II

(Nelegislativní akty)

ROZHODNUTÍ

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2021/1772

ze dne 28. června 2021

podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající ochraně osobních údajů poskytované Spojeným královstvím

(oznámeno pod číslem C(2021) 4800)

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) ([1]), a zejména na čl. 45 odst. 3 uvedeného nařízení,

vzhledem k těmto důvodům:

1. ÚVOD

(1) Nařízení (EU) 2016/679 stanoví pravidla pro předávání osobních údajů správci nebo zpracovateli v Evropské unii do třetích zemí a mezinárodním organizacím, pokud toto předávání spadá do oblasti působnosti uvedeného nařízení. Pravidla pro mezinárodní předávání údajů stanoví kapitola V uvedeného nařízení, tzn. články 44 až 50. Jakkoli je tok osobních údajů do zemí a ze zemí mimo Evropskou unii nezbytný pro rozšiřování mezinárodní spolupráce a přeshraničního obchodu, úroveň ochrany osobních údajů v Evropské unii nesmí být oslabena předáváním těchto údajů do třetích zemí ([2]).

(2) Podle čl. 45 odst. 3 nařízení (EU) 2016/679 může Komise prostřednictvím prováděcího aktu rozhodnout, že určitá třetí země, určité území či jedno nebo více konkrétních odvětví v určité třetí zemi nebo určitá mezinárodní organizace zajišťuje odpovídající úroveň ochrany. Za této podmínky se může předávání osobních údajů do třetí země bez nutnosti získat další povolení uskutečnit, jak stanoví čl. 45 odst. 1 a 103. bod odůvodnění uvedeného nařízení.

(3) Podle čl. 45 odst. 2 nařízení (EU) 2016/679 musí přijetí rozhodnutí o odpovídající ochraně vycházet z komplexní analýzy právního řádu dané třetí země, a to jak z hlediska pravidel použitelných pro dovozce údajů, tak z hlediska omezení a záruk vztahujících se k přístupu orgánů veřejné moci k osobním údajům. V tomto posouzení musí Komise určit, zda daná třetí země zaručí úroveň ochrany „v zásadě rovnocennou“ úrovni ochrany zajištěné v Evropské unii (104. bod odůvodnění nařízení (EU) 2016/679). Standard, vůči němuž je „zásadní rovnocennost“ posuzována, je stanoven právními předpisy Evropské unie, a to zejména nařízením (EU) 2016/679, jakož i judikaturou Soudního dvora Evropské unie ([3]). V tomto ohledu je významný i referenční rámec Evropského sboru pro ochranu osobních údajů (EDPB) pro odpovídající ochranu ([4]).

([1]) Úř. věst. L 119, 4.5.2016, s. 1.
([2]) Viz 101. bod odůvodnění nařízení (EU) 2016/679.
([3]) Nejnověji viz věc C-311/18, Facebook Ireland a Schrems (dále jen „rozsudek ve věci Schrems II“), ECLI:EU:C:2020:559.
([4]) Evropský sbor pro ochranu osobních údajů, Referenční rámec pro odpovídající ochranu, WP 254 rev. 01, k dispozici na této adrese: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Jak objasnil Soudní dvůr Evropské unie, toto nevyžaduje zjištění stejné úrovně ochrany ([5]). Zejména prostředky, které dotyčná třetí země k ochraně osobních údajů využívá, se mohou lišit od prostředků zavedených v Evropské unii, pokud se v praxi ukážou jako účinné k zajištění odpovídající úrovně ochrany ([6]). Standard odpovídající ochrany tedy nevyžaduje opakování pravidel Unie slovo od slova. Kritériem je spíše to, zda zahraniční systém jako celek zajišťuje prostřednictvím podstaty práv na ochranu údajů a jejich účinného uplatňování, dozoru nad nimi a vymáhání těchto práv požadovanou úroveň ochrany ([7]).

(5) Komise pečlivě analyzovala právo a praxi ve Spojeném království. Na základě zjištění uvedených v (8). až (270). bodě odůvodnění dospěla Komise k závěru, že Spojené království zajišťuje odpovídající úroveň ochrany osobních údajů předávaných v rámci oblasti působnosti nařízení (EU) 2016/679 z Evropské unie do Spojeného království.

(6) Tento závěr se netýká osobních údajů předávaných pro účely kontroly imigrace ve Spojeném království nebo osobních údajů, které jinak spadají do oblasti působnosti výjimky z určitých práv subjektu údajů za účelem zachování účinné kontroly imigrace (dále jen „imigrační výjimka“) podle bodu 4 odst. 1 přílohy 2 britského zákona o ochraně údajů. Platnost a výklad imigrační výjimky podle právních předpisů Spojeného království nejsou v návaznosti na rozhodnutí Odvolacího soudu (Anglie a Wales) ze dne 26. května 2021 ustáleny. Ačkoli odvolací soud uznal, že práva subjektu údajů mohou být v zásadě omezena pro účely kontroly imigrace jako „důležitého aspektu veřejného zájmu“, zároveň konstatoval, že imigrační výjimka je ve své současné podobě neslučitelná s právem Spojeného království, neboť v legislativním opatření chybí konkrétní ustanovení stanovující záruky uvedené v čl. 23 odst. 2 britského obecného nařízení o ochraně údajů (dále jen „britské nařízení GDPR“) ([8]). Za těchto podmínek by měla být předání osobních údajů z Unie do Spojeného království, na která lze použít imigrační výjimku, vyloučena z oblasti působnosti tohoto rozhodnutí ([9]). Jakmile bude odstraněna neslučitelnost s právem Spojeného království, měly by být imigrační výjimka, jakož i potřeba zachovat omezení oblasti působnosti tohoto rozhodnutí znovu posouzeny.

(7) Tímto rozhodnutím by nemělo být dotčeno přímé uplatňování nařízení (EU) 2016/679 na organizace usazené ve Spojeném království, pokud jsou splněny podmínky týkající se místní působnosti uvedeného nařízení, stanovené v jeho článku 3.

2. PRAVIDLA TÝKAJÍCÍ SE ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

2.1 Ústavní rámec

(8) Spojené království je parlamentní demokracií, v níž je hlavou státu konstituční panovník. Stát má svrchovaný parlament nadřazený všem ostatním vládním institucím, vládu jako orgán výkonné moci, který je sestavován z členů parlamentu a tomuto parlamentu je také odpovědný, a nezávislé soudnictví. Vláda odvozuje své oprávnění ze své schopnosti získat důvěru zvolené Dolní sněmovny Spojeného království a zodpovídá se oběma komorám parlamentu Spojeného království, které nesou odpovědnost za kontrolu vlády a za projednávání a přijímání zákonů.

([5]) Věc C-362/14, Schrems (dále jen „rozsudek ve věci Schrems I“), ECLI:EU:C:2015:650, bod 73.

([6]) Rozsudek ve věci Schrems I, bod 74.

([7]) Viz sdělení Komise Evropskému parlamentu a Radě, Výměna a ochrana osobních údajů v globalizovaném světě, COM(2017) 7 ze dne 10.1.2017, oddíl 3.1, s. 6–7, k dispozici na této adrese: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

([8]) Odvolací soud (občanskoprávní oddělení) („Open Rights Group v Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport“, [2021] EWCA Civ 800, body 53 až 56. Odvolací soud zrušil rozhodnutí vrchního soudu, který výjimku dříve posoudil ve světle nařízení (EU) 2016/679 (zejména jeho článku 23) a Listiny základních práv Evropské unie a shledal výjimku zákonnou (Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562).

([9]) Budou-li splněny příslušné podmínky, lze předání pro účely kontroly imigrace ve Spojeném království provádět na základě mechanismů pro předávání údajů stanovených v článcích 46 až 49 nařízení (EU) 2016/679.

(9) V oblasti přijímání právních předpisů týkajících se vnitrostátních záležitostí ve Skotsku, Walesu a Severním Irsku, které nevyhradil sám sobě, přenesl Parlament Spojeného království odpovědnost na Skotský parlament, Velšský parlament (Senedd Cymru) a na Shromáždění Severního Irska. Zatímco ochrana údajů je vyhrazenou oblastí, tj. v celé zemi platí stejné právní předpisy, jiné oblasti politiky významné pro toto rozhodnutí jsou decentralizované. Například systémy trestního soudnictví včetně činnosti policie ve Skotsku a Severním Irsku spadají do odpovědnosti přenesené na Skotský parlament, resp. Shromáždění Severního Irska. Spojené království nemá kodifikovanou ústavu ve smyslu pevně zakotveného ústavního dokumentu. Ústavní principy se vyvíjely postupně, a to zejména na základě judikatury a zvyklostí. Ústavní hodnota některých právních předpisů, jako je Magna Carta (Velká listina práv a svobod), Bill of Rights 1689 (Listina práv z roku 1689) a Human Rights Act 1998 (zákon o lidských právech z roku 1998), byla uznána soudy. Základní práva jednotlivců se jako součást ústavního rámce rozvíjela prostřednictvím zvykového práva (common law), uvedených právních předpisů a mezinárodních smluv, zejména Evropské úmluvy o lidských právech, kterou Spojené království ratifikovalo v roce 1951. Spojené království také v roce 1987 ratifikovalo Úmluvu Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat (úmluva č. 108) ([10]).

(10) Zákon o lidských právech z roku 1998 začleňuje práva obsažená v Evropské úmluvě o lidských právech do práva Spojeného království. Zákon o lidských právech přiznává každému jednotlivci základní práva a svobody stanovené v článcích 2 až 12 a v článku 14 Evropské úmluvy o lidských právech, v článcích 1, 2 a 3 prvního protokolu této úmluvy a v článku 1 jejího třináctého protokolu ve spojení s články 16, 17 a 18 uvedené úmluvy. To zahrnuje právo na respektování soukromého a rodinného života (a právo na ochranu údajů jako součást tohoto práva) a právo na spravedlivý proces ([11]). Zejména, podle článku 8 úmluvy může orgán veřejné moci do práva na soukromí zasahovat pouze v souladu se zákonem, je-li to v demokratické společnosti nezbytné v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a trestné činnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

(11) V souladu se zákonem o lidských právech z roku 1998 musí být jakékoli opatření orgánů veřejné moci slučitelné s právem podle úmluvy ([12]). Kromě toho je třeba primární a podřízené právní předpisy vykládat a uplatňovat způsobem, který je slučitelný s právy podle úmluvy ([13]).

2.2 **Rámec ochrany údajů ve Spojeném království**

(12) Spojené království dne 31. ledna 2020 vystoupilo z Evropské unie. Podle Dohody o vystoupení Spojeného království Velké Británie a Severního Irska z Evropské unie a Evropského společenství pro atomovou energii ([14]) se ve Spojeném království během přechodného období do 31. prosince 2020 nadále používalo právo Unie. Před vystoupením a během přechodného období tvořily legislativní rámec ochrany osobních údajů ve Spojeném království příslušné právní předpisy EU (zejména nařízení Evropského parlamentu a Rady (EU) 2016/679 a směrnice Evropského parlamentu a Rady (EU) 2016/680 ([15])) a vnitrostátní právní předpisy, zejména zákon o ochraně údajů z roku 2018 ([16]), který stanovil vnitrostátní pravidla v případech, které umožňuje nařízení (EU) 2016/679, upřesňoval a omezoval použití pravidel podle nařízení (EU) 2016/679 a prováděl ve vnitrostátním právu směrnici (EU) 2016/680.

([10]) Zásady úmluvy č. 108 byly původně v právu Spojeného království provedeny prostřednictvím zákona o ochraně údajů z roku 1984, který byl nahrazen zákonem o ochraně údajů z roku 1998 a poté zákonem o ochraně údajů z roku 2018 (ve spojení s obecným nařízením o ochraně osobních údajů ve Spojeném království). Spojené království rovněž v roce 2018 podepsalo Protokol o změně úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat (označovaný jako úmluva č. 108+) a v současné době pracuje na ratifikaci úmluvy.

([11]) Články 6 a 8 EÚLP (viz také příloha 1 zákona o lidských právech z roku 1998).

([12]) Článek 6 zákona o lidských právech z roku 1998.

([13]) Článek 3 zákona o lidských právech z roku 1998.

