskej službe poskytnúť lehota 20 pracovných dní na poskytnutie odpovedí na otázky predložené Komisárom pre informácie, pričom sa použijú vhodné zabezpečené kanály, ak sa otázky týkajú utajovaných skutočností. Od apríla 2018 ku dnešnému dňu dostal Komisár pre informácie od jednotlivcov 21 sťažností na spravodajské služby. Každá sťažnosť bola posúdená a výsledok bol oznámený dotknutej osobe ([446]).

([441]) § 116 zákona o ochrane údajov z roku 2018.

([442]) Podľa prílohy 13 bodu 2 k zákonu o ochrane údajov z roku 2018 možno prevádzkovateľovi alebo sprostredkovateľovi vydať presadzovacie oznámenie a oznámenie o uložení sankcie v súvislosti s porušením časti 4 kapitoly 2 zákona o ochrane údajov z roku 2018 (zásady spracúvania), ustanovenia časti 4 zákona o ochrane údajov z roku 2018, ktorým sa dotknutej osobe udeľujú práva, požiadavky oznámiť porušenie ochrany osobných údajov Komisárovi podľa § 108 zákona o ochrane údajov z roku 2018, ako aj v súvislosti s porušením zásad prenosu osobných údajov do tretích krajín, krajín, ktoré nie sú zmluvnými stranami dohovoru, a medzinárodným organizáciám podľa § 109 zákona o ochrane údajov z roku 2018 (pre podrobné informácie o presadzovacom oznámení a oznámení o uložení sankcie pozri odôvodnenie 92).

([443]) Podľa § 147 ods. 6 zákona o ochrane údajov z roku 2018 Komisár pre informácie nemôže vydať oznámenie o posúdení orgánu uvedenému v § 23 ods. 3 zákona o slobodnom prístupe k informáciám z roku 2000. Patria sem Bezpečnostná služba (MI5), tajná spravodajská služba (MI6) a vládne komunikačné ústredie (Government Communications Headquarter).

([444]) Výnimka sa môže vzťahovať na tieto ustanovenia: § 108 (oznámenie porušenia ochrany osobných údajov Komisárovi), § 119 (inšpekcia v súlade s medzinárodnými záväzkami), § 142 až § 154 a príloha 15 (oznámenia Komisára a právomoci na vstup a inšpekciu) a § 170 až § 173 (trestné činy týkajúce sa osobných údajov). V súvislosti so spracovaním zo strany spravodajských služieb sa môže vzťahovať aj na prílohu 13 (Ďalšie všeobecné funkcie Komisára), odsek 1 písm. a) a g) a odsek 2.

([445]) Memorandum o porozumení medzi Komisárom pre informácie a spravodajskými službami Spojeného kráľovstva, pozri poznámku pod čiarou č. 165.

([446]) V siedmich z týchto prípadov Komisár pre informácie sťažovateľovi odporučil, aby podal podnet prevádzkovateľovi údajov (bolo tomu tak v prípade, že fyzická osoba podala podnet Komisárovi, hoci ho mal najprv podať prevádzkovateľovi), v jednom z týchto prípadov Komisár poskytol prevádzkovateľovi všeobecné poradenstvo (deje sa tak vtedy, keď prevádzkovateľ svojim konaním právne predpisy zrejme neporušil, ale zlepšenie postupov mohlo zabrániť tomu, aby bola Komisárovi podaná sťažnosť) a v zostávajúcich 13 prípadoch nebolo potrebné podniknúť žiadne kroky zo strany prevádzkovateľa (deje sa tak vtedy, ak podnet predložený jednotlivcom nespadá pod zákon o ochrane údajov z roku 2018, pretože sa týka spracúvania osobných údajov, ale na základe poskytnutých informácií sa zdá, že prevádzkovateľ neporušil právne predpisy).

3.3.3.2. Dohľad nad použitím vyšetrovacích právomocí podľa zákona o vyšetrovacích právomociach z roku 2016

(250) Na základe ustanovení časti 8 zákona o vyšetrovacích právomociach z roku 2016 vykonáva dohľad nad použitím vyšetrovacích právomocí Komisár pre vyšetrovacie právomoci. Komisárovi pomáhajú ďalší Komisári pre justíciu, ktorí sa spoločne uvádzajú ako Komisári pre justíciu ([447]). V zákone o vyšetrovacích právomociach z roku 2016 sa stanovujú záruky, ktoré chránia nezávislosť Komisárov pre justíciu. Komisári pre justíciu musia zastávať alebo v minulosti museli zastávať vysokú súdnu funkciu (t. j. musia byť alebo museli byť členmi vyšších súdov) ([448]) a podobne ako každý člen justície majú nezávislé postavenie od vlády ([449]). Podľa § 227 zákona o vyšetrovacích právomociach z roku 2016 predseda vlády vymenúva Komisára pre vyšetrovacie právomoci a Komisárov pre justíciu tak, ako považuje za potrebné. Všetci Komisári, či už sú súčasní alebo bývalí členovia justície, môžu byť vymenovaní len na základe spoločného odporúčania troch šéfov justície pre Anglicko a Wales, Škótsko a Severné Írsko a lorda kancelára ([450]). Minister musí pre Komisára pre vyšetrovacie právomoci zabezpečiť personál, ubytovanie, výbavu a ďalšie zariadenia a služby ([451]). Funkčné obdobie Komisárov, ktorí môžu byť opätovne vymenovaní, trvá tri roky ([452]). Ďalšou zárukou ich nezávislosti je to, že Komisári pre justíciu môžu byť odvolaní z funkcie len na základe prísnych podmienok, ktoré ukladajú vysokú prahovú hodnotu: za osobitných podmienok, ktoré sú podrobne uvedené v § 228 ods. 5 zákona o vyšetrovacích právomociach z roku 2016 (napríklad vyhlásenie konkurzu alebo uväznenie), ich môže odvolať predseda vlády alebo parlament uznesením o ich odvolaní schválenom v každej zo snemovní parlamentu ([453]).

(251) Komisára pre vyšetrovacie právomoci a Komisárov pre justíciu podporuje v ich funkciách Úrad Komisára pre vyšetrovacie právomoci. Medzi zamestnancov Úradu Komisára pre vyšetrovacie právomoci patrí tím inšpektorov, interní právni a technickí odborníci a panel poradcov pre technológie s cieľom poskytovať odborné poradenstvo. Pre každého individuálneho Komisára pre justíciu platí, že nezávislosť Úradu Komisára pre vyšetrovacie právomoci je chránená. Úrad Komisára pre vyšetrovacie právomoci je nezávislý orgán ministerstva vnútra, čo znamená, že je financovaný ministerstvom vnútra, ale svoje funkcie vykonáva nezávisle ([454]).

(252) Hlavné funkcie Komisárov pre justíciu sú stanovené v § 229 zákona o vyšetrovacích právomociach z roku 2016 ([455]). Komisári pre justíciu majú najmä rozsiahle právomoci, pokiaľ ide o schvaľovanie vopred, čo je súčasťou záruk zavedených v právnom rámci Spojeného kráľovstva obsahujúcom zákon o vyšetrovacích právomociach z roku 2016. Všetky príkazy v súvislosti s cieleným zachytávaním, so zasahovaním do zariadení, súbormi hromadných osobných údajov, s hromadným získavaním údajov o komunikácii, ako aj príkazy na uchovávanie údajov o komunikácii musia byť schválené Komisármi pre justíciu ([456]). Komisár pre vyšetrovacie právomoci musí vždy vopred povoliť získavanie údajov o komunikácii na účely presadzovania práva ([457]). Ak Komisár odmietne schváliť príkaz, minister môže podať odvolanie Komisárovi pre vyšetrovacie právomoci, ktorého rozhodnutie je konečné.

([447]) V súlade s § 227 ods. 7 a 8 zákona o vyšetrovacích právomociach z roku 2016 Komisár pre vyšetrovacie právomoci je Komisárom pre justíciu a Komisár pre vyšetrovacie právomoci a ďalší Komisári pre justíciu sa spoločne označujú ako Komisári pre justíciu. V súčasnosti funkciu vykonáva 15 Komisárov pre justíciu.