([14]) Dohoda o vystoupení Spojeného království Velké Británie a Severního Irska z Evropské unie a Evropského společenství pro atomovou energii, 2019/C 384 I/01, XT/21054/2019/INIT, (Úř. věst. C 384I, 12.11.2019, s. 1), k dispozici na této adrese: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN

([15]) Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (Úř. věst. L 119, 4.5.2016, s. 89), k dispozici na této adrese: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016L0680&from=EN.

([16]) Zákon o ochraně údajů z roku 2018, k dispozici na této adrese: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

(13) Aby se připravila na vystoupení z Evropské unie, přijala vláda Spojeného království zákon o Evropské unii (o vystoupení z Evropské unie) z roku 2018 ([17]), který začleňuje přímo použitelné právní předpisy Unie do práva Spojeného království ([18]). Tyto tzv. ponechané právní předpisy EU zahrnují nařízení (EU) 2016/679 v jeho plném rozsahu (včetně bodů odůvodnění) ([19]). V souladu s uvedeným zákonem musí soudy Spojeného království vykládat nepozměněné ponechané právní předpisy EU v souladu s příslušnou judikaturou Evropského soudního dvora a s obecnými zásadami práva Unie účinnými bezprostředně před koncem přechodného období (označovanými jako „ponechaná judikatura EU“, resp. „ponechané obecné zásady práva EU“) ([20]).

(14) Podle zákona o Evropské unii (o vystoupení z Evropské unie) z roku 2018 mají ministři Spojeného království pravomoc zavádět prostřednictvím zákonných nástrojů sekundární právní předpisy, aby provedli nutné úpravy ponechaného práva Evropské unie po vystoupení Spojeného království z Evropské unie. V rámci výkonu této pravomoci přijali nařízení v oblasti ochrany údajů, soukromí a elektronických komunikací (změny atd.) (vystoupení z EU) z roku 2019 (dále jen „nařízení v oblasti ochrany údajů, soukromí a elektronických komunikací“) ([21]). Nařízení v oblasti ochrany údajů, soukromí a elektronických komunikací pozměňují nařízení (EU) 2016/679, které do práva Spojeného království začlenil zákon o Evropské unii (o vystoupení z Evropské unie) z roku 2018, zákon o ochraně údajů z roku 2018 a ostatní právní předpisy v oblasti ochrany údajů, aby odpovídaly vnitrostátním souvislostem ([22]).

(15) Právní rámec ochrany osobních údajů ve Spojeném království po skončení přechodného období tedy tvoří:

— britské nařízení GDPR ve znění začleněném do práva Spojeného království podle zákona o Evropské unii (o vystoupení z Evropské unie) z roku 2018 a pozměněném nařízeními v oblasti ochrany údajů, soukromí a elektronických komunikací ([23]) a

— zákon o ochraně údajů z roku 2018 ([24]) ve znění pozměněném nařízeními v oblasti ochrany údajů, soukromí a elektronických komunikací.

(16) Jelikož britské nařízení GDPR vychází z právních předpisů EU, pravidla ochrany údajů ve Spojeném království v mnoha ohledech velmi přesně odrážejí odpovídající pravidla platná v Evropské unii.

(17) Kromě pravomocí, které ministrovi přiznává zákon o Evropské unii (o vystoupení z Evropské unie) z roku 2018, několik ustanovení zákona o ochraně údajů z roku 2018 uděluje ministrovi pravomoc přijímat sekundární právní předpisy, kterými se mění některá ustanovení zákona nebo stanoví doplňková a doplňující pravidla ([25]). Ministr

([17]) European Union (Withdrawal) Act 2018 (zákon o Evropské unii (o vystoupení z Evropské unie) z roku 2018), k dispozici na této adrese: https://www.legislation.gov.uk/ukpga/2018/16/contents

([18]) Záměr a účinek zákona o Evropské unii (o vystoupení z Evropské unie) z roku 2018 je takový, že všechny přímé právní předpisy Unie, které byly ke konci přechodného období začleněny do práva Spojeného království, budou začleněny do práva Spojeného království s účinností, jakou mají v právu EU bezprostředně před koncem přechodného období, viz článek 3 zákona o Evropské unii (o vystoupení z Evropské unie) z roku 2018.

([19]) Vysvětlivky k zákonu o Evropské unii (o vystoupení z Evropské unie) z roku 2018 upřesňují, že: „V případě, že je právní předpis převeden podle tohoto článku, bude součástí vnitrostátních právních předpisů vlastní znění právního předpisu. To bude zahrnovat úplné znění jakéhokoli nástroje EU (včetně jeho bodů odůvodnění)“. (Explanatory Notes to the European Union (Withdrawal) Act 2018 (Vysvětlivky k zákonu o Evropské unii (o vystoupení z Evropské unie) z roku 2018), bod 83, k dispozici na této adrese: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Podle informací, které poskytly orgány Spojeného království, vzhledem k tomu, že body odůvodnění nemají status závazných právních pravidel, nebylo nutné je pozměnit takovým způsobem, jakým byly články nařízení (EU) 2016/679 pozměněny nařízeními v oblasti ochrany údajů, soukromí a elektronických komunikací.

([20]) Článek 6 zákona o Evropské unii (o vystoupení z Evropské unie) z roku 2018.

([21]) Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (nařízení v oblasti ochrany údajů, soukromí a elektronických komunikací (změny atd.) (vystoupení z EU) z roku 2019), k dispozici na této adrese: https://www.legislation.gov.uk/uksi/2019/419/contents/made, ve znění nařízení v oblasti ochrany údajů, soukromí a elektronických komunikací z roku 2020, k dispozici na této adrese: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([22]) Tyto změny britského obecného nařízení o ochraně osobních údajů a zákona o ochraně údajů z roku 2018 jsou převážně technické povahy, například výmaz odkazů na „členské státy“ nebo úpravy terminologie, například náhrada odkazů na nařízení (EU) 2016/679 odkazy na britské obecné nařízení o ochraně osobních údajů. V některých případech byly zapotřebí změny, které zohlední čistě vnitrostátní souvislosti ustanovení, například pokud jde o to, „kdo“ přijímá „nařízení o odpovídající ochraně“ pro účely britského legislativního rámce ochrany údajů (viz článek 17A zákona o ochraně údajů z roku 2018), tj. ministr, nikoli Evropská komise.

([23]) General Data Protection Regulation, Keeling Schedule (Obecné nařízení o ochraně osobních údajů, informativní text se zvýrazněním změn nařízení), k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([24]) Data Protection Act 2018, Keeling Schedule (Zákon o ochraně údajů z roku 2018, informativní text se zvýrazněním změn zákona), k dispozici na této adrese: 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]) Tyto pravomoci jsou obsaženy například v článku 16 (pravomoc ve zvláštních, úzce vymezených situacích stanovit další výjimky z konkrétních ustanovení britského nařízení GDPR), článku 17A (pravomoc přijímat nařízení o odpovídající ochraně), článcích 212 a 213 (pravomoci stanovit vstup právních předpisů v platnost a účinnost a přijímat přechodná ustanovení) a v článku 211 (pravomoc provádět drobné a následné změny) zákona o ochraně údajů z roku 2018.

dosud vykonával pouze pravomoc podle článku 137 zákona o ochraně údajů z roku 2018, a to přijmout nařízení o ochraně údajů (poplatky a informace) (změna) z roku 2019, které stanoví okolnosti, za nichž jsou správci údajů povinni platit roční poplatek nezávislému úřadu pro ochranu osobních údajů ve Spojeném království, tedy komisaři pro informace.

(18) A v neposlední řadě jsou další pokyny k právním předpisům Spojeného království v oblasti ochrany údajů uvedeny v kodexech zásad a dalších pokynech přijatých komisařem pro informace. Ačkoli tyto pokyny nejsou formálně právně závazné, mají svou váhu z hlediska výkladu a ukazují, jak se právní předpisy o ochraně údajů používají a jak je komisař v praxi vymáhá. Zejména články 121 až 125 zákona o ochraně údajů z roku 2018 vyžadují, aby komisař vypracoval kodexy postupů pro sdílení údajů, přímý marketing, design odpovídající věku a pro ochranu údajů a žurnalistiku.

(19) Právní rámec Spojeného království, který se použije na údaje předávané podle tohoto rozhodnutí, je tedy z hlediska své struktury a hlavních prvků velmi podobný právnímu rámci, který se používá v Evropské unii. Zahrnuje to skutečnost, že takový rámec se neopírá pouze o povinnosti stanovené ve vnitrostátním právu, které byly formovány právem EU, ale také o povinnosti zakotvené v mezinárodním právu, zejména prostřednictvím dodržování EÚLP a úmluvy č. 108 a podrobení se pravomoci Evropského soudu pro lidská práva ze strany Spojeného království. Tyto povinnosti vyplývají z právně závazných mezinárodních nástrojů, zejména pokud jde o ochranu osobních údajů, a jsou proto obzvláště důležitým prvkem právního rámce posuzovaného v tomto rozhodnutí.

2.3 **Časová a územní působnost**

(20) Obdobně jako nařízení (EU) 2016/679 se i britské nařízení GDPR použije na zcela nebo částečně automatizované zpracování osobních údajů nebo na jiné zpracování osobních údajů, pokud jsou obsažena v evidenci ([26]). Definice „osobních údajů“, „subjektu údajů“ a „zpracování“ v britském nařízení GDPR jsou totožné s definicemi v nařízení (EU) 2016/679 ([27]). Kromě toho se britské nařízení GDPR použije na zpracování ručně zpracovávaných nestrukturovaných osobních údajů ([28]) v držení určitých orgánů veřejné moci Spojeného království ([29]), ačkoli články 24 a 25 zákona o ochraně údajů z roku 2018 ruší použití zásad a práv podle britského nařízení GDPR, které nejsou pro takové osobní údaje použitelné. Podobně, jako je stanoveno v nařízení (EU) 2016/679, se britské nařízení GDPR nepoužije na zpracování osobních údajů prováděné fyzickou osobou v průběhu výlučně osobních či domácích činností ([30]).

(21) Britské nařízení GDPR rozšiřuje svou působnost také na zpracování v průběhu činnosti, která bezprostředně před koncem přechodného období nespadala do oblasti působnosti práva Evropské unie (např. národní bezpečnost) ([31]) nebo spadala do oblasti působnosti hlavy V kapitoly 2 Smlouvy o Evropské unii (činnosti v oblasti společné zahraniční a bezpečnostní politiky) ([32]). Stejně jako v systému Evropské unie se britské nařízení GDPR nepoužije na zpracování osobních údajů příslušným orgánem za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a předcházení těmto hrozbám (tzv. „účely prosazování práva“) (taková zpracování namísto toho upravuje část 3 zákona o ochraně údajů z roku

([26]) Ustanovení čl. 2 odst. 1 a 5 britského nařízení GDPR.

([27]) Ustanovení čl. 4 odst. 1 a 2 britského nařízení GDPR.

([28]) Ruční nestrukturované zpracování osobních údajů je vymezeno v čl. 2 odst. 5 písm. b) jako zpracování osobních údajů, které není automatizovaným nebo strukturovaným zpracováním osobních údajů.

([29]) Ustanovení čl. 2 odst. 1A britského nařízení GDPR stanoví, že nařízení se použije i na ruční nestrukturované zpracování osobních údajů v držení orgánu veřejné moci podle zákona o svobodě informací. Odkaz na orgány veřejné moci podle zákona o svobodě informací znamená jakékoli orgány veřejné moci vymezené v zákoně o svobodě informací z roku 2000 nebo jakékoli skotské orgány veřejné moci vymezené v zákoně o svobodě informací (Skotsko) z roku 2002 (zákon Skotského parlamentu 13). Ustanovení čl. 21 odst. 5 zákona o ochraně údajů z roku 2018.

([30]) Ustanovení čl. 2 odst. 2 písm. a) britského nařízení GDPR.