([448]) Podľa ustanovení časti 3 § 60 ods. 2 zákona o reforme Ústavy z roku 2005 (Constitutional Reform Act) „vysoká súdna funkcia" je funkcia sudcu na ktoromkoľvek z týchto súdov: i) najvyšší súd; ii) odvolací súd pre Anglicko a Wales; iii) Vrchný súd pre Anglicko a Wales; iv) najvyšší civilný súd pre Škótsko (Court of Session); v) odvolací súd pre Severné Írsko; vi) Vrchný súd pre Severné Írsko (High Court in Northern Ireland) alebo ako osobitný sudca na najvyššom súde (Lord of Appeal in Ordinary).

([449]) Nezávislosť súdnej moci je založená na zvyklostiach a je široko uznávaná od prijatia zákonu o nástupníctve z roku 1701 (Act of Settlement).

([450]) § 227 ods. 3 zákona o vyšetrovacích právomociach z roku 2016. Komisári pre justíciu musia byť odporučení aj Komisárom pre vyšetrovacie právomoci, § 227 ods. 4 písm. e) zákona o vyšetrovacích právomociach z roku 2016.

([451]) § 238 zákona o vyšetrovacích právomociach z roku 2016.

([452]) § 227 ods. 2 zákona o vyšetrovacích právomociach z roku 2016.

([453]) Proces odvolania je totožný s procesom odvolania iných sudcov v Spojenom kráľovstve [pozri napríklad § 11 ods. 3 zákona o vyšších súdoch z roku 1981 (Senior Courts Act) a § 33 zákona o reforme Ústavy z roku 2005, v ktorých sa takisto vyžaduje uznesie po schválení oboma snemovňami parlamentu]. Ku dnešnému dňu nebol odvolaný žiadny Komisár pre justíciu z funkcie.

([454]) Nezávislý orgán je organizáciou alebo úradom, ktorý je financovaný vládou, ale môže konať nezávisle (definícia a podrobnejšie informácie o nezávislom orgáne sa nachádzajú v Príručke úradu vlády o klasifikácii verejných orgánov, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf, a v Prvej správe zo zasadnutia užšieho výboru Dolnej snemovne pre verejnú správu 2014 – 2015, k dispozícii na tomto odkaze: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf).

([455]) Podľa § 229 zákona o vyšetrovacích právomociach z roku 2016 má Komisár pre justíciu rozsiahle právomoci nad dohľadom, ktoré sa týkajú aj dohľadu nad uchovávaním a poskytovaním údajov získaných spravodajskými službami.

([456]) O schvaľovaní rozhodnutí ministra vydať príkaz rozhodujú samotní Komisári pre justíciu. Ak Komisár odmietne schváliť príkaz, minister môže podať odvolanie Komisárovi pre vyšetrovacie právomoci, ktorého rozhodnutie je konečné.

([457]) O povolenie Komisára pre vyšetrovacie právomoci sa žiada vždy, keď sa údaje o komunikácii získavajú na účely presadzovania práva (§ 60A zákona o vyšetrovacích právomociach z roku 2016). Ak sa údaje o komunikácii získavajú na účely národnej bezpečnosti, povolenie môže udeliť Komisár pre vyšetrovacie právomoci alebo prípadne určený vyšší úradník príslušného orgánu verejnej moci (pozri § 61 a 61A zákona o vyšetrovacích právomociach z roku 2016 a odôvodnenie 203).

(253) Osobitný spravodajca OSN pre právo na súkromie vskutku uvítal zriadenie funkcií Komisárov pre justíciu prostredníctvom zákona o vyšetrovacích právomociach z roku 2016, keďže „všetky citlivejšie alebo rušivejšie žiadosti o vykonanie sledovania musí povoliť minister vlády alebo Úrad Komisára pre vyšetrovacie právomoci". Zdôraznil najmä, že „tento prvok súdneho preskúmania [prostredníctvom úlohy Komisára pre vyšetrovacie právomoci], pri ktorom pomáha lepšie vybavený tím skúsených inšpektorov a technických odborníkov, je jednou z najvýznamnejších nových záruk, ktoré sa zaviedli zákonom o vyšetrovacích právomociach", ktorý nahradil predtým rozdrobený systém orgánov dohľadu a dopĺňa úlohu parlamentného výboru pre spravodajstvo a bezpečnosť a tribunálu pre kontrolu vyšetrovacích právomocí ([458]).

(254) Komisár pre vyšetrovacie právomoci má navyše podľa zákona o vyšetrovacích právomociach z roku 2016 ([459]) právomoc vykonávať dohľad *ex post*, a to aj formou auditu, kontroly a vyšetrovania, a niektoré ďalšie právomoci a funkcie, ktoré sú stanovené v príslušných právnych predpisoch ([460]). Výsledky takéhoto dohľadu *ex post* sú uvedené v správe, ktorú Komisár pre vyšetrovacie právomoci musí každoročne vypracovať a predložiť predsedovi vlády ([461]) a ktorá sa musí uverejniť a predložiť parlamentu ([462]). Správa obsahuje relevantné štatistické údaje a informácie o využívaní vyšetrovacích právomocí spravodajskými službami a orgánmi presadzovania práva, ako aj o zavádzaní záruk v súvislosti s položkami, na ktoré sa vzťahuje povinnosť advokáta zachovávať mlčanlivosť, s dôvernými žurnalistickými materiálmi a so zdrojmi žurnalistických informácií, informácie o prijatých opatreniach a operačných účeloch využívaných v kontexte hromadných príkazov. Napokon sa vo výročnej správe Úradu Komisára pre vyšetrovacie právomoci uvádza, v ktorej oblasti sa vydali odporúčania orgánom verejnej moci a akým spôsobom boli podané ([463]).

(255) V súlade s § 231 zákona o vyšetrovacích právomociach z roku 2016, ak sa Komisár pre vyšetrovacie právomoci dozvie o akejkoľvek relevantnej chybe zo strany orgánov verejnej moci pri využívaní vyšetrovacích právomocí, musí o tom informovať dotknutú osobu, ak sa domnieva, že ide o závažnú chybu a že je vo verejnom záujme, aby osoba bola informovaná ([464]). Konkrétne v § 231 zákona o vyšetrovacích právomociach z roku 2016 sa uvádza, že Komisár pre vyšetrovacie právomoci pri informovaní osoby o chybe musí uviesť informácie o všetkých právach, ktoré si osoba môže uplatniť na tribunáli pre kontrolu vyšetrovacích právomocí, a uviesť také informácie, aké Komisár považuje za nevyhnutné na výkon týchto práv a pri ktorých existuje verejný záujem na poskytnutí ([465]).

([458]) Záverečná správa z misie osobitného spravodajcu OSN pre právo na súkromie na záver jeho misie v Spojenom kráľovstve Veľkej Británie a Severného Írska (pozri poznámku pod čiarou č. 281).

([459]) § 229 zákona o vyšetrovacích právomociach z roku 2016. Vyšetrovanie Komisárom pre justíciu a právomoci týkajúce sa informácií sú uvedené v § 235 zákona o vyšetrovacích právomociach z roku 2016.

([460]) Patria sem opatrenia v oblasti sledovania podľa zákona o regulácii vyšetrovacích právomocí z roku 2000, výkon funkcií podľa časti 3 zákona o polícii z roku 1997 (Police Act) (povolenie konania v súvislosti s majetkom) a vykonávanie funkcií ministrom podľa § 5 až 7 zákona o spravodajských službách z roku 1994 (príkazy na zasahovanie do bezdrôtovej telegrafie, vstup na majetok a zasahovanie doň) (§ 229 zákona o vyšetrovacích právomociach z roku 2016).

([461]) § 230 zákona o vyšetrovacích právomociach z roku 2016. Komisár pre vyšetrovacie právomoci môže takisto z vlastnej iniciatívy podať predsedovi vlády správu týkajúcu sa akejkoľvek záležitosti súvisiacej s jeho funkciami. Komisár pre vyšetrovacie právomoci musí podať správu predsedovi vlády aj na jeho žiadosť a predseda vlády môže nariadiť Komisárovi pre vyšetrovacie právomoci, aby preskúmal všetky funkcie spravodajských služieb.