([31]) Činnosti v oblasti národní bezpečnosti jsou do oblasti působnosti britského nařízení GDPR zahrnuty pouze za předpokladu, že nejsou prováděny příslušným orgánem pro účely prosazování práva, v takovém případě se použije část 3 zákona o ochraně údajů z roku 2018, nebo zpravodajskou službou či v zastoupení zpravodajské služby, jejíž činnosti jsou vyňaty z oblasti působnosti britského nařízení GDPR a řídí se částí 4 zákona o ochraně údajů z roku 2018 podle čl. 2 odst. 2 písm. c) britského nařízení GDPR. Například policejní orgán může provádět bezpečnostní kontroly zaměstnance s cílem zajistit, že zaměstnanci lze svěřit přístup k materiálům týkajícím se národní bezpečnosti. Přestože policie je příslušným orgánem pro účely prosazování práva, dotčené zpracování není prováděno pro účely prosazování práva a použilo by se britské nařízení GDPR. Viz britský dokument Explanatory Framework for Adequacy Discussions (Vysvětlující rámec pro diskuse o odpovídající ochraně), oddíl H: Ochrana údajů týkajících se národní bezpečnosti a rámec vyšetřovacích pravomocí, s. 8, k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf

([32]) Ustanovení čl. 2 odst. 1 písm. a) a b) britského nařízení GDPR.

2018 podobně jako směrnice (EU) 2016/680 podle práva Evropské unie) nebo na zpracování osobních údajů zpravodajskými službami (Security Service (Bezpečnostní služba), Secret Intelligence Service (Tajná zpravodajská služba) a Government Communications Headquarters (Vládní ředitelství pro komunikace)), které upravuje část 4 zákona o ochraně údajů z roku 2018 ([33]).

(22) Územní působnost britského nařízení GDPR je popsána v článku 3 britského nařízení GDPR ([34]) a zahrnuje zpracování osobních údajů v souvislosti s činnostmi provozovny správce nebo zpracovatele ve Spojeném království (bez ohledu na to, kde zpracování probíhá), jakož i zpracování osobních údajů subjektů údajů, které se nacházejí ve Spojeném království, pokud činnosti zpracování souvisejí s nabídkou zboží nebo služeb těmto subjektům údajů nebo s monitorováním jejich chování ([35]). To odráží přístup uplatněný v článku 3 nařízení (EU) 2016/679.

2.4 **Definice osobních údajů a pojmy správce a zpracovatele**

(23) Definice osobních údajů, zpracování, správce, zpracovatele, jakož i definice pseudonymizace stanovené v nařízení (EU) 2016/679 jsou v britském nařízení GDPR ([36]) zachovány bez podstatných úprav. V čl. 9 odst. 1 britského nařízení GDPR jsou navíc stejným způsobem jako v nařízení (EU) 2016/679 definovány zvláštní kategorie údajů („osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby“). Článek 205 zákona o ochraně údajů z roku 2018 uvádí definici „biometrických údajů“ ([37]), „údajů o zdravotním stavu“ ([38]) a „genetických údajů“ ([39]).

2.5 **Záruky, práva a povinnosti**

2.5.1 *Zákonnost a korektnost zpracování*

(24) Osobní údaje by měly být zpracovávány zákonným a korektním způsobem.

(25) Zásady zákonnosti, korektnosti a transparentnosti a důvody pro zákonné zpracování jsou v právu Spojeného království zaručeny prostřednictvím čl. 5 odst. 1 písm. a) a čl. 6 odst. 1 britského nařízení GDPR, které jsou totožné s odpovídajícími ustanoveními nařízení (EU) 2016/679 ([40]). Článek 8 zákona o ochraně údajů z roku 2018 doplňuje čl. 6 odst. 1 písm. e) tím, že stanoví, že zpracování osobních údajů podle čl. 6 odst. 1 písm. e) britského nařízení GDPR (nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci správce),

([33]) Ustanovení čl. 2 odst. 2 písm. b) a c) britského nařízení GDPR.

([34]) Tatáž územní působnost platí pro zpracování osobních údajů podle části 2 zákona o ochraně údajů z roku 2018, který doplňuje britské nařízení GDPR (článek 207 odst. 1A).

([35]) To zejména znamená, že zákon o ochraně údajů z roku 2018, a proto i toto rozhodnutí, se nepoužije na závislá území Britské koruny (Jersey, Guernsey a Ostrov Man) a zámořská území Spojeného království, například Falklandské ostrovy a území Gibraltaru.

([36]) Ustanovení čl. 4 odst. 1, 2, 5, 7 a 8 britského nařízení GDPR.

([37]) „Biometrickými údaji“ se rozumí osobní údaje vyplývající z konkrétního technického zpracování, které se týkají fyzických či fyziologických znaků nebo znaků chování jednotlivce a umožňují nebo potvrzují jeho jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje.

([38]) „Údaji o zdravotním stavu“ se rozumí osobní údaje týkající se tělesného nebo duševního zdraví jednotlivce, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jeho zdravotním stavu.

([39]) „Genetickými údaji“ se rozumí osobní údaje týkající se zděděných nebo získaných genetických znaků jednotlivce, které poskytují jedinečné informace o jeho fyziologii či zdraví, a které vyplývají zejména z analýzy biologického vzorku dotčeného jednotlivce.

([40]) Podle čl. 6 odst. 1 britského nařízení GDPR je zpracování zákonné pouze tehdy a do té míry, pokud: a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů; b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů; c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje; d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby; e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, nebo f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

zahrnuje zpracování osobních údajů, které je nezbytné pro výkon spravedlnosti, výkon funkce kterékoli komory parlamentu Spojeného království, výkon funkce svěřené osobě na základě právního předpisu nebo v rámci právního státu, výkon funkce Koruny, ministra Koruny nebo vládního ministerstva nebo činnost, která podporuje nebo prosazuje demokratickou angažovanost.

(26) Pokud jde o souhlas (jeden z důvodů pro zákonné zpracování), britské nařízení GDPR také beze změny zachovává podmínky stanovené v článku 7 nařízení (EU) 2016/679, to znamená, že správce musí být schopen prokázat, že subjekt údajů udělil souhlas, písemná žádost o vyjádření souhlasu musí být předložena jasně a srozumitelně, subjekt údajů musí mít právo svůj souhlas kdykoli odvolat a při posuzování toho, zda je souhlas svobodný, musí být zohledněna skutečnost, zda je plnění smlouvy podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné. Podle článku 8 britského nařízení GDPR je navíc v souvislosti s poskytováním služeb informační společnosti souhlas dítěte zákonný pouze v případě, že je dítě ve věku nejméně 13 let. To splňuje věkové rozmezí stanovené v článku 8 nařízení (EU) 2016/679.

2.5.2 *Zpracování zvláštních kategorií osobních údajů*

(27) Pokud se zpracovávají „zvláštní kategorie“ údajů, měly by existovat zvláštní záruky.

(28) Britské nařízení GDPR a zákon o ochraně údajů z roku 2018 obsahují konkrétní pravidla týkající se zpracování zvláštních kategorií osobních údajů, které jsou v čl. 9 odst. 1 britského nařízení GDPR definovány stejným způsobem jako v nařízení (EU) 2016/679 (viz 23. bod odůvodnění výše). Podle článku 9 britského nařízení GDPR je zpracování zvláštních kategorií údajů v zásadě zakázáno, pokud se nepoužije zvláštní výjimka.

(29) Tyto výjimky (vyjmenované v čl. 9 odst. 2 a 3 britského nařízení GDPR) neznamenají žádné podstatné změny oproti čl. 9 odst. 2 a 3 nařízení (EU) 2016/679. Pokud subjekt údajů neudělil výslovný souhlas se zpracováním těchto osobních údajů, je zpracování zvláštních kategorií osobních údajů povoleno pouze za konkrétních a omezených okolností. Zpracování citlivých údajů musí být ve většině případů nezbytné pro konkrétní účel vymezený v příslušném ustanovení (viz čl. 9 odst. 2 písm. b), c), f), g), h), i) a j)).

(30) Kromě toho, pokud výjimka podle čl. 9 odst. 2 britského nařízení GDPR vyžaduje zmocnění ze zákona nebo odkazuje na veřejný zájem, článek 10 zákona o ochraně údajů z roku 2018 společně s přílohou 1 tohoto zákona blíže specifikuje podmínky, které musí být splněny, aby bylo možné výjimek využít. Například v případě zpracování citlivých údajů za účelem ochrany „veřejného zdraví“ (čl. 9 odst. 2 písm. i) britského nařízení GDPR) ustanovení čl. 3 písm. b) části 1 přílohy 1 vyžaduje, aby kromě splnění testu nezbytnosti bylo takové zpracování prováděno „zdravotnickým pracovníkem nebo na jeho odpovědnost“ nebo „jinou osobou, která je vázána povinností mlčenlivosti na základě právního předpisu nebo v rámci právního státu“, a to včetně řádně zavedené povinnosti mlčenlivosti podle zvykového práva.

(31) Pokud jsou citlivé údaje zpracovávány z důvodu významného veřejného zájmu (čl. 9 odst. 2 písm. g) britského nařízení GDPR), část 2 přílohy 1 zákona o ochraně údajů z roku 2018 uvádí úplný seznam účelů, které lze považovat za podstatný veřejný zájem, a pro každý z těchto účelů stanoví zvláštní dodatečné podmínky. Za významný veřejný zájem je například považováno prosazování rasové a etnické rozmanitosti na vyšších úrovních struktury organizací. Zpracování citlivých údajů pro tento zvláštní účel podléhá podrobným požadavkům, včetně toho, že je prováděno v rámci postupu identifikace osob vhodných k zastávání vyšších funkcí, je nezbytné k prosazování rasové a etnické rozmanitosti a není pravděpodobné, že by subjektu údajů způsobilo podstatnou újmu nebo tíseň.

(32) Ustanovení čl. 11 odst. 1 zákona o ochraně údajů z roku 2018 stanoví podmínky pro zpracování osobních údajů za okolností popsaných v čl. 9 odst. 3 britského nařízení GDPR v souvislosti s povinností mlčenlivosti. To zahrnuje situace, kdy je zpracování prováděno zdravotnickým nebo sociálním pracovníkem nebo na jeho odpovědnost nebo jinou osobou, která je za daných okolností vázána povinností mlčenlivosti ze zákona nebo v rámci právního státu.

(33) Kromě toho použití mnoha výjimek vyjmenovaných v čl. 9 odst. 2 britského nařízení GDPR vyžaduje zvláštní a vhodné záruky. V závislosti na povaze zpracování a míře rizika z hlediska práv a svobod subjektů údajů stanoví podmínky zpracování uvedené v příloze 1 zákona o ochraně údajů z roku 2018 různé záruky. Příloha 1 pak stanoví podmínky pro každou situaci zpracování.

(34) V některých případech zákon o ochraně údajů z roku 2018 upravuje a omezuje druh citlivých údajů, které lze zpracovávat pro účely dodržení konkrétního právního základu. Například článek 8 přílohy 1 povoluje zpracování citlivých údajů za účelem prosazování rovnosti příležitostí nebo zacházení. Tuto podmínku zpracování lze použít pouze v případě, že údaje vypovídají o rasovém či etnickém původu, náboženském vyznání či filozofickém přesvědčení, sexuální orientaci nebo se jedná o údaje o zdravotním stavu.

(35) V některých případech zákon o ochraně údajů z roku 2018 omezuje druh správce údajů, který může podmínky zpracování využít. Například článek 23 přílohy 1 upravuje zpracování citlivých údajů v souvislosti s odpověďmi volených zástupců veřejnosti. Tuto podmínku zpracování lze použít pouze v případě, že správcem je volený zástupce nebo správce jedná z jeho pověření.

(36) V některých jiných případech zákon o ochraně údajů z roku 2018 pro možnost použití podmínky zpracování stanoví meze kategorií subjektu údajů. Například článek 21 příloha 1 reguluje zpracování citlivých údajů pro systémy zaměstnaneckého penzijního pojištění. Tuto podmínku lze použít pouze v případě, že dotyčným subjektem údajů je sourozenec, rodič, prarodič nebo praprarodič účastníka systému.

(37) Při využití výjimek podle čl. 9 odst. 2 britského nařízení GDPR, které jsou dále upřesněny v článku 10 zákona o ochraně údajů z roku 2018 a jeho příloze 1, je správce ve většině případů povinen vypracovat „dokument o vhodné politice“. Ten musí vymezovat postupy správce pro zajištění souladu se zásadami uvedenými v článku 5 britského nařízení GDPR. Musí také stanovit koncepce pro uchovávání a výmaz uvedením pravděpodobné doby uchovávání. Správci musí tento dokument podle potřeby revidovat a aktualizovat. Správce musí koncepční dokument uchovávat po dobu šesti měsíců po dokončení zpracování a na požádání jej musí zpřístupnit komisaři pro informace ([41]).

(38) Podle článku 41 přílohy 1 zákona o ochraně údajů z roku 2018 musí být ke koncepčnímu dokumentu vždy přiložen rozšířený záznam o zpracování. Tento záznam musí sledovat závazky obsažené v koncepčním dokumentu, tj. zda jsou údaje mazány nebo uchovávány v souladu s koncepcí. Pokud koncepce není dodržena, musí protokol zaznamenat příslušné důvody. Záznam musí také popisovat, jak zpracování splňuje článek 6 britského nařízení GDPR (zákonnost zpracování) a uplatněnou zvláštní podmínku v příloze 1 zákona o ochraně údajů z roku 2018.

(39) A v neposlední řadě britské nařízení GDPR stejně jako nařízení (EU) 2016/679 poskytuje obecné záruky pro určité operace zpracování zvláštních kategorií údajů. Článek 35 britského nařízení GDPR vyžaduje posouzení vlivu na ochranu osobních údajů, pokud jsou zvláštní kategorie údajů zpracovávány ve velkém rozsahu. Podle článku 37 britského nařízení GDPR musí správce nebo zpracovatel jmenovat pověřence pro ochranu osobních údajů, pokud jeho hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií údajů.

(40) Pokud jde o osobní údaje týkající se rozsudků v trestních věcech a trestných činů, článek 10 britského nařízení GDPR je totožný s článkem 10 nařízení (EU) 2016/679. Povoluje zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů pouze pod dozorem orgánu veřejné moci nebo jestliže je oprávněné podle vnitrostátního práva poskytujícího vhodné záruky, pokud jde o práva a svobody subjektů údajů.

(41) Pokud zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů neprobíhá pod dozorem orgánu veřejné moci, čl. 10 odst. 5 zákona o ochraně údajů z roku 2018 stanoví, že toto zpracování může probíhat pouze pro konkrétní účely / v konkrétních situacích stanovených v částech 1, 2 a 3 přílohy 1 zákona o ochraně údajů z roku 2018 a podléhá zvláštním požadavkům, které jsou stanoveny pro každý z těchto účelů / každou z těchto situací. Například údaje týkající se rozsudků v trestních věcech mohou zpracovávat neziskové subjekty, pokud a) zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a b) za podmínky i) že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a ii) že tyto osobní údaje nejsou bez souhlasu subjektů údajů zpřístupňovány mimo tento subjekt.

([41]) Články 38–40 přílohy 1 zákona o ochraně údajů z roku 2018.

(42) Kromě toho část 3 přílohy 1 zákona o ochraně údajů z roku 2018 vymezuje další okolnosti, za nichž lze použít údaje týkající se rozsudků v trestních věcech, které odpovídají právním důvodům pro zpracování citlivých údajů podle čl. 9 odst. 2 nařízení (EU) 2016/679 a britského nařízení GDPR (např. souhlas subjektu údajů, životně důležité zájmy jednotlivce, pokud subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas, pokud již subjekt údajů údaje zjevně zveřejnil, pokud je zpracování nezbytné pro určení, výkon nebo obhajobu právního nároku atd.).

2.5.3 *Účelové omezení, přesnost, minimalizace údajů, omezení uložení a zabezpečení údajů*

(43) Osobní údaje by měly být zpracovávány za konkrétním účelem a následně používány, pouze pokud to není neslučitelné s účelem zpracování.

(44) Tuto zásadu stanoví čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679 a beze změn ji zachovává čl. 5 odst. 1 písm. b) britského nařízení GDPR. Podmínky dalšího slučitelného zpracování podle čl. 6 odst. 4 nařízení (EU) 2016/679 jsou rovněž bez podstatných úprav zachovány v čl. 6 odst. 4 písm. a) až e) britského nařízení GDPR.

(45) Údaje by navíc měly být přesné a v případě potřeby aktualizované. Měly by být také přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelům, pro které jsou zpracovávány, a v zásadě by se neměly uchovávat déle, než je nezbytné pro účely, k nimž jsou dané osobní údaje zpracovávány.

(46) Tyto zásady minimalizace údajů, přesnosti a omezení uložení vymezuje čl. 5 odst. 1 písm. c) až e) nařízení (EU) 2016/679 a beze změn je zachovává čl. 5 odst. 1 písm. c) až e) britského nařízení GDPR.

(47) Osobní údaje by také měly být zpracovávány způsobem, který zajišťuje jejich zabezpečení, včetně ochrany před neoprávněným nebo protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Za tímto účelem by podnikatelské subjekty měly přijmout vhodná technická nebo organizační opatření na ochranu osobních údajů před možnými hrozbami. Tato opatření by měla být posuzována s přihlédnutím ke stavu techniky a k souvisejícím nákladům.

(48) Zabezpečení údajů je v právu Spojeného království zakotveno prostřednictvím zásady celistvosti a důvěrnosti v čl. 5 odst. 1 písm. f) britského nařízení GDPR a v článku 32 britského nařízení GDPR, který se týká zabezpečení zpracování. Tato ustanovení jsou totožná s příslušnými ustanoveními nařízení (EU) 2016/679. Navíc britské nařízení GDPR vyžaduje za stejných podmínek, jaké jsou stanoveny v článcích 33 a 34 nařízení (EU) 2016/679, ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu (článek 33 britského nařízení GDPR) a oznamování případů porušení zabezpečení osobních údajů subjektu údajů (článek 34 britského nařízení GDPR).

2.5.4 *Transparentnost*

(49) Subjekty údajů by měly být informovány o hlavních znacích zpracování jejich osobních údajů.

(50) To zajišťují články 13 a 14 britského nařízení GDPR, které kromě obecné zásady transparentnosti stanoví pravidla týkající se informací, které mají být poskytovány subjektu údajů ([42]). Britské nařízení GDPR nezavádí žádné podstatné úpravy těchto pravidel ve srovnání s odpovídajícími články nařízení (EU) 2016/679. Stejně jako v nařízení (EU) 2016/679 však požadavky těchto článků týkající se transparentnosti podléhají několika výjimkám stanoveným v zákoně o ochraně údajů z roku 2018 (viz 55. až 72. bod odůvodnění).

([42]) V čl. 13 odst. 1 písm. f) a čl. 14 odst. 1 písm. f) jsou odkazy na rozhodnutí Komise o odpovídající ochraně nahrazeny odkazy na rovnocenný nástroj Spojeného království, tj. nařízení o odpovídající ochraně podle zákona o ochraně údajů z roku 2018. Kromě toho byly odkazy na právo EU nebo členského státu v čl. 14 odst. 5 písm. c) až d) nahrazeny odkazem na vnitrostátní právo (jako příklady takových vnitrostátních právních předpisů, které mohou spadat do oblasti působnosti čl. 14 odst. 5 písm. c), Spojené království uvedlo článek 7 zákona o subjektech obchodujících se železným šrotem z roku 2013, který stanoví pravidla pro registraci povolení týkajících se železného šrotu, nebo část 35 zákona o společnostech z roku 2006, která stanoví pravidla týkající se úředníka vedoucího obchodní rejstřík. Obdobně by k příkladům vnitrostátních právních předpisů, které mohou spadat do oblasti působnosti čl. 14 odst. 5 písm. d), mohly patřit právní předpisy, které stanoví pravidla profesní mlčenlivosti, nebo povinnosti, které zohledňují pracovní smlouvy, nebo povinnost mlčenlivosti podle zvykového práva (například osobní údaje zpracovávané pracovníky v oblasti zdravotnictví, lidských zdrojů, sociálními pracovníky atd.).

2.5.5 *Individuální práva*

(51) Subjekty údajů by měly mít určitá práva, která lze vůči správci nebo zpracovateli vymáhat, zejména právo na přístup k údajům, právo vznést námitku proti zpracování a právo na opravu a výmaz údajů. Tato práva mohou zároveň podléhat omezením, pokud jsou tato omezení nezbytná a přiměřená k zajištění veřejné bezpečnosti nebo jiných důležitých cílů obecného veřejného zájmu.

2.5.5.1 Hmotná práva

(52) Britské nařízení GDPR uděluje jednotlivcům stejná vymahatelná práva jako nařízení (EU) 2016/679. Ustanovení, z nichž vyplývají práva jednotlivců, jsou v britském nařízení GDPR zachována bez podstatných změn.

(53) Tato práva zahrnují právo subjektu údajů na přístup k osobním údajům (článek 15 britského nařízení GDPR), právo na opravu (článek 16 britského nařízení GDPR), právo na výmaz (článek 17 britského nařízení GDPR), právo na omezení zpracování (článek 18 britského nařízení GDPR), oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování (článek 19 britského nařízení GDPR), právo na přenositelnost údajů (článek 20 britského nařízení GDPR) a právo vznést námitku (článek 21 britského nařízení GDPR) ([43]). Poslední zmíněný článek obsahuje i právo subjektu údajů vznést námitku vůči zpracování osobních údajů pro účely přímého marketingu, které stanoví čl. 21 odst. 2 a 3 nařízení (EU) 2016/679. Podle článku 122 zákona o ochraně údajů z roku 2018 musí komisař pro informace vypracovat kodex zásad týkající se provádění přímého marketingu v souladu s požadavky právních předpisů v oblasti ochrany údajů (a nařízení o ochraně soukromí a elektronických komunikacích (směrnice ES) z roku 2003) a další pokyny k podpoře správné praxe v oblasti přímého marketingu, které bude komisař považovat za vhodné. Úřad komisaře pro informace v současné době připravuje kodex přímého marketingu ([44]).

(54) Právo subjektu údajů nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, které má pro subjekt údajů právní účinky nebo se ho obdobným způsobem významně dotýká, jak je stanoveno v článku 22 obecného nařízení o ochraně osobních údajů, je bez podstatných změn zachováno i v britském nařízení GDPR. Byl však doplněn nový odstavec 3A, který uvádí, že článek 14 zákona o ochraně údajů z roku 2018 stanoví záruky pro práva, svobody a oprávněné zájmy subjektů údajů, pokud je zpracování prováděno podle čl. 22 odst. 2 písm. b) britského nařízení GDPR. Toto ustanovení platí pouze v případě, že základem takového rozhodnutí je povolení nebo požadavek podle práva Spojeného království, a nepoužije se v případech, kdy je rozhodnutí nezbytné na základě smlouvy nebo je učiněno s výslovným souhlasem subjektu údajů. Použije-li se článek 14 zákona o ochraně údajů z roku 2018, musí správce, jakmile je to přiměřeně proveditelné, písemně oznámit subjektu údajů, že bylo přijato rozhodnutí založené výhradně na automatizovaném zpracování. Subjekt údajů má právo požadovat, aby správce (do jednoho měsíce od obdržení oznámení) rozhodnutí znovu zvážil nebo aby přijal nové rozhodnutí, které nebude založeno výhradně na automatizovaném zpracování. Ministr je zmocněn přijmout další ochranná opatření, pokud jde o automatizované rozhodování. Tato pravomoc dosud nebyla využita.

2.5.5.2 Omezení individuálních práv a jiná ustanovení

(55) Zákon o ochraně údajů z roku 2018 stanoví několik omezení individuálních práv, která odpovídají rámci článku 23 britského nařízení GDPR. V tomto rámci nejsou zavedena žádná omezení týkající se práva vznést námitku vůči přímému marketingu podle čl. 21 odst. 2 a 3 britského nařízení GDPR nebo práva nebýt předmětem automatizovaného rozhodování podle článku 22 britského nařízení GDPR.

(56) Omezení jsou upřesněna v přílohách 2–4 zákona o ochraně údajů z roku 2018. Orgány Spojeného království vysvětlily, že se řídí dvěma zásadami: zásadou specifičnosti (uplatnění podrobného přístupu, rozdělení obecných omezení na více specifičtějších ustanovení) a zásadou podmíněnosti (každé ustanovení je doplněno zárukami v podobě omezení nebo podmínek zabraňujících zneužívání) ([45]).