([462]) Niektoré časti možno vylúčiť, ak by ich zverejnenie bolo v rozpore s národnou bezpečnosťou.

([463]) Napríklad vo výročnej správe Úradu Komisára pre vyšetrovacie právomoci za rok 2019 (bod 6.38) sa uvádza, že Bezpečnostnej službe (MI5) sa odporučilo, aby zmenila svoju politiku uchovávania súborov hromadných osobných údajov vzhľadom na to, že mala zvoliť prístup, pri ktorom sa zohľadňuje proporcionalita uchovávania v prípade všetkých polí v držaných súboroch hromadných osobných údajov a pre každý držaný súbor hromadných osobných údajov. Úrad Komisára pre vyšetrovacie právomoci na konci roka 2018 vyjadril nespokojnosť s dodržiavaním tohto odporúčania a v správe za rok 2019 sa vysvetľuje, že Bezpečnostná služba (MI5) teraz zavádza nový proces na plnenie tejto požiadavky. Vo výročnej správe za rok 2019 (bod 8.22) sa okrem toho uvádza, že Vládnemu komunikačnému ústrediu sa poskytol súbor odporúčaní týkajúcich sa zaznamenávania proporcionality jeho vyhľadávania v hromadných údajoch. V správe sa potvrdzuje, že v tejto oblasti došlo koncom roka 2018 k zlepšeniam. Výročná správa Úradu Komisára pre vyšetrovacie právomoci z roku 2019, k dispozícii na tomto odkaze: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Každá kontrola orgánu verejnej moci vykonaná Úradom Komisára pre vyšetrovacie právomoci sa navyše uzatvára správou, ktorá sa poskytuje orgánu a zahŕňa akékoľvek odporúčania, ktoré vyplynuli z takejto kontroly. Každú následnú kontrolu potom začína Úrad Komisára pre vyšetrovacie právomoci preskúmaním akýchkoľvek posledných predchádzajúcich odporúčaní a prejaví sa to v novej správe o kontrole uvedením, či už boli predchádzajúce odporúčania splnené, alebo bol v ich plnení zaznamenaný pokrok.

([464]) Chyba sa považuje za „závažnú", ak sa Komisár domnieva, že dotknutej osobe spôsobila významnú škodu alebo ujmu (§ 231 ods. 2 zákona o vyšetrovacích právomociach z roku 2016). V roku 2018 bolo nahlásených 22 chýb, z ktorých sa osem považovalo za závažné a viedli k informovaniu dotknutej osoby. Pozri Výročnú správu Úradu Komisára pre vyšetrovacie právomoci z roku 2018, príloha C (pozri na tomto odkaze: https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018 %20final.pdf). V roku 2019 došlo k 14 chybám, ktoré boli považované za závažné. Pozri Výročnú správu Úradu Komisára pre vyšetrovacie právomoci z roku 2019, príloha C, pozri poznámku pod čiarou č. 463.

([465]) V § 231 zákona o vyšetrovacích právomociach z roku 2016 sa uvádza, že Komisár pre vyšetrovacie právomoci musí pri informovaní osoby o chybe uviesť také informácie, aké Komisár považuje za nevyhnutné na výkon týchto práv, najmä so zreteľom na rozsah, v ktorom by poskytnutie informácií bolo v rozpore s verejným záujmom alebo by poškodzovalo predchádzanie závažnej trestnej činnosti alebo jej odhaľovanie, hospodársky blahobyt Spojeného kráľovstva alebo ďalšie plnenie funkcií ktorejkoľvek spravodajskej služby.

3.3.3.3. Parlamentný dohľad nad spravodajskými službami

(256) Parlamentný dohľad výboru pre spravodajstvo a bezpečnosť má svoj právny základ v zákone o spravodlivosti a bezpečnosti z roku 2013 ([466]). Týmto zákonom sa v parlamente Spojeného kráľovstva zriaďuje výbor pre spravodajstvo a bezpečnosť. Od roku 2013 má výbor pre spravodajstvo a bezpečnosť väčšie právomoci vrátane dohľadu nad operačnými činnosťami bezpečnostných služieb. Podľa § 2 zákona o spravodlivosti a bezpečnosti z roku 2013 má tento výbor za úlohu dohliadať na výdavky, správu, politiku a činnosť služieb v oblasti národnej bezpečnosti. V zákone o spravodlivosti a bezpečnosti z roku 2013 sa uvádza, že výbor pre spravodajstvo a bezpečnosť môže prešetrovať operačné záležitosti, ak nesúvisia s prebiehajúcimi operáciami ([467]). V memorande o porozumení medzi predsedom vlády a výborom pre spravodajstvo a bezpečnosť ([468]) sa podrobne uvádzajú prvky, ktoré sa majú zohľadniť pri posudzovaní toho, či určitá činnosť nie je súčasťou žiadnej prebiehajúcej operácie ([469]). Výbor pre spravodajstvo a bezpečnosť môže o prešetrenie prebiehajúcich operácií požiadať aj predseda vlády a tento výbor môže preskúmavať aj informácie, ktoré poskytli služby dobrovoľne.

(257) Podľa prílohy 1 k zákonu o spravodlivosti a bezpečnosti z roku 2013 môže výbor pre spravodajstvo a bezpečnosť požiadať vedúcich ktorejkoľvek z troch spravodajských služieb o poskytnutie akýchkoľvek informácií. Daná služba nemusí tieto informácie sprístupniť, len ak príslušný minister neuplatnil právo veta ([470]). Podľa vysvetlení, ktoré poskytli orgány Spojeného kráľovstva, sa v praxi tomuto výboru zamieta prístup len k veľmi málo informáciám ([471]).

(258) Tento výbor pozostáva z členov oboch snemovní parlamentu, pričom za členov výboru ich vymenúva predseda vlády po konzultácii s lídrom opozície ([472]). Výbor pre spravodajstvo a bezpečnosť je povinný predkladať parlamentu výročnú správu o plnení svojich funkcií a ďalšie správy, ktoré považuje za vhodné ([473]). Výbor pre spravodajstvo a bezpečnosť má okrem toho nárok na to, aby mu bol každé tri mesiace doručený zoznam operačných účelov, ktorý sa využíva na preskúmanie hromadne získaných materiálov ([474]). Predseda vlády poskytuje kópie vyšetrovaní, kontrol alebo auditov Komisára pre vyšetrovacie právomoci výboru pre spravodajstvo a bezpečnosť, ak záležitosti uvedené v správach patria do zákonnej pôsobnosti výboru ([475]). Napokon výbor môže požiadať Komisára pre vyšetrovacie právomoci, aby uskutočnil vyšetrovanie, a Komisár musí výbor pre spravodajstvo a bezpečnosť informovať o rozhodnutí, či sa takéto vyšetrovanie uskutoční ([476]).

(259) Výbor pre spravodajstvo a bezpečnosť takisto poskytol podnety k návrhu zákona o vyšetrovacích právomociach z roku 2016, čo viedlo k viacerým zmenám, ktoré sú teraz začlenené do zákona o vyšetrovacích právomociach z roku 2016 ([477]). Výbor pre spravodajstvo a bezpečnosť konkrétne odporučil posilnenie ochrany súkromia, a to

([466]) Ako vysvetlili orgány Spojeného kráľovstva, zákonom o spravodlivosti a bezpečnosti z roku 2013 sa rozšíril rozsah pôsobnosti výboru pre spravodajstvo a bezpečnosť tak, aby zahŕňal úlohu dohľadu nad spravodajskou komunitou nad rámec troch agentúr a umožnil retrospektívny dohľad nad operačnými činnosťami týchto agentúr v otázkach významného národného záujmu.

([467]) § 2 zákona o spravodlivosti a bezpečnosti z roku 2013.

([468]) Memorandum o porozumení medzi predsedom vlády a výborom pre spravodajstvo a bezpečnosť, k dispozícii na tomto odkaze: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.