([43]) V čl. 17 odst. 1 písm. e) a čl. 17 odst. 3 písm. b) byly odkazy na právo EU nebo členského státu nahrazeny odkazem na vnitrostátní právní předpisy (jako příklady takových vnitrostátních právních předpisů podle čl. 17 odst. 1 písm. e) Spojené království uvedlo nařízení o vzdělávání (informace o žácích) (Anglie) z roku 2006, které vyžaduje, aby byla jména žáků vymazána ze školních rejstříků poté, co žáci školu opustí, nebo článek 34F zákona o lékařské péči z roku 1983, který stanoví pravidla pro výmaz jmen z rejstříku praktických lékařů a rejstříků odborných lékařů.

([44]) Návrh kodexu zásad je k dispozici na této adrese: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf

([45]) Britský vysvětlující rámec pro diskuse o odpovídající ochraně, oddíl E: Omezení, s. 1, k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf

(57) Omezení popsaná v čl. 23 odst. 1 britského nařízení GDPR jsou formulována tak, aby bylo zajištěno jejich použití pouze za vymezených okolností, jsou-li v demokratické společnosti nutná, a jsou přiměřená sledovanému legitimnímu cíli. V souladu s ustálenou judikaturou týkající se výkladu omezení lze výjimku z režimu ochrany údajů použít v každém konkrétním případě pouze tehdy, je-li to nezbytné a přiměřené ([46]). Test nezbytnosti musí být „přísný a musí vyžadovat, aby jakýkoli zásah do práv subjektu údajů byl úměrný závažnosti ohrožení veřejného zájmu. Zahrnuje proto klasickou analýzu proporcionality“ ([47]).

(58) Cíle sledované těmito omezeními odpovídají cílům uvedeným v článku 23 nařízení (EU) 2016/679, s výjimkou omezení týkajících se národní bezpečnosti a obrany, která jsou upravena v článku 26 zákona o ochraně údajů z roku 2018, ale podléhají stejným požadavkům na nezbytnost a přiměřenost (viz 63. až 66. bod odůvodnění).

(59) Některá omezení, například ta, která se týkají prevence nebo odhalování trestné činnosti, zadržování nebo trestního stíhání pachatelů a vyměřování nebo výběru daní či cel ([48]), umožňují omezení veškerých individuálních práv a povinností transparentnosti (vyjma práv podle čl. 21 odst. 2 a článku 22). Rozsah dalších omezení se omezuje na povinnosti transparentnosti a práva na přístup, například omezení týkající se povinnosti mlčenlivosti advokáta ([49]), práva na osvobození od požadavku poskytovat informace k vlastnímu neprospěchu ([50]) a financování společností, zejména prevence obchodování zasvěcených osob ([51]). Malý počet omezení umožňuje omezit povinnost správce oznámit subjektu údajů porušení zabezpečení údajů a zásady účelového omezení a zákonnosti, korektnosti a transparentnosti zpracování ([52]).

(60) Některá omezení se na určitý druh zpracování osobních údajů vztahují automaticky „v plném rozsahu“ (uplatnění povinností transparentnosti a individuálních práv je například vyloučeno při zpracování osobních údajů za účelem posouzení vhodnosti osoby pro soudní funkci nebo pro zpracování údajů soudem, tribunálem nebo jednotlivcem, který jedná v rámci soudních pravomocí).

(61) Ve většině případů však příslušný bod přílohy 2 zákona o ochraně údajů z roku 2018 stanoví, že omezení se použije pouze tehdy (a do té míry), pokud by použití ustanovení „pravděpodobně bylo na újmu“ sledovaného legitimního cíle tohoto omezení: například uvedená ustanovení britského nařízení GDPR se nepoužijí na osobní údaje zpracovávané za účelem prevence nebo odhalování trestné činnosti, zadržení nebo trestního stíhání pachatelů nebo vyměření či výběru daní nebo cel „v rozsahu, v jakém by použití těchto ustanovení pravděpodobně bylo na újmu“ kterékoli z uvedených záležitostí ([53]).

(62) Standardní formulaci „by pravděpodobně bylo na újmu“ soudy ve Spojeném království důsledně vykládají ve smyslu „velmi významné a závažné možnosti újmy na určených veřejných zájmech“ ([54]). Omezení, které podléhá testu újmy, se tedy lze dovolávat pouze v případě, že existuje velmi významná a závažná možnost, že by přiznání určitého práva ohrozilo dotčený veřejný zájem, a to v rozsahu, v jakém uvedená možnost existuje. Správce je povinen v každém jednotlivém případě posoudit, zda jsou tyto podmínky splněny ([55]).

(63) Vedle omezení uvedených v příloze 2 zákona o ochraně údajů z roku 2018 stanoví článek 26 zákona o ochraně údajů z roku 2018 výjimku, kterou lze použít u určitých ustanovení britského nařízení GDPR a zákona o ochraně údajů z roku 2018, je-li tato výjimka nutná pro účely ochrany národní bezpečnosti nebo pro účely obrany. Tato výjimka se použije na zásady ochrany údajů (vyjma zásady zákonnosti), povinnosti transparentnosti, práva subjektu údajů, povinnost oznámit porušení zabezpečení údajů, pravidla pro mezinárodní předávání, některé povinnosti

([46]) Věc Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin), body 40 a 41.
([47]) Věc Guriev v Community Safety Development (United Kingdom) Ltd [2016] EWHC 643 (QB), bod 43. V tomto ohledu viz také věc Lin v Commissioner of Police for the Metropolis [2015] EWHC 2484 (QB), bod 80.
([48]) Bod 2 přílohy 2 zákona o ochraně údajů z roku 2018.
([49]) Bod 19 přílohy 2 zákona o ochraně údajů z roku 2018.
([50]) Bod 20 přílohy 2 zákona o ochraně údajů z roku 2018.
([51]) Bod 21 přílohy 2 zákona o ochraně údajů z roku 2018.
([52]) Například omezení práva oznámení případu porušení zabezpečení údajů jsou povolena pouze v souvislosti s trestnou činností a zdaněním (bod 2 přílohy 2 zákona o ochraně údajů z roku 2018), parlamentními výsadami (bod 13 přílohy 2 zákona o ochraně údajů z roku 2018) a zpracování údajů pro novinářské, akademické, umělecké a literární účely (bod 26 přílohy 2 zákona o ochraně údajů z roku 2018).
([53]) Bod 2 přílohy 2 zákona o ochraně údajů z roku 2018.
([54]) Věc R (Lord) v Secretary of State for the Home Department [2003] EWHC 2073 (Admin), bod 100 a Guriev v Community Safety Development (United Kingdom) Ltd [2016] EWHC 643 (QB), bod 43.
([55]) Věc Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor, bod 31.

a pravomoci komisaře pro informace a pravidla o právní ochraně, odpovědnosti a sankcích, s výjimkou ustanovení o obecných podmínkách pro ukládání správních pokut stanovených v článku 83 britského GDPR a ustanovení o sankcích v článku 84 britského nařízení GDPR. Ustanovení článku 28 zákona o ochraně údajů z roku 2018 navíc upravuje použití čl. 9 odst. 1 tak, aby umožnil zpracování zvláštních kategorií údajů podle čl. 9 odst. 1 britského nařízení GDPR, pokud je zpracování prováděno z důvodu ochrany národní bezpečnosti nebo pro účely obrany, a to s příslušnými zárukami týkajícími se práv a svobod subjektů údajů ([56]).

(64) Výjimku lze použít pouze v případě, že je to nezbytné k zajištění národní bezpečnosti nebo obrany. Stejně jako v případě ostatních výjimek stanovených zákonem o ochraně údajů z roku 2018 musí správce údajů výjimku posoudit a použít případ od případu. Jakékoli použití výjimky musí být navíc v souladu se standardy lidských práv (podle zákona o lidských právech z roku 1998), podle nichž by jakýkoli zásah do práv na soukromí měl být v demokratické společnosti nezbytný a přiměřený ([57]).

(65) Tento výklad výjimky potvrzuje Úřad komisaře pro informace, který vydal podrobné pokyny k používání výjimky z důvodu národní bezpečnosti a obrany a objasnil, že správce musí výjimku posoudit a použít případ od případu ([58]). Pokyny zejména zdůrazňují, že „[n]ejde o plošnou výjimku“ a že pro její použití „nestačí, aby byly údaje zpracovávány pro účely národní bezpečnosti“. Správce, který výjimku využívá, musí naopak „prokázat, že existuje reálná možnost nepříznivého dopadu na národní bezpečnost“, a v případě potřeby se od něj očekává, že „poskytne [Úřadu komisaře pro informace] důkazy o důvodech, proč tuto výjimku použil“. Pokyny obsahují kontrolní seznam a řadu příkladů k dalšímu objasnění podmínek, za nichž se lze této výjimky dovolávat.

(66) Skutečnost, že jsou údaje zpracovávány pro účely národní bezpečnosti nebo obrany, proto sama o sobě pro použití výjimky nestačí. Správce musí posoudit, jaké by byly skutečné důsledky pro národní bezpečnost, pokud by musel dodržet konkrétní ustanovení o ochraně údajů. Výjimku lze použít pouze na ta konkrétní ustanovení, u nichž bylo zjištěno, že představují riziko, a musí být uplatňována v co nejomezenější míře ([59]).

(67) Tento přístup potvrdil Tribunál pro informace ([60]). Ve věci Baker v Secretary of State for the Home Department (dále jen „rozsudek ve věci Baker v Secretary of State“) dospěl k závěru, že bylo nezákonné použít výjimku z důvodu národní bezpečnosti jako plošnou výjimku pro přístup k žádostem přijatým zpravodajskými službami. Namísto toho bylo nutné používat výjimku individuálně, na základě posouzení každé žádosti z hlediska její podstaty a s ohledem na právo jednotlivců na respektování jejich soukromého života ([61]).

([56]) Podle informací poskytnutých orgány Spojeného království, pokud zpracování probíhá v kontextu národní bezpečnosti, budou správci obvykle uplatňovat posílené rozšířené záruky a ochranná opatření, které odrážejí citlivou povahu zpracování. Vhodnost konkrétních záruk bude záviset na rizicích, která představuje prováděné zpracování. Mohly by zahrnovat omezení přístupu k údajům, při němž budou mít k údajům přístup pouze oprávněné osoby s příslušnou bezpečnostní prověrkou, přísná omezení týkající se sdílení údajů a vysoký standard zabezpečení uplatňovaný na postupy uchovávání a manipulace.

([57]) Viz také věc Guriev v Community Safety Development (United Kingdom) Ltd [2016] EWHC 643 (QB), bod 45; Věc Lin v Commissioner of the Police for the Metropolis [2015] EWHC 2484 (QB), bod 80.

([58]) Viz pokyny Úřadu komisaře pro informace k výjimce z důvodu národní bezpečnosti a obrany, k dispozici na adrese: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/

([59]) Podle příkladu, který uvedly orgány Spojeného království, pokud by osoba podezřelá z terorismu, která je předmětem aktivního vyšetřování službou MI5, podala u Ministerstva vnitra žádost o přístup (například proto, že je účastníkem sporu s Ministerstvem vnitra ohledně imigračních záležitostí), bylo by nezbytné chránit před zpřístupněním subjektu údajů veškeré údaje, které služba MI5 případně sdílela s Ministerstvem vnitra v souvislosti s probíhajícím vyšetřováním a které by mohly způsobit újmu, pokud jde o citlivé zdroje, metody nebo techniky a/nebo vést ke zvýšení hrozby, kterou daná osoba představuje. Za takových okolností je pravděpodobné, že by byla splněna prahová hranice pro uplatnění výjimky podle článku 26 a výjimka ze zveřejnění informací by byla vyžadována pro zajištění národní bezpečnosti. Pokud by však Ministerstvo vnitra o dané osobě uchovávalo také osobní údaje, které se netýkají vyšetřování služby MI5, a tyto informace by mohly být poskytnuty bez rizika narušení národní bezpečnosti, pak by se výjimka z důvodu národní bezpečnosti při zvažování zpřístupnění údajů dané osobě nepoužila. Úřad komisaře pro informace v současné době připravuje pokyny, jak by měli správci přistupovat k použití výjimky podle článku 26. Pokyny by měl být zveřejněny do konce března 2021.