([469]) Memorandum o porozumení medzi predsedom vlády a výborom pre spravodajstvo a bezpečnosť, bod 14, pozri poznámku pod čiarou č 468.

([470]) Minister môže vetovať poskytnutie informácií len z dvoch dôvodov: informácie sú citlivé a nemali by byť výboru pre spravodajstvo a bezpečnosť sprístupnené v záujme národnej bezpečnosti, resp. ide o informácie takej povahy, že ak by bol minister požiadaný, aby ich predložil užšiemu rezortnému výboru Dolnej snemovne, považoval by ich predloženie (z dôvodov neobmedzujúcich sa len na dôvody národnej bezpečnosti) za nevhodné (príloha 1 bod 4 ods. 2 k zákonu o spravodlivosti a bezpečnosti z roku 2013).

([471]) Vysvetľujúci rámec Spojeného kráľovstva pre diskusiu o primeranosti, oddiel H s názvom National Security (Národná bezpečnosť), s. 43 (pozri poznámku pod čiarou č. 31).

([472]) § 1 zákona o spravodlivosti a bezpečnosti z roku 2013. Ministri nemôžu byť členmi. Poslanci sú členmi tohto výboru počas funkčného obdobia parlamentu, v rámci ktorého boli vymenovaní. Členstva v tomto výbore môžu byť zbavení uznesením snemovne, ktorá ich vymenovala, resp. ak stratia poslanecký mandát alebo sa stanú ministrami. Člen výboru sa takisto môže svojho členstva vzdať.

([473]) Správy a vyhlásenia výboru sú dostupné online na tomto odkaze: https://isc.independent.gov.uk/publications/. V roku 2015 vydal výbor pre spravodajstvo a bezpečnosť správu s názvom „Súkromie a bezpečnosť: moderný a transparentný právny rámec“ (pozri: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), v ktorom posúdil právny rámec techník sledovania, ktoré používajú spravodajské služby, a vydal súbor odporúčaní, ktoré boli následne posúdené a začlenené do návrhu zákona o vyšetrovacích právomociach, ktorý sa stal zákonom o vyšetrovacích právomociach z roku 2016. Odpoveď vlády na túto správu je k dispozícii na tomto odkaze: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

([474]) § 142, § 161 a § 183 zákona o vyšetrovacích právomociach z roku 2016.

([475]) § 234 zákona o vyšetrovacích právomociach z roku 2016.

([476]) § 236 zákona o vyšetrovacích právomociach z roku 2016.

([477]) Výbor parlamentu pre spravodajstvo a bezpečnosť, Správa k návrhu zákona o vyšetrovacích právomociach, k dispozícii na tomto odkaze: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf.

zavedením súboru opatrení na ochranu súkromia, ktoré sa uplatňujú v celej škále vyšetrovacích právomocí ([478]). Výbor okrem toho navrhol zmeny navrhnutých spôsobilostí v oblasti zasahovania do zariadení, súborov hromadných osobných údajov a údajov o komunikácii a požiadal o ďalšie konkrétne zmeny na posilnenie obmedzení a záruk využívania vyšetrovacích právomocí ([479]).

3.3.4. *Náprava*

(260) V oblasti prístupu vlády na účely národnej bezpečnosti musia mať dotknuté osoby možnosť uplatniť právne prostriedky nápravy pred nezávislým a nestranným súdom, aby mali prístup k osobným údajom, ktoré sa ich týkajú, alebo dosiahnuť opravu alebo vymazanie takýchto údajov ([480]). Takýto súdny orgán musí mať najmä právomoc prijímať záväzné rozhodnutia týkajúce sa spravodajských služieb ([481]). V Spojenom kráľovstve, ako sa vysvetľuje v odôvodneniach (261) až (271), niekoľko súdnych prostriedkov nápravy poskytuje dotknutým osobám možnosť vyžadovať a získať takéto právne prostriedky nápravy.

3.3.4.1. Mechanizmy nápravy dostupné podľa časti 4 zákona o ochrane údajov

(261) Podľa § 165 zákona o ochrane údajov z roku 2018 má dotknutá osoba právo podať sťažnosť Komisárovi pre informácie, ak sa domnieva, že v súvislosti s osobnými údajmi, ktoré sa jej týkajú, došlo k porušeniu časti 4 zákona o ochrane údajov z roku 2018. Komisár pre informácie má právomoc posúdiť dodržiavanie zákona o ochrane údajov z roku 2018 zo strany prevádzkovateľa a sprostredkovateľa a požadovať od nich, aby prijali potrebné kroky. Okrem toho podľa časti 4 zákona o ochrane údajov z roku 2018 sú jednotlivci oprávnení podať na Vrchný súd (High Court), resp. v Škótsku na Court of Session, návrh na vydanie príkazu, ktorým sa od prevádzkovateľa vyžaduje, aby dodržiaval právo na prístup k údajom ([482]), právo namietať voči spracúvaniu ([483]) a právo na opravu alebo vymazanie ([484]).

(262) Jednotlivci sú tiež oprávnení požadovať od prevádzkovateľa alebo sprostredkovateľa náhradu škody utrpenej v dôsledku porušenia požiadavky časti 4 zákona o ochrane údajov z roku 2018 ([485]). Škoda zahŕňa tak finančnú ujmu, ako aj škodu, ktorá nezahŕňa finančnú ujmu, ako napríklad nemajetkovú ujmu ([486]).

3.3.4.2. Mechanizmy nápravy dostupné podľa zákona o vyšetrovacích právomociach z roku 2016

(263) Osoby môžu vymôcť nápravu za porušenie zákona o vyšetrovacích právomociach z roku 2016 pred tribunálom pre kontrolu vyšetrovacích právomocí.

(264) Tribunál pre kontrolu vyšetrovacích právomocí sa zriaďuje na základe zákona o regulácii vyšetrovacích právomocí z roku 2000 a je nezávislý od výkonnej moci ([487]). V súlade s § 65 zákona o regulácii vyšetrovacích právomocí z roku 2000 členov tribunálu pre kontrolu vyšetrovacích právomocí vymenúva jej veličenstvo na obdobie piatich rokov. Z funkcie môže člena tribunálu odvolať jej veličenstvo na základe jej určenému prejavu vôle (tzv. Address) ([488]) oboch snemovní parlamentu ([489]).

([478]) Tieto všeobecné povinnosti súvisiace so súkromím sú teraz uvedené v § 2 ods. 2 zákona o vyšetrovacích právomociach z roku 2016, v ktorom sa stanovuje, že orgán verejnej moci konajúci na základe zákona o vyšetrovacích právomociach z roku 2016 musí prihliadať na to, či by sa to, čo sa má dosiahnuť príkazom, povolením alebo oznámením, mohlo primerane dosiahnuť inými menej rušivými prostriedkami, či úroveň ochrany, ktorá sa má uplatňovať v súvislosti s akýmkoľvek získavaním informácií na základe príkazu, povolenia alebo oznámenia, je vyššia z dôvodu osobitnej citlivosti týchto informácií, ako aj na verejný záujem na integrite a bezpečnosti telekomunikačných systémov a poštových služieb a akékoľvek iné aspekty verejného záujmu na ochrane súkromia.

([479]) Napríklad na základe žiadosti výboru pre spravodajstvo a bezpečnosť sa počet dní, počas ktorých môže byť zavedený „naliehavý" príkaz pred tým, ako ho Komisár pre justíciu musí schváliť, sa znížil z piatich na tri pracovné dni a výboru pre spravodajstvo a bezpečnosť bola udelená právomoc postúpiť záležitosti Komisárovi pre vyšetrovacie právomoci, aby ich vyšetril.

([480]) Schrems II, bod 194.

([481]) Schrems II, bod 197.

([482]) § 94 ods. 11 zákona o ochrane údajov z roku 2018.

([483]) § 99 ods. 4 zákona o ochrane údajov z roku 2018.

([484]) § 100 ods. 1 zákona o ochrane údajov z roku 2018.

([485]) § 169 zákona o ochrane údajov z roku 2018 umožňuje uplatnenie si nároku osobám, ktoré utrpeli škodu v dôsledku porušenia požiadavky právnych predpisov o ochrane údajov. Z informácií, ktoré uviedli orgány Spojeného kráľovstva, vyplýva, že v praxi sa pravdepodobne uplatní nárok alebo sťažnosť voči spravodajským službám na tribunáli pre kontrolu vyšetrovacích právomocí, ktorý má rozsiahlu právomoc a môže vydať rozhodnutie o náhrade škody, a to ak sa uplatňuje nárok, ktorý nezahŕňa žiadne náklady.

([486]) § 169 ods. 5 zákona o ochrane údajov z roku 2018.

([487]) Podľa prílohy 3 k zákonu o regulácii vyšetrovacích právomocí z roku 2000 musia členovia tribunálu mať konkrétne skúsenosti v súdnictve a musia byť oprávnení na opätovné vymenovanie.

([488]) „Address" je návrh predložený parlamentu, ktorého cieľom je upovedomiť monarchu o stanoviskách parlamentu k určitej téme.

([489]) Príloha 3 bod 1 ods. 5 k zákonu o regulácii vyšetrovacích právomocí z roku 2000.

(265) Na základe § 65 zákona o regulácii vyšetrovacích právomocí z roku 2000 je tribunál príslušným súdnym orgánom na podanie sťažnosti osobou, ktorá bola poškodená konaním podľa ustanovení zákona o vyšetrovacích právomociach z roku 2016, zákona o regulácii vyšetrovacích právomocí z roku 2000 alebo akýmkoľvek konaním spravodajských služieb ([490]).

(266) Keď chce jednotlivec podať návrh na začatie konania na tribunáli pre kontrolu vyšetrovacích právomocí (ďalej len „požiadavka na aktívnu legitimáciu"), musí byť podľa § 65 zákona o regulácii vyšetrovacích právomocí z roku 2000 presvedčený ([491]), že spravodajská služba konala vo vzťahu k nemu, k jeho akémukoľvek majetku, k akejkoľvek komunikácii uskutočnenej ním alebo jemu určenej, k jeho využitiu akejkoľvek poštovej služby, telekomunikačnej služby alebo telekomunikačného systému ([492]). Okrem toho musí byť sťažovateľ presvedčený, že k tomuto konaniu došlo za „napadnuteľných okolností" ([493]) alebo „bolo vykonané spravodajskými službami alebo v ich mene" ([494]). Keďže najmä tento štandard „presvedčenia" bol vykladaný pomerne široko ([495]), podanie návrhu na tento tribunál podlieha pomerne nízkym požiadavkám na aktívnu legitimáciu.

(267) Ak sa tribunál pre kontrolu vyšetrovacích právomocí zaoberá sťažnosťou, ktorá mu bola predložená, je jeho povinnosťou preskúmať, či osoby, voči ktorým sťažnosť smeruje, vyvíjali určité aktivity vo vzťahu k sťažovateľovi, ako aj vyšetriť orgán, ktorý sa údajne dopustil porušenia a či k údajnej aktivite došlo ([496]). Uvedený tribunál je povinný v rámci svojho akéhokoľvek konania pri rozhodovaní v tomto konaní uplatniť rovnaké zásady, aké by uplatnil súd v prípade návrhu na súdne preskúmanie ([497]). Okrem toho adresáti príkazov alebo oznámení podľa zákona o vyšetrovacích právomociach z roku 2016 a každá ďalšia osoba vykonávajúca funkciu v rámci koruny, ktorá je zamestnancom policajnej zložky alebo Komisára pre policajné vyšetrovanie a kontrolu, má povinnosť poskytnúť alebo sprístupniť uvedenému tribunálu všetky dokumenty a informácie, ktoré tribunál môže požadovať, aby bol schopný vykonávať svoju právomoc ([498]).

(268) Tribunál pre kontrolu vyšetrovacích právomocí musí sťažovateľovi oznámiť, či bolo rozhodnuté v jeho prospech ([499]). Podľa § 67 ods. 6 a 7 zákona o regulácii vyšetrovacích právomocí z roku 2000 má tribunál právomoc vydať predbežné uznesenie a vydať akékoľvek rozhodnutie o náhrade škody alebo iné rozhodnutie, ktoré považuje za vhodné. Môže to zahŕňať rozhodnutie, ktorým sa zruší alebo anuluje akýkoľvek príkaz alebo povolenie, a rozhodnutie, ktorým sa vyžaduje zničenie akýchkoľvek záznamov informácií získaných pri výkone akejkoľvek

([490]) § 65 ods. 5 zákona o regulácii vyšetrovacích právomocí z roku 2000.

([491]) Pokiaľ ide o kritérium štandardu „presvedčenia", pozri vec Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH, bod 41. V tomto prípade tribunál pre kontrolu vyšetrovacích právomocí s odvolaním sa na judikatúru Európskeho súdu pre ľudské práva rozhodol, že kritériom, pokiaľ ide o overenie existencie údajného presvedčenia, že akékoľvek konanie patriace pod § 68 ods. 5 zákona o regulácii vyšetrovacích právomocí z roku 2000 bolo vykonané niektorou zo spravodajských služieb alebo v ich mene, je to, či existuje nejaký základ pre toto presvedčenie, podľa ktorého jednotlivec môže tvrdiť, že je obeťou porušenia spôsobeného samotnou existenciou utajovaných opatrení alebo právnych predpisov umožňujúcich utajované opatrenia, čiže iba ak je tento jednotlivec schopný preukázať, že vzhľadom na jeho osobnú situáciu je potenciálne vystavený riziku, že bude podrobený takýmto opatreniam.

([492]) § 65 ods. 4 písm. a) zákona o regulácii vyšetrovacích právomocí z roku 2000.

([493]) Takéto okolnosti sa týkajú konania orgánov verejnej moci, ku ktorému dochádza pri výkone právomoci (napr. príkaz, povolenie na získanie komunikácie alebo oznámenie s cieľom získať ju atď.), resp. ak sú okolnosti také, že (bez ohľadu na to, či takáto právomoc existuje), by nebolo náležité, ak by sa dané konanie uskutočňovalo bez nej, alebo prinajmenšom bez toho, aby sa náležite zvážilo, či by daný verejný orgán nemal takouto právomocou disponovať. Konanie povolené Komisárom pre justíciu sa považuje za konania uskutočnené za napadnuteľných okolností [§ 65 (7ZA) zákona o regulácii vyšetrovacích právomocí z roku 2000], zatiaľ čo iné konania, ku ktorým dochádza so súhlasom osoby vykonávajúcej sudcovskú funkciu, sa považujú za také, ku ktorým nedošlo za napadnuteľných okolností (§ 65 ods. 7 a 8 zákona o regulácii vyšetrovacích právomocí z roku 2000).

([494]) Podľa informácií, ktoré poskytli orgány Spojeného kráľovstva, nízke požiadavky na podanie sťažnosti vedú k tomu, že nie je nezvyčajné, aby sa po súdnom prešetrovaní dospelo k záveru, že sťažovateľ nebol nikdy predmetom vyšetrovania zo strany orgánu verejnej moci. V najnovšej štatistickej správe tribunálu pre kontrolu vyšetrovacích právomocí sa uvádza, že v roku 2016 dostal tento tribunál 209 sťažností, 52 % z nich bolo považovaných za zjavne neopodstatnené alebo šikanujúce sťažnosti a 25 % bolo uzavretých „bez určenia". Orgány Spojeného kráľovstva vysvetlili, že to znamená, že vo vzťahu k sťažovateľovi nebola realizovaná žiadna utajená činnosť ani právomoci, resp. že boli použité utajené prostriedky, ale tribunál dospel k záveru, že sa tak stalo v súlade so zákonom. Ďalších 11 % bolo vylúčených z dôvodu chýbajúcej právomoci, stiahnutých alebo neplatných, 5 % bolo vylúčených z dôvodu premeškania lehoty na podanie sťažnosti a 7 % bolo uzavretých v prospech sťažovateľa. Štatistická správa tribunálu pre kontrolu vyšetrovacích právomocí z roku 2016 je k dispozícii na tomto odkaze: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([495]) Pozri vec Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH. V tomto prípade tribunál pre kontrolu vyšetrovacích právomocí s odvolaním sa na judikatúru ESĽP rozhodol, že kritériom, pokiaľ ide o overenie existencie presvedčenia, že akékoľvek konanie spadajúce pod § 68 ods. 5 zákona o regulácii vyšetrovacích právomocí z roku 2000 bolo vykonané niektorou zo spravodajských služieb alebo v ich mene, je to, či existuje nejaký základ pre takéto presvedčenie vrátane skutočnosti, že jednotlivec môže tvrdiť, že je obeťou porušenia spôsobeného samotnou existenciou utajovaných opatrení alebo právnych predpisov umožňujúcich utajované opatrenia iba vtedy, ak je tento jednotlivec schopný preukázať, že vzhľadom na jeho osobnú situáciu je potenciálne vystavený riziku, že bude podrobený takýmto opatreniam (pozri rozsudok Human Rights Watch/Secretary of State, bod 41).