([60]) Tribunál pro informace byl zřízen k projednávání opravných prostředků týkajících se ochrany údajů podle zákona o ochraně osobních údajů z roku 1984. V roce 2010 se Tribunál pro informace stal v rámci reformy struktury britského systému tribunálů součástí Všeobecné regulační komory Tribunálu prvního stupně.

([61]) Viz rozsudek ve věci Baker v Secretary of State for the Home Department [2001] UKIT NSA2 (dále jen „rozsudek ve věci Baker v Secretary of State“).

2.5.6 *Omezení týkající se osobních údajů zpracovávaných pro novinářské, umělecké, akademické a literární účely, jakož i pro archivaci a výzkum*

(68) Ustanovení čl. 85 odst. 2 britského nařízení GDPR umožňuje přijmout ustanovení o vynětí osobních údajů zpracovávaných pro novinářské, umělecké, akademické a literární účely z působnosti několika ustanovení britského nařízení GDPR. Výjimky pro zpracování za uvedenými účely uvádí část 5 přílohy 2 zákona o ochraně údajů z roku 2018. Stanoví výjimky ze zásad ochrany údajů (vyjma zásady integrity a důvěrnosti), právní důvody zpracování (včetně zvláštních kategorií údajů a údajů týkajících se rozsudků v trestních věcech atd.), podmínky souhlasu, povinnosti transparentnosti, práva subjektů údajů, povinnost oznamovat případy porušení zabezpečení údajů, požadavek konzultovat s komisařem pro informace před vysoce rizikovým zpracováním a pravidla pro mezinárodní předávání údajů ([62]). V tomto ohledu se britské nařízení GDPR významně neodchyluje od nařízení (EU) 2016/679, které ve svém článku 85 rovněž stanoví možnost vyjmout zpracování prováděné pro novinářské účely a pro účely akademického, uměleckého či literárního projevu z řady požadavků nařízení (EU) 2016/679. Ustanovení zákona o ochraně údajů z roku 2018, jmenovitě části 5 přílohy 2, jsou slučitelná s britským nařízením GDPR.

(69) Základní vyvažování, které má být provedeno podle článku 85 britského nařízení GDPR, se týká toho, zda je výjimka z pravidel ochrany údajů uvedená v 68. bodě odůvodnění „nutná k uvedení práva na ochranu osobních údajů do souladu se svobodou projevu a informací“ ([63]). Podle bodu 26 odst. 2 a 3 přílohy 2 zákona o ochraně údajů z roku 2018 Spojené království za účelem dosažení této vyváženosti uplatňuje test „důvodné domněnky“. Aby byla výjimka odůvodněná, musí se správce důvodně domnívat, i) že zveřejnění je ve veřejném zájmu a ii) že použití příslušného ustanovení nařízení GDPR by bylo neslučitelné s novinářskými, akademickými, uměleckými nebo literárními účely. Jak potvrzuje judikatura ([64]), test „důvodné domněnky“ obsahuje subjektivní i objektivní prvek: nestačí, aby správce prokázal, že byl sám přesvědčen, že dodržet ustanovení je neslučitelné s výše uvedenými účely. Jeho domněnka musí být důvodná, tj. taková, aby o ní mohla být přesvědčena rozumná osoba obeznámená s relevantními skutečnostmi. Správce proto musí při formování své domněnky postupovat s náležitou péčí, aby mohl prokázat její důvodnost. Podle vysvětlení poskytnutých orgány Spojeného království musí být test „důvodné domněnky“ uplatněn u každé jednotlivé výjimky ([65]). Jsou-li podmínky splněny, považuje se výjimka podle právních předpisů Spojeného království za nezbytnou a přiměřenou.

(70) Podle článku 124 zákona o ochraně údajů z roku 2018 musí Úřad komisaře pro informace vypracovat kodex zásad v oblasti ochrany údajů a žurnalistiky. Práce na tomto kodexu pokračují. V této záležitosti byly vydány pokyny podle zákona o ochraně údajů z roku 1998, které zejména zdůrazňují, že k využití této výjimky

([62]) Viz článek 85 britského nařízení GDPR a bod 26 odst. 9 části 5 přílohy 2 zákona o ochraně údajů z roku 2018.

([63]) V souladu s bodem 26 odst. 2 části 5 přílohy 2 zákona o ochraně údajů z roku 2018 se výjimka vztahuje na zpracování osobních údajů prováděné pro zvláštní účely (novinářské účely, akademické účely, umělecké účely a literární účely), pokud je zpracování prováděno za tím účelem, aby určitá osoba zveřejnila novinářský, akademický, umělecký nebo literární materiál, a pokud se správce důvodně domnívá, že by zveřejnění tohoto materiálu bylo ve veřejném zájmu. Při určování toho, zda by zveřejnění bylo ve veřejném zájmu, musí správce zohlednit zvláštní význam veřejného zájmu z hlediska svobody projevu a informací. Správce musí navíc přihlédnout ke kodexům zásad nebo pokynům týkajícím se daného zveřejnění (Redakční pokyny BBC, Kodex vysílání OFCOM a Kodex zásad pro vydavatele). Aby mohla výjimka platit, musí se také správce důvodně domnívat, že dodržení příslušného ustanovení by bylo neslučitelné se zvláštními účely (bod 26 odst. 3 přílohy 2 zákona o ochraně údajů z roku 2018).

([64]) Rozsudek ve věci NT1 v. Google [2018] EWHC 799 (QB) se v bodě 102 zabýval diskusí o tom, zda měl správce údajů důvodnou domněnku, že zveřejnění je ve veřejném zájmu a že dodržení příslušných ustanovení je neslučitelné se zvláštními účely. Soud uvedl, že čl. 32 odst. 1 písm. b) a c) zákona o ochraně osobních údajů z roku 1998 obsahuje subjektivní a objektivní prvek: správce údajů musí prokázat, že se domníval, že zveřejnění bude ve veřejném zájmu a že tato domněnka byla objektivně důvodná; musí prokázat subjektivní domněnku, že dodržení ustanovení, z něhož požaduje výjimku, by bylo neslučitelné s dotčeným zvláštním účelem.

([65]) Příklad použití testu „důvodné domněnky“ je obsažen v rozhodnutí Úřadu komisaře pro informace uložit pokutu společnosti True Visions Productions, které bylo učiněno na základě zákona o ochraně osobních údajů z roku 1998. Úřad komisaře pro informace připustil, že správce údajů v daném sdělovacím prostředku se subjektivně domníval, že dodržení první zásady ochrany údajů (korektnost a zákonnost) je neslučitelné s novinářskými účely. Nepřistoupil však na to, že tato domněnka byla objektivně důvodná. Rozhodnutí Úřadu komisaře pro informace je k dispozici na této adrese: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf

nestačí pouze konstatovat, že dodržení ustanovení by pro novinářskou činnost znamenalo komplikace, ale musí existovat jasný argument, že dotčené ustanovení představuje překážku odpovědné žurnalistiky ([66]). Pokyny k uplatnění testu veřejného zájmu a vyvážení veřejného zájmu vůči zájmu jednotlivce na ochraně soukromí publikovaly i britský regulační úřad pro telekomunikace OFCOM a společnost BBC ve svých redakčních pokynech ([67]). Tyto pokyny zejména uvádějí příklady informací, které lze považovat za informace ve veřejném zájmu, a vysvětlují nutnost schopnosti prokázat, že veřejný zájem za konkrétních okolností daného případu převažuje nad právy na soukromí.

(71) Po vzoru ustanovení článku 89 nařízení GDPR mohou být z řady vyjmenovaných ustanovení britského nařízení GDPR vyňaty i osobní údaje zpracovávané pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely ([68]). Pokud jde o výzkum a statistiku, jsou možné výjimky z ustanovení britského nařízení GDPR týkající se potvrzení zpracování, přístupu k údajům a záruk za předání do třetích zemí; práva na opravu; omezení zpracování a námitky vůči zpracování. Pokud jde o archivaci ve veřejném zájmu, jsou možné výjimky také z oznamovací povinnosti ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování a z práva na přenositelnost údajů.

(72) Podle bodu 27 odst. 1 a bodu 28 odst. 1 přílohy 2 zákona o ochraně údajů z roku 2018 jsou výjimky z vyjmenovaných ustanovení britského nařízení GDPR možné, pokud by použití ustanovení „znemožnilo nebo vážně narušilo splnění“ dotčených účelů ([69]).

(73) Vzhledem k jejich významu pro účinný výkon práv jednotlivce bude jakýkoli relevantní vývoj týkající se výkladu a používání výše uvedených výjimek v praxi (kromě výjimky týkající se zachování účinné kontroly imigrace, jak je vysvětlena v 6. bodě odůvodnění) včetně případného dalšího vývoje judikatury a pokynů Úřadu komisaře pro informace a donucovacích opatření, náležitě zohledněn v rámci nepřetržitého sledování tohoto rozhodnutí ([70]).

2.5.7 *Omezení dalšího předávání*

(74) Úroveň ochrany osobních údajů předávaných z Evropské unie správcům nebo zpracovatelům ve Spojeném království nesmí být oslabena dalším předáváním těchto údajů příjemcům ve třetí zemi. Taková „další předání“, která z pohledu správce nebo zpracovatele ve Spojeném království představují mezinárodní předání ze Spojeného království, by měla být povolena pouze tehdy, pokud další příjemce mimo Spojené království sám podléhá pravidlům, která zajišťují úroveň ochrany obdobnou té, která je zaručena v právním řádu Spojeného království. Z tohoto důvodu je použití pravidel britského nařízení GDPR a zákona o ochraně údajů z roku 2018 pro mezinárodní předávání osobních údajů důležitým faktorem k zajištění kontinuity ochrany v případě osobních údajů předávaných z Evropské unie do Spojeného království podle tohoto rozhodnutí.

([66]) Podle pokynů musí být organizace schopny prokázat, proč je dodržení příslušného ustanovení zákona o ochraně údajů z roku 1998 neslučitelné s novinářskými účely. Správci musí zejména vyvážit nepříznivý dopad, který by dodržení ustanovení mělo na žurnalistiku, a nepříznivý dopad, který by nedodržení ustanovení mělo na práva subjektu údajů. Pokud může novinář přiměřeně dosáhnout svých redakčních cílů způsobem, který je v souladu se standardními ustanoveními zákona o ochraně údajů, musí tak učinit. Organizace musí být schopny odůvodnit použití omezení ve vztahu ke každému ustanovení, které nedodržely. „Ochrana údajů a žurnalistika: příručka pro sdělovací prostředky“, k dispozici na této adrese: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf

([67]) K příkladům veřejného zájmu patří odhalování nebo zjišťování trestné činnosti, ochrana veřejného zdraví nebo bezpečnosti, odhalování zavádějících tvrzení jednotlivců nebo organizací nebo zveřejňování nekompetentnosti, která má dopad na veřejnost. Viz pokyny úřadu OFCOM, k dispozici na této adrese: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf a Redakční pokyny BBC, k dispozici na této adrese: https://www.bbc.com/editorialguidelines/guidelines/privacy

([68]) Viz článek 89 britského nařízení GDPR a bod 27 odst. 2 a bod 28 odst. 2 části 6 přílohy 2 zákona o ochraně údajů z roku 2018.

([69]) S výhradou požadavku, aby byly osobní údaje zpracovávány v souladu s čl. 89 odst. 1 britského nařízení GDPR doplněným článkem 19 zákona o ochraně údajů z roku 2018.

([70]) Viz (281). až (287). bod odůvodnění.