([496]) § 67 ods. 3 zákona o regulácii vyšetrovacích právomocí z roku 2000.

([497]) § 67 ods. 2 zákona o regulácii vyšetrovacích právomocí z roku 2000.

([498]) § 68 ods. 6 a 7 zákona o regulácii vyšetrovacích právomocí z roku 2000.

([499]) § 68 ods. 4 zákona o regulácii vyšetrovacích právomocí z roku 2000.

právomoci, ktorá bola udelená na základe príkazu, povolenia alebo oznámenia, alebo informácií, ktoré má ktorýkoľvek orgán verejnej moci v súvislosti s ktoroukoľvek osobou ([500]). Podľa § 67A zákona o regulácii vyšetrovacích právomocí z roku 2000 možno proti rozhodnutiu tribunálu podať odvolanie s výhradou povolenia udeleného tribunálom alebo príslušným odvolacím súdom.

(269) Napokon je potrebné poznamenať, že o úlohe tribunálu pre kontrolu vyšetrovacích právomocí sa niekoľkokrát diskutovalo v kontexte konaní na Európskom súde pre ľudské práva, najmä vo veci Kennedy/the United Kingdom ([501]) a nedávnejšie vo veci Big Brother Watch and others/United Kingdom ([502]), keď súd vyhlásil že „tribunál pre kontrolu vyšetrovacích právomocí sa osvedčil ako dostupný prostriedok nápravy pre každého, kto má podozrenie, že jeho komunikáciu zachytili spravodajské služby“ ([503]).

3.3.4.3. Iné dostupné mechanizmy nápravy

(270) Ako sa uvádza v odôvodneniach (109) až (111), prostriedky nápravy, ktoré sú dostupné podľa zákona o ľudských právach z roku 1998 a možno ich vymáhať na Európskom súde pre ľudské práva ([504]), sú dostupné aj v oblasti národnej bezpečnosti. V § 65 ods. 2 zákona o regulácii vyšetrovacích právomocí z roku 2000 sa stanovuje, že tribunál pre kontrolu vyšetrovacích právomocí má výlučnú právomoc pre všetky žaloby opierajúce sa o zákon o ľudských právach vo vzťahu k spravodajským službám ([505]). To znamená, ako uviedol Vrchný súd (High Court), že to, „či došlo k porušeniu zákona o ľudských právach v súvislosti so skutkovými okolnosťami konkrétneho prípadu, je niečo, čo môže v zásade prerokovať a rozhodnúť nezávislý súd, ktorý môže mať prístup ku všetkým relevantným materiálom vrátane tajných materiálov. [...] V tejto súvislosti berieme do úvahy aj to, že aj na tribunál pre kontrolu vyšetrovacích právomocí sa teraz vzťahuje možnosť podať odvolanie na príslušný odvolací súd [v Anglicku a Walese by to bol odvolací súd (Court of Appeal)], pričom najvyšší súd (Supreme Court) nedávno rozhodol, že tribunál pre kontrolu vyšetrovacích právomocí v zásade podlieha súdnemu preskúmaniu: pozri R (Privacy International)/Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219“ ([506]).

(271) Z uvedeného vyplýva, že ak orgány presadzovania práva Spojeného kráľovstva alebo národné bezpečnostné orgány majú prístup k osobným údajom patriacim do pôsobnosti tohto rozhodnutia, takýto prístup upravujú zákony, v ktorých sa stanovujú podmienky, za ktorých sa prístup môže získať, pričom zabezpečujú, že prístup k údajom a ich ďalšie používanie je obmedzené na to, čo je nevyhnutné a primerané na sledované ciele presadzovania práva alebo národnej bezpečnosti. Okrem toho takýto prístup vo väčšine prípadov podlieha predchádzajúcemu povoleniu súdneho orgánu prostredníctvom schválenia príkazu alebo príkazu na predloženie dôkazov a v každom prípade podlieha nezávislému dohľadu. Keď orgány verejnej moci získajú prístup k údajom, na ich spracúvanie, a to aj na ich ďalšie poskytovanie a následný prenos sa vzťahujú osobitné záruky ochrany údajov podľa časti 3 zákona o ochrane údajov z roku 2018, ktoré odrážajú záruky stanovené v smernici (EÚ) 2016/680, na účely spracúvania orgánmi presadzovania práva a podľa časti 4 zákona o ochrane údajov z roku 2018 na účely spracúvania spravodajskými službami. Dotknuté osoby napokon majú v tejto oblasti nárok na účinné správne a súdne prostriedky nápravy vrátane práva na prístup k svojim údajom alebo práva na opravu alebo vymazanie takýchto údajov.

(272) Vzhľadom na dôležitosť takých podmienok, obmedzení a záruk na účely tohto rozhodnutia bude Komisia dôkladne monitorovať uplatňovanie a výklad pravidiel Spojeného kráľovstva súvisiacich s prístupom vlády k údajom. Toto bude zahŕňať vývoj príslušných právnych prepisov, vývoj v oblasti regulácie a judikatúry, ako aj činnosti Komisára pre informácie a ostatných orgánov dohľadu v tejto oblasti. Zvláštna pozornosť bude venovaná aj výkonu

([500]) Príkladom uplatňovania týchto právomocí je vec Liberty & Others/the Security Service, SIS, GCHQ, [2015] UKIP Trib 13_77-H_2. Tribunál rozhodol v prospech dvoch sťažovateľov, v jednom prípade preto, že jeho komunikácia bola uchovávaná dlhšie, ako bola určená lehota, a v druhom preto, že postup preskúmania nebol v súlade so stanovenými vnútornými pravidlami Vládneho komunikačného ústredia. V prvom prípade súd vydal príkaz, aby spravodajské služby zničili komunikáciu, ktorá bola uchovávaná dlhšie, než bola príslušná lehota. V druhom prípade nedošlo k vydaniu príkazu na zničenie, pretože komunikácia sa neuchovala.

([501]) Kennedy, pozri poznámku pod čiarou č. 129.

([502]) Európsky súd pre ľudské práva, vec Big Brother Watch and others/United Kingdom, (pozri poznámku pod čiarkou č. 268), body 413 až 415.

([503]) Európsky súd pre ľudské práva, Big Brother Watch, bod 425.

([504]) Ako je to znázornené napríklad v nedávnom rozsudku veľkej komory Európskeho súdu pre ľudské práva vo veci Big Brother Watch and others/United Kingdom (pozri poznámku pod čiarou č. 279), toto umožní účinné súdne preskúmanie – podobné tomu, ktoré sa vzťahuje na členské štáty EÚ – medzinárodným súdom, pokiaľ ide o dodržiavanie základných práv orgánmi verejnej moci pri získavaní prístupu k osobným údajom. Výkon rozsudkov Európskeho súdu pre ľudské práva podlieha osobitnému dohľadu Rady Európy.

([505]) Vo veci Belhaj & others [2017] UKSC 3 je základom pre rozhodnutie o nezákonnosti zachytávania materiálu, na ktorý sa vzťahuje povinnosť advokáta zachovávať mlčanlivosť, článok 8 Európskeho dohovoru o ľudských právach (pozri rozhodnutie 11).

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

príslušných rozsudkov Európskeho súdu pre ľudské práva v Spojenom kráľovstve vrátane opatrení identifikovaných v „akčných plánoch“ a „správach o opatreniach“, ktoré v rámci dohľadu nad dodržiavaním rozhodnutí Súdneho dvora predloží Výbor ministrov.

4. ZÁVER

(273) Komisia sa domnieva, že všeobecným nariadením Spojeného kráľovstva o ochrane údajov a zákonom o ochrane údajov z roku 2018 sa zabezpečuje úroveň ochrany osobných údajov prenášaných v Európskej únii, ktorá v zásade zodpovedá úrovni zaručenej nariadením (EÚ) 2016/679.

(274) Komisia sa okrem toho domnieva, že mechanizmy dohľadu a možnosti získania nápravy v právnom poriadku Spojeného kráľovstva umožňujú ako celok v praxi odhaliť a postihnúť porušovanie a poskytujú dotknutej osobe právne prostriedky nápravy na získanie prístupu k osobným údajom, ktoré sa jej týkajú, a prípadne aj na dosiahnutie opravy alebo vymazania takýchto údajov.

(275) Komisia sa napokon na základe dostupných informácií o právnom poriadku Spojeného kráľovstva domnieva, že akýkoľvek zásah do základných práv jednotlivcov, ktorých osobné údaje do Spojeného kráľovstva prenášajú orgány verejnej moci Spojeného kráľovstva z Európskej únie na účely verejného záujmu, a to najmä na účely presadzovania práva a národnej bezpečnosti, sa obmedzí na to, čo je nevyhnutne potrebné na dosiahnutie dotknutého legitímneho cieľa, a že existuje účinná právna ochrana proti takémuto zásahu.

(276) Vzhľadom na zistenia vyplývajúce z tohto rozhodnutia by sa preto malo rozhodnúť, že Spojené kráľovstvo zabezpečuje primeranú úroveň ochrany v zmysle článku 45 nariadenia (EÚ) 2016/679, vykladaného so zreteľom na Chartu základných práv Európskej únie.

(277) Tento záver vychádza tak z príslušného vnútroštátneho režimu Spojeného kráľovstva, ako aj z jeho medzinárodných záväzkov, najmä z dodržiavania Európskeho dohovoru o ľudských právach a z podriadenia sa právomoci Európskeho súdu pre ľudské práva. Pretrvávajúce dodržiavanie týchto medzinárodných záväzkov je preto mimoriadne dôležitým prvkom posúdenia, na ktorom sa zakladá toto rozhodnutie.

5. ÚČINKY TOHTO ROZHODNUTIA A KONANIE ORGÁNOV PRE OCHRANU ÚDAJOV

(278) Členské štáty a ich orgány sú povinné prijať opatrenia potrebné na dosiahnutie súladu s aktmi inštitúcií Únie, lebo tieto akty požívajú prezumpciu zákonnosti a majú z tohto dôvodu právne účinky dovtedy, kým neuplynie ich platnosť, kým nie sú derogované, zrušené v konaní o žalobe o neplatnosť alebo vyhlásené za neplatné v nadväznosti na návrh na začatie prejudiciálneho konania alebo námietku nezákonnosti.

(279) Rozhodnutie Komisie o primeranosti prijaté podľa článku 45 ods. 3 nariadenia (EÚ) 2016/679 je preto záväzné pre všetky orgány členských štátov, ktorým je určené, vrátane ich nezávislých dozorných orgánov. Najmä počas obdobia uplatňovania tohto rozhodnutia sa prenosy od prevádzkovateľa alebo sprostredkovateľa v Európskej únii k prevádzkovateľom alebo sprostredkovateľom v Spojenom kráľovstve môžu uskutočniť bez toho, aby bolo potrebné získať akékoľvek ďalšie povolenie.

(280) Zároveň treba pripomenúť, že podľa článku 58 ods. 5 nariadenia (EÚ) 2016/679 a ako Súdny dvor ozrejmil v rozsudku vo veci Schrems ([507]), ak vnútroštátny orgán pre ochranu údajov spochybňuje, a to aj na základe sťažnosti, zlučiteľnosť rozhodnutia Komisie o primeranosti so základnými právami jednotlivca na súkromie a ochranu údajov, vnútroštátne právo mu musí poskytnúť právny prostriedok nápravy umožňujúci uplatniť tieto výhrady na vnútroštátnom súde, ktorý môže mať povinnosť podať návrh na začatie prejudiciálneho konania na Súdnom dvore ([508]).

([507]) Schrems, bod 65.

([508]) Schrems, bod 65: „V tomto ohľade je úlohou vnútroštátneho zákonodarcu stanoviť prostriedky nápravy umožňujúce dotknutému vnútroštátnemu dozornému orgánu uplatniť výhrady, ktoré považuje za dôvodné, na vnútroštátnych súdoch, aby tieto podali, ak majú rovnaké pochybnosti ako tento orgán, pokiaľ ide o platnosť rozhodnutia Komisie, návrh na začatie prejudiciálneho konania na účely preskúmania platnosti tohto rozhodnutia.“

6. MONITOROVANIE, POZASTAVENIE, ZRUŠENIE ALEBO ZMENA TOHTO ROZHODNUTIA

(281) Podľa článku 45 ods. 4 nariadenia (EÚ) 2016/679 má Komisia po prijatí tohto rozhodnutia priebežne monitorovať príslušný vývoj v Spojenom kráľovstve, s cieľom posúdiť, či Spojené kráľovstvo stále zabezpečuje v zásade rovnocennú úroveň ochrany. Takéto monitorovanie je v tomto prípade osobitne dôležité, keďže Spojené kráľovstvo bude spravovať, uplatňovať a presadzovať nový režim ochrany údajov, ktorý už nepodlieha právu Európskej únie a ktorý sa môže vyvíjať. V tejto súvislosti sa bude osobitná pozornosť venovať praktickému uplatňovaniu pravidiel Spojeného kráľovstva o prenosoch osobných údajov do tretích krajín a dosahu, ktorý tento prenos môže mať na úroveň ochrany poskytovanej údajom prenášaným na základe tohto rozhodnutia. účinnosti uplatňovania individuálnych práv vrátane akejkoľvek relevantnej zmeny v právnych predpisoch a praxi týkajúcej sa výnimiek z takých práv alebo obmedzení takých práv (najmä toho, ktoré sa týka zachovania účinnej imigračnej kontroly), ako aj dodržiavania obmedzení a záruk s ohľadom na prístup vlády. Monitorovanie Komisie bude okrem iných prvkov vychádzať z informácií o vývoji judikatúry a dohľade zo strany Komisára pre informácie a ďalších nezávislých orgánov.

(282) Aby sa toto monitorovanie uľahčilo, orgány Spojeného kráľovstva by mali bezodkladne informovať Komisiu o každej podstatnej zmene právneho poriadku Spojeného kráľovstva, ktorá má vplyv na právny rámec, ktorý je predmetom tohto rozhodnutia, ako aj o akomkoľvek vývoji postupov týkajúcich sa spracúvania osobných údajov posudzovaných v tomto rozhodnutí, pokiaľ ide o spracúvanie osobných údajov tak prevádzkovateľmi, ako aj sprostredkovateľmi podľa všeobecného nariadenia Spojeného kráľovstva o ochrane osobných údajov a obmedzenia a záruky, ktoré sú uplatniteľné na prístup orgánov verejnej moci k osobným údajom. To by malo zahŕňať vývoj týkajúci sa prvkov uvedených v odôvodnení 281.

(283) Navyše, aby Komisia mohla účinne vykonávať svoju monitorovaciu funkciu, mali by ju členské štáty informovať o všetkých relevantných opatreniach, ktoré prijali vnútroštátne orgány pre ochranu údajov, najmä pokiaľ ide o otázky alebo sťažnosti dotknutých osôb z EÚ týkajúce sa prenosu osobných údajov z Únie prevádzkovateľom alebo sprostredkovateľom v Spojenom kráľovstve. Komisia by mala byť informovaná aj o akýchkoľvek známkach toho, že opatrenia orgánov verejnej moci Spojeného kráľovstva zodpovedných za predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie alebo za národnú bezpečnosť vrátane akýchkoľvek dozorných orgánov nezabezpečujú požadovanú úroveň ochrany.