(75) Režim mezinárodního předávání osobních údajů ze Spojeného království je stanoven v článcích 44–49 britského nařízení GDPR doplněných zákonem o ochraně údajů z roku 2018 a je v podstatě totožný s pravidly stanovenými v kapitole V nařízení (EU) 2016/679 ([71]). Předávání osobních údajů do třetí země nebo mezinárodní organizaci může probíhat pouze na základě nařízení o odpovídající ochraně (britský ekvivalent rozhodnutí o odpovídající ochraně podle nařízení (EU) 2016/679), nebo pokud nařízení o odpovídající ochraně neexistuje, jestliže správce nebo zpracovatel poskytl vhodné záruky v souladu s článkem 46 britského nařízení GDPR. Pokud nařízení o odpovídající ochraně nebo vhodné záruky neexistují, lze předání provést pouze na základě výjimek stanovených v článku 49 britského nařízení GDPR.

(76) Nařízení o odpovídající ochraně vydaná ministrem mohou stanovit, že určitá třetí země (nebo území nebo odvětví ve třetí zemi), mezinárodní organizace nebo postavení ([72]) takové země, území, odvětví nebo organizace zajišťuje odpovídající úroveň ochrany osobních údajů. Při posuzování odpovídající úrovně ochrany musí ministr zohlednit naprosto tytéž aspekty, jaké má posoudit Komise podle čl. 45 odst. 2 písm. a) až c) nařízení (EU) 2016/679 vykládaného společně se 104. bodem odůvodnění nařízení (EU) 2016/679 a ponechanou judikaturou EU. To znamená, že při posuzování odpovídající úrovně ochrany ve třetí zemi bude příslušným standardem to, zda dotyčná třetí země zajišťuje úroveň ochrany „v zásadě rovnocennou“ úrovni ochrany zajištěné ve Spojeném království.

(77) Pokud jde o postup, na nařízení o odpovídající ochraně se vztahují „obecné“ procedurální náležitosti stanovené v článku 182 zákona o ochraně údajů z roku 2018. V rámci tohoto postupu musí ministr při navrhování přijetí britských nařízení o odpovídající ochraně Spojeného království konzultovat komisaře pro informace ([73]). Jakmile ministr nařízení přijme, jsou předložena parlamentu Spojeného království a podléhají postupu „zamítavého rozhodnutí“, v němž mohou obě komory parlamentu tato nařízení přezkoumat a podat návrh na zrušení těchto nařízení ve lhůtě 40 dnů ([74]).

(78) Podle čl. 17B odst. 1 zákona o ochraně údajů z roku 2018 musí být nařízení o odpovídající ochraně přezkoumávána v nejvýše čtyřletých intervalech a ministr musí průběžně sledovat vývoj ve třetích zemích a mezinárodních organizacích, který by mohl ovlivnit rozhodnutí vydat nařízení o odpovídající ochraně nebo tato nařízení pozměnit či zrušit. Pokud ministr zjistí, že určitá země nebo organizace již nezajišťuje odpovídající úroveň ochrany osobních údajů, musí v nezbytném rozsahu nařízení změnit nebo zrušit a zahájit konzultace s dotčenou třetí zemí nebo mezinárodní organizací ohledně nápravy nedostatečné úrovně ochrany. Tyto procedurální aspekty jsou rovněž odrazem odpovídajících požadavků nařízení (EU) 2016/679.

([71]) S výjimkou článku 48 nařízení (EU) 2016/679, který se Spojené království rozhodlo do britského nařízení GDPR nezařadit. V tomto ohledu je třeba v první řadě připomenout, že standard, který má být považován za standard, jenž poskytuje odpovídající úroveň ochrany, je standardem „zásadní rovnocennosti“, nikoli totožnosti, jak objasnil Soudní dvůr Evropské unie (rozsudek ve věci Schrems I, body 73–74) a uznal Evropský sbor pro ochranu osobních údajů (Referenční rámec pro odpovídající ochranu, s. 3). Jak Evropský sbor pro ochranu osobních údajů vysvětlil ve svém referenčním rámci, „[c]ílem tedy není kopírovat legislativu EU krok za krokem, nýbrž stanovit podstatu – klíčové požadavky této legislativy“. V tomto ohledu je důležité upozornit, že jakkoli právní řád Spojeného království formálně neobsahuje ustanovení totožné s článkem 48, zaručují stejný účinek jiná právní ustanovení a zásady, tj. při odpovědi na žádost o osobní údaje ze strany soudu nebo správního orgánu ve třetí zemi lze osobní údaje do této třetí země předat pouze v případě, že existuje mezinárodní dohoda (na jejímž základě jsou dotčený rozsudek soudu dané třetí země nebo správní rozhodnutí z třetí země uznávány nebo vymáhány ve Spojeném království) nebo je-li předání založeno na jednom z mechanismů předávání údajů stanovených v kapitole V britského nařízení GDPR. Konkrétněji, aby bylo možné vykonat zahraniční soudní rozhodnutí, musí mít soudy ve Spojeném království možnost poukázat na zvykové právo nebo na právní předpis, který umožňuje vykonatelnost tohoto soudního rozhodnutí. Avšak ani obecné právo (viz Adams and Others v Cape Industries Plc., [1990] 2 W.L.R. 657), ani právní předpisy nestanoví možnost výkonu zahraničních soudních rozhodnutí vyžadujících předání údajů bez existence mezinárodní dohody. V důsledku toho, pokud taková mezinárodní dohoda neexistuje, jsou žádosti o údaje podle právních předpisů Spojeného království nevymahatelné. Kromě toho jakékoli předání osobních údajů do třetích zemí (a to i na žádost zahraničního soudu nebo správního orgánu) podléhá omezením stanoveným v kapitole V britského nařízení GDPR, která jsou totožná s odpovídajícími ustanoveními nařízení (EU) 2016/679, a proto se musí opírat o jeden z důvodů pro předání, které jsou k dispozici podle kapitoly V, a to za zvláštních podmínek, kterým předání podle uvedené kapitoly podléhá.

([72]) Orgány Spojeného království vysvětlily, že postavení země nebo mezinárodní organizace odkazuje na situaci, kdy by bylo nutné provést konkrétní a částečné určení odpovídající ochrany s příslušnými omezeními (například v případě nařízení o odpovídající ochraně týkajících se pouze určitých druhů předávání údajů).

([73]) Viz memorandum o porozumění mezi ministrem pro digitální oblast, kulturu, sdělovací prostředky a Úřadem komisaře pro informace o úloze Úřadu komisaře pro informace ve vztahu k novému posouzení odpovídající ochrany ve Spojeném království, k dispozici na adrese: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([74]) Je-li takové usnesení odhlasováno, nařízení ztratí jakýkoli další právní účinek.

(79) Pokud neexistují nařízení o odpovídající ochraně, lze mezinárodní předání provést, pokud správce nebo zpracovatel poskytl vhodné záruky v souladu s článkem 46 britského nařízení GDPR. Tyto záruky jsou obdobné jako záruky podle článku 46 nařízení (EU) 2016/679. Zahrnují právně závazné a vymahatelné nástroje mezi orgány veřejné moci nebo veřejnými subjekty, závazná podniková pravidla ([75]), standardní doložky o ochraně údajů, schválené kodexy chování, schválené mechanismy pro vydání osvědčení a se souhlasem komisaře pro informace smluvní doložky mezi správci (nebo zpracovateli) nebo správní ujednání mezi orgány veřejné moci. Pravidla však byla z procesního hlediska upravena tak, aby fungovala v rámci Spojeného království, zejména standardní doložky o ochraně údajů může přijmout ministr (článek 17C) nebo komisař pro informace (článek 119A) v souladu se zákonem o ochraně údajů z roku 2018.

(80) Pokud neexistuje rozhodnutí o odpovídající ochraně nebo vhodné záruky, lze předání provést pouze na základě výjimek stanovených v článku 49 britského nařízení GDPR ([76]). Britské nařízení GDPR nezavádí žádné podstatné změny těchto pravidel ve srovnání s odpovídajícími pravidly nařízení (EU) 2016/679. Podle britského nařízení GDPR lze stejně jako podle nařízení (EU) 2016/679 některé výjimky využít pouze za předpokladu, že předání je příležitostné ([77]). Kromě toho Úřad komisaře pro informace ve svých pokynech k mezinárodním předáním vysvětluje: „Měli byste je používat pouze jako skutečné „výjimky" z obecného pravidla, podle kterého byste neměli provádět omezená předání, pokud se na ně nevztahuje rozhodnutí o odpovídající ochraně nebo pokud neexistují vhodné záruky" ([78]). Pokud jde o předání, která jsou nezbytná z důležitých důvodů veřejného zájmu (čl. 49 odst. 1 písm. d), může ministr vydat nařízení, která stanoví okolnosti, za nichž předání osobních údajů do třetí země nebo mezinárodní organizaci z důležitých důvodů veřejného zájmu není nezbytné. Kromě toho může ministr nařízeními předání určité kategorie osobních údajů do třetí země nebo mezinárodní organizaci omezit, pokud k předání nemůže dojít na základě nařízení o odpovídající ochraně a ministr považuje toto omezení za nezbytné z důležitých důvodů veřejného zájmu. Žádná taková nařízení dosud nebyla přijata.

(81) Tento rámec pro mezinárodní předání se stal použitelným na konci přechodného období ([79]). Bod 4 přílohy 21 zákona o ochraně údajů z roku 2018 (zavedený nařízeními v oblasti ochrany údajů a soukromí) však stanoví, že ke konci přechodného období se k určitým předáním osobních údajů přistupuje tak, jako by se opírala o nařízení o odpovídající ochraně. Tato předání zahrnují předání do státu EHP, na území Gibraltaru, do orgánu, instituce, úřadu nebo agentury Unie zřízených Smlouvou o EU nebo na základě Smlouvy o EU a do třetích zemí, na které se na konci tohoto období vztahuje unijní rozhodnutí o odpovídající ochraně. V důsledku toho mohou předávání do těchto zemí pokračovat stejně jako před vystoupením Spojeného království z EU. Po skončení přechodného období musí ministr ve lhůtě čtyř let, tedy do konce prosince 2024,

([75]) Britské nařízení GDPR zachovává pravidla podle článku 47 nařízení (EU) 2016/679, s výhradou změn pouze za účelem přizpůsobení pravidel vnitrostátním souvislostem, například náhradou odkazů na příslušný dozorový úřad odkazy na komisaře pro informace, zrušením odkazů na mechanismus jednotnosti v odstavci 1 a zrušením celého odstavce 3.

([76]) Podle článku 49 britského nařízení GDPR jsou předání údajů možná, je-li splněna jedna z těchto podmínek: a) daný subjekt údajů byl informován o možných rizicích, která pro něj v důsledku absence rozhodnutí o odpovídající ochraně a vhodných záruk vyplývají, a následně k navrhovanému předání vydal svůj výslovný souhlas; b) předání je nezbytné pro splnění smlouvy mezi subjektem údajů a správcem nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost subjektu údajů; c) předání je nezbytné pro uzavření nebo splnění smlouvy, která byla uzavřena v zájmu subjektu údajů mezi správcem a jinou fyzickou nebo právnickou osobou; d) předání je nezbytné z důležitých důvodů veřejného zájmu; e) předání je nezbytné pro určení, výkon nebo obhajobu právních nároků; f) předání je nezbytné k ochraně životně důležitých zájmů subjektu údajů nebo jiných osob v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit svůj souhlas; g) k předání dochází z rejstříku, který je na základě vnitrostátního práva určen pro informování veřejnosti a je přístupný k nahlížení veřejnosti obecně nebo jakékoli osobě, která může prokázat oprávněný zájem, avšak pouze pokud jsou v daném případě splněny podmínky pro nahlížení stanovené vnitrostátním právem. Kromě toho, nelze-li použít žádnou z výše uvedených podmínek, může k předání dojít pouze tehdy, pokud tento převod není opakovaný, týká se pouze omezeného počtu subjektů údajů, je nezbytný pro účely závažných oprávněných zájmů správce, které nejsou převáženy zájmy nebo právy a svobodami subjektu údajů, a pokud správce posoudil všechny okolnosti daného předání údajů a na základě tohoto posouzení poskytl vhodné záruky pro ochranu osobních údajů.

([77]) 111. bod odůvodnění britského nařízení GDPR uvádí, že k předáním souvisejícím se smlouvou nebo právním nárokem může dojít pouze v případě, že jsou příležitostná.