(284) Ak dostupné informácie, najmä informácie vyplývajúce z monitorovania tohto rozhodnutia alebo poskytnuté orgánmi Spojeného kráľovstva alebo členských štátov, odhalia, že úroveň ochrany poskytovaná Spojeným kráľovstvom už nemusí byť primeraná, Komisia by o tom mala informovať príslušné orgány Spojeného kráľovstva a požiadať o prijatie náležitých opatrení v určenej lehote, ktorá nesmie presiahnuť tri mesiace. Táto lehota sa môže predĺžiť v prípade potreby o určený čas, a to pri zohľadnení povahu príslušnej záležitosti a/alebo opatrenia, ktoré majú byť prijaté. Taký postup by sa napríklad uplatnil v prípadoch, keď by sa následné prenosy vrátane prenosov na základe nových právnych predpisov o primeranosti prijatých ministrom alebo medzinárodných dohôd uzavretých Spojených kráľovstvom už nevykonávali podľa záruk zabezpečujúcich kontinuitu ochrany v zmysle článku 44 nariadenia (EÚ) 2016/679.

(285) Ak po uplynutí uvedenej stanovenej lehoty príslušné orgány Spojeného kráľovstva neprijmú takéto opatrenia alebo inak uspokojivo nepreukážu, že toto rozhodnutie sa naďalej zakladá na primeranej úrovni ochrany, Komisia začne postup uvedený v článku 93 ods. 2 nariadenia (EÚ) 2016/679 s cieľom čiastočne alebo úplne pozastaviť alebo zrušiť toto rozhodnutie.

(286) Alternatívne Komisia začne postup s cieľom zmeniť toto rozhodnutie, najmä podriadením prenosu údajov dodatočným podmienkam alebo obmedzením rozsahu konštatovanej primeranosti len na tie prenosy údajov, pri ktorých je naďalej zabezpečená primeraná úroveň ochrany.

(287) Komisia využije z riadne odôvodnených vážnych a naliehavých dôvodov možnosť prijať v súlade s postupom uvedeným v článku 93 ods. 3 nariadenia (EÚ) 2016/679 okamžite uplatniteľné vykonávacie akty, ktorými sa pozastaví, zruší alebo zmení toto rozhodnutie

7. OBDOBIE PLATNOSTI TOHTO ROZHODNUTIA A PREDĹŽENIE JEHO PLATNOSTI

(288) Komisia musí zohľadniť, že po skončení prechodného obdobia stanoveného v dohode o vystúpení a hneď, ako sa prestane uplatňovať dočasné ustanovenie podľa článku 782 Dohody o obchode a spolupráci medzi EÚ a Spojeným kráľovstvom, bude Spojené kráľovstvo v porovnaní s režimom uplatňovaným v čase, keď bolo viazané právom EÚ, spravovať, uplatňovať a presadzovať nový režim ochrany údajov. Môže to zahŕňať najmä zmeny rámca ochrany údajov, ktorý bol predmetom posúdenia v tomto rozhodnutí, ako aj ďalší relevantný vývoj.

(289) Preto je vhodné stanoviť, že toto rozhodnutie sa bude uplatňovať počas obdobia štyroch rokov od nadobudnutia jeho účinnosti.

(290) Ak najmä z informácií vyplývajúcich z monitorovania tohto rozhodnutia vyplynie, že zistenia týkajúce sa primeranosti úrovne ochrany zabezpečenej v Spojenom kráľovstve sú stále fakticky a právne odôvodnené, Komisia by mala najneskôr šesť mesiacov pred skončením uplatňovania tohto rozhodnutia začať postup na zmenu tohto rozhodnutia predĺžením jeho časovej pôsobnosti v zásade o ďalšie štyri roky. Akýkoľvek takýto vykonávací akt, ktorým sa mení toto rozhodnutie, sa má prijať v súlade s postupom uvedeným v článku 93 ods. 2 nariadenia (EÚ) 2016/679.

8. **ZÁVEREČNÉ ÚVAHY**

(291) Európsky výbor pre ochranu údajov zverejnil svoje stanovisko ([509]), ktoré bolo zohľadnené pri príprave tohto rozhodnutia.

(292) Opatrenia stanovené v tomto rozhodnutí sú v súlade so stanoviskom výboru zriadeného podľa článku 93 nariadenia (EÚ) 2016/679,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

1. Spojené kráľovstvo na účely článku 45 nariadenia (EÚ) 2016/679 zabezpečuje primeranú úroveň ochrany osobných údajov prenášaných v rámci rozsahu pôsobnosti nariadenia (EÚ) 2016/679 z Európskej únie do Spojeného kráľovstva.

2. Toto rozhodnutie sa nevzťahuje na osobné údaje prenášané na účely imigračnej kontroly Spojeného kráľovstva ani na také, ktoré inak patria do rozsahu výnimky určitých práv dotknutých osôb na účely zachovania účinnej imigračnej kontroly podľa bodu 4 ods. 1 prílohy 2 k zákonu o ochrane údajov z roku 2018.

Článok 2

Vždy, keď dozorné príslušné orgány v členských štátoch uplatnia svoje právomoci podľa článku 58 nariadenia (EÚ) 2016/679, aby ochránili fyzické osoby v súvislosti so spracúvaním ich osobných údajov, pokiaľ ide o prenosy údajov patriacich do rozsahu pôsobnosti stanoveného v článku 1, dotknutý členský štát o tejto skutočnosti bezodkladne informuje Komisiu.

Článok 3

1. Komisia nepretržite monitoruje uplatňovanie právneho rámca, z ktorého vychádza toto rozhodnutie, vrátane podmienok, za ktorých sa uskutočňujú následné prenosy, uplatňujú individuálne práva a za ktorých majú orgány verejnej moci Spojeného kráľovstva prístup k údajom preneseným na základe tohto rozhodnutia, s cieľom posúdiť, či Spojené kráľovstvo naďalej zabezpečuje primeranú úroveň ochrany v zmysle článku 1.

2. Členské štáty a Komisia sa vzájomne informujú o prípadoch, v ktorých Komisár pre informácie alebo akýkoľvek iný príslušný orgán Spojeného kráľovstva nezabezpečuje dodržiavanie právneho rámca, na ktorom je založené toto rozhodnutie.

3. Členské štáty a Komisia sa vzájomne informujú o všetkých náznakoch toho, že zásahy orgánov verejnej moci Spojeného kráľovstva do práva fyzických osôb na ochranu ich osobných údajov prekračujú rámec toho, čo je nevyhnutne potrebné, alebo že neexistuje účinná právna ochrana pred takými zásahmi.

4. Ak má Komisia informácie o tom, že primeraná úroveň ochrany už nie je zabezpečená, informuje o tom príslušné orgány Spojeného kráľovstva a môže pozastaviť, zrušiť alebo zmeniť toto rozhodnutie.

([509]) Stanovisko č. 14/2021 k návrhu vykonávacieho rozhodnutia Európskej komisie podľa nariadenia (EÚ) 2016/679 o primeranej ochrane osobných údajov v Spojenom kráľovstve, k dispozícii na tomto odkaze: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

5. Komisia môže pozastaviť, zrušiť alebo zmeniť toto rozhodnutie, ak nedostatočná spolupráca vlády Spojeného kráľovstva bráni Komisii určiť, či je dotknutý záver uvedený v článku 1 ods. 1.

Článok 4

Toto rozhodnutie stráca účinnosť 27. júna 2025, pokiaľ sa nepredĺži v súlade s postupom uvedeným v článku 93 ods. 2 nariadenia (EÚ) 2016/679.

Článok 5

Toto rozhodnutie je určené členským štátom.

V Bruseli 28. júna 2021

Za Komisiu
Didier REYNDERS
člen Komisie