([78]) Pokyny Úřadu komisaře pro informace k mezinárodním předáním – k dispozici na této adrese: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7

([79]) Ve lhůtě nejvýše šesti měsíců, která skončí dne 30. června 2021, musí být použitelnost tohoto nového rámce vykládána ve smyslu článku 782 Dohody o obchodu a spolupráci mezi Evropskou unií a Evropským společenstvím pro atomovou energii na jedné straně a Spojeným královstvím Velké Británie a Severního Irska na straně druhé (L 444/14 ze dne 31.12.2020) (dále jen „dohoda o obchodu a spolupráci mezi EU a Spojeným královstvím"), k dispozici na této adrese: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN

provést přezkum těchto zjištění o odpovídající úrovni ochrany. Podle vysvětlení, které poskytly orgány Spojeného království, ačkoli ministr musí tento přezkum provést do konce prosince 2024, přechodná ustanovení neobsahují ustanovení o „skončení platnosti“ a příslušná přechodná ustanovení automaticky nepřestanou být účinná, pokud přezkum nebude do konce prosince 2024 dokončen.

(82) A konečně, pokud jde o budoucí vývoj režimu mezinárodního předávání osobních údajů ve Spojeném království (prostřednictvím přijetí nových předpisů o odpovídající ochraně, uzavření mezinárodních dohod nebo zřízení jiných mechanismů předávání), Komise bude situaci pozorně sledovat a posoudí, zda jsou jednotlivé mechanismy předávání osobních údajů používány způsobem, který zajišťuje kontinuitu ochrany, a v případě potřeby přijme vhodná opatření k řešení možných nepříznivých dopadů na tuto kontinuitu (viz 278. až 287. bod odůvodnění). Jelikož EU a Spojené království mají pro mezinárodní předávání osobních údajů podobná pravidla, předpokládá se, že problémovým rozdílům by se dalo předcházet také prostřednictvím spolupráce, výměny informací a sdílení zkušeností, a to i mezi Úřadem komisaře pro informace a Evropským sborem pro ochranu osobních údajů.

2.5.8 *Odpovědnost*

(83) Podle zásady odpovědnosti se od subjektů zpracovávajících údaje vyžaduje zavedení vhodných technických a organizačních opatření, aby mohly účinně plnit své povinnosti v oblasti ochrany údajů a jejich plnění byly schopny prokázat, zejména příslušnému dozorovému úřadu.

(84) Zásada odpovědnosti stanovená v nařízení (EU) 2016/679 je v čl. 5 odst. 2 britského nařízení GDPR zachována bez podstatných změn a totéž platí pro článek 24 o odpovědnosti správce, článek 25 o záměrné a standardní ochraně osobních údajů a článek 30 o záznamech o činnostech zpracování. Rovněž jsou zachovány články 35 a 36 o posouzení vlivu na ochranu osobních údajů a předchozích konzultacích s dozorovým úřadem. Články 37 až 39 nařízení (EU) 2016/679 o jmenování a úkolech pověřenců pro ochranu osobních údajů jsou v britském GDPR zachovány bez podstatných změn. Kromě toho jsou v britském nařízení GDPR zachována ustanovení článků 40 a 42 nařízení (EU) 2016/679 o kodexech chování a vydávání osvědčení ([80]).

2.6 **Dohled a vymáhání**

2.6.1 *Nezávislý dohled*

(85) Aby se zajistilo, že odpovídající úroveň ochrany údajů je zaručena v praxi, měl by být zřízen nezávislý dozorový úřad oprávněný monitorovat a vymáhat dodržování pravidel v oblasti ochrany údajů. Při plnění svých povinností a výkonu své pravomoci by tento úřad měl jednat zcela nezávisle a nestranně.

(86) Ve Spojeném království provádí dohled a vymáhání v souvislosti s dodržováním britského nařízení GDPR a zákona o ochraně údajů z roku 2018 komisař pro informace. Komisař pro informace je tzv. výhradní korporace: samostatná právnická osoba, kterou tvoří jedna osoba. Komisaři pro informace je při práci nápomocen úřad. Ke dni 31. března 2020 měl Úřad komisaře pro informace 768 stálých zaměstnanců ([81]). Sponzorským ministerstvem komisaře pro informace je ministerstvo pro digitální oblast, kulturu, sdělovací prostředky a sport ([82]).

(87) Nezávislost komisaře je výslovně stanovena v článku 52 britského nařízení GDPR, který podstatným způsobem nemění čl. 52 odst. 1 až 3 nařízení GDPR. Komisař musí při plnění svých úkolů a výkonu svých pravomocí podle britského nařízení GDPR jednat zcela nezávisle, nesmí podléhat vnějšímu vlivu, ať již přímému, nebo nepřímému,

([80]) Dle potřeby jsou tyto odkazy nahrazeny odkazy na orgány Spojeného království. Například podle článku 17 zákona o ochraně údajů z roku 2018 může komisař pro informace nebo vnitrostátní akreditační orgán udělit osobě, která splňuje požadavky stanovené v článku 43 britského nařízení GDPR, akreditaci k monitorování souladu s osvědčením.

([81]) Výroční zpráva a účetní závěrka komisaře pro informace za období 2019–2020, k dispozici na této adrese: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf

([82]) Vztah mezi těmito dvěma subjekty je upraven dohodou o řízení. Mezi hlavní povinnosti ministerstva pro digitální oblast, kulturu, sdělovací prostředky a sport jakožto sponzorského ministerstva patří zejména: zajistit, aby bylo komisaři pro informace poskytnuto odpovídající financování a zdroje; zastupovat zájmy komisaře pro informace před parlamentem Spojeného království a ostatními ministerstvy; zajistit, aby existoval silný vnitrostátní rámec ochrany údajů, a poskytovat Úřadu komisaře pro informace pokyny a podporu týkající se záležitostí úřadu, jako jsou oblast nemovitostí, nájmů a veřejných zakázek (dohoda o řízení na období 2018–2021, k dispozici na této adrese: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf)

a nesmí od nikoho vyžadovat ani přijímat pokyny. Komisař se rovněž musí zdržet jakéhokoli jednání neslučitelného s jeho funkcí a během svého funkčního období nesmí vykonávat žádnou výdělečnou ani nevýdělečnou pracovní činnost neslučitelnou s touto funkcí.

(88) Podmínky jmenování a odvolání komisaře pro informace jsou stanoveny v příloze 12 zákona o ochraně údajů z roku 2018. Komisaře pro informace jmenuje Její Veličenstvo na doporučení vlády na základě spravedlivého a otevřeného výběrového řízení. Uchazeč musí mít odpovídající kvalifikaci, dovednosti a způsobilost. V souladu s Kodexem pro jmenování do veřejných funkcí ([83]) sestavuje poradní hodnotící panel seznam kandidátů, kteří pro jmenování přicházejí v úvahu. Nežli ministr pro digitální oblast, kulturu, sdělovací prostředky a sport vydá své konečné rozhodnutí, musí příslušná parlamentní výběrová komise provést prověření před jmenováním. Stanovisko komise se zveřejňuje ([84]).

(89) Komisař pro informace vykonává svou funkci po dobu až sedmi let. Jednotlivec nemůže být komisařem pro informace jmenován vícekrát. Komisaře pro informace může z funkce odvolat Její Veličenstvo na návrh (address) obou komor parlamentu Spojeného království ([85]). Žádné komoře parlamentu Spojeného království nelze předložit žádost o odvolání komisaře pro informace, pokud ministr nepředloží zprávu, v níž uvede, že dle jeho přesvědčení je komisař pro informace vinen závažným pochybením nebo již nesplňuje podmínky požadované pro výkon jeho funkcí ([86]).

(90) Financování komisaře pro informace pochází ze tří zdrojů: i) poplatky za ochranu údajů placené správci, které jsou stanoveny v nařízeních ministra ([87]) (nařízení o ochraně údajů (poplatky a informace) z roku 2018) a představují 85–90 % ročního rozpočtu úřadu ([88]); ii) podpůrný grant vyplácený vládou komisaři pro informace. Podpůrný grant se používá zejména k financování provozních nákladů komisaře pro informace, pokud jde o úkoly nesouvisející s ochranou údajů ([89]), a iii) poplatky účtované za služby ([90]). V současné době nejsou žádné takové poplatky účtovány.

(91) Obecné funkce komisaře pro informace týkající se zpracování osobních údajů, na které se vztahuje britské nařízení GDPR, jsou stanoveny v článku 57 britského nařízení GDPR, který úzce odráží odpovídající pravidla nařízení (EU) 2016/679. Mezi jeho funkce patří sledování a vymáhání britského nařízení GDPR, zvyšování povědomí veřejnosti, vyřizování stížností podaných subjekty údajů, vedení vyšetřování atd. Kromě toho článek 115 zákona o ochraně údajů z roku 2018 vymezuje další obecné funkce komisaře, k nimž patří povinnost poskytovat poradenství parlamentu Spojeného království, vládě a ostatním orgánům a institucím ohledně legislativních a správních opatření týkajících se ochrany práv a svobod jednotlivců v souvislosti se zpracováním osobních údajů a pravomoc vydávat z vlastního podnětu komisaře nebo na požádání stanoviska pro parlament, vládu nebo jiné instituce

([83]) Správní kodex pro jmenování do veřejných funkcí, k dispozici na této adrese: 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 zpráva Výboru Dolní sněmovny Spojeného království pro kulturu, sdělovací prostředky a sport za období 2015–2016, k dispozici na této adrese: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf

([85]) Tzv. „address" je návrh předložený v Parlamentu Spojeného království, který má panovníka informovat o stanoviscích parlamentu v konkrétní věci.

([86]) Ustanovení čl. 3 odst. 3 přílohy 12 zákona o ochraně údajů z roku 2018.

([87]) Článek 137 zákona o ochraně údajů z roku 2018, viz (17). bod odůvodnění.

([88]) Články 137 a 138 zákona o ochraně údajů z roku 2018 obsahují řadu záruk, které zajišťují stanovení poplatků v odpovídající výši. Zejména čl. 137 odst. 4 vyjmenovává záležitosti, které musí ministr zohlednit při přípravě nařízení, jež stanoví částku, kterou musí různé organizace zaplatit. Dále čl. 138 odst. 1 a článek 182 zákona o ochraně údajů z roku 2018 rovněž obsahují právní požadavek, aby ministr před přijetím nařízení konzultoval s komisařem pro informace a dalšími zástupci osob, které by mohly být nařízeními ovlivněny, aby bylo možné zohlednit jejich stanoviska. Podle čl. 138 odst. 2 zákona o ochraně údajů z roku 2018 je také komisař pro informace povinen průběžně přezkoumávat, jak nařízení o poplatcích fungují, a může ministrovi předkládat návrhy na změny nařízení. A konečně, s výjimkou případů, kdy jsou nařízení vydána pouze za účelem zohlednění nárůstu indexu maloobchodních cen (a kdy budou podléhat postupu zamítavého usnesení), podléhají nařízení postupu souhlasného usnesení a nesmí být přijaty, nežli je usnesením schválí každá z komor parlamentu Spojeného království.

([89]) Dohoda o řízení objasnila, že „ministr může provádět platby ve prospěch komisaře pro informace z finančních prostředků poskytnutých parlamentem Spojeného království podle článku 9 přílohy 12 zákona o ochraně údajů z roku 2018. Po konzultaci s komisařem pro informace vyplatí ministerstvo pro digitální oblast, kulturu, sdělovací prostředky a sport příslušné částky (podpůrný grant) na administrativní náklady komisaře pro informace a výkon jeho funkcí ve vztahu k řadě konkrétních úkolů, včetně svobody informací" (článek 1.12 dohody o řízení na období 2018–2021, viz poznámka pod čarou 82).

([90]) Viz článek 134 zákona o ochraně údajů z roku 2018.

a orgány i veřejnost k jakékoli otázce související s ochranou osobních údajů. V zájmu zachování nezávislosti soudnictví není komisař pro informace oprávněn vykonávat své funkce v souvislosti se zpracováním osobních údajů jednotlivcem, který jedná v rámci soudních pravomocí, nebo soudem či tribunálem jednajícím v rámci své soudní pravomoci. Dohled nad soudnictvím však vykonávají specializované úřady (viz 99. až 103. bod odůvodnění.)

2.6.2 *Vymáhání včetně sankcí*

(92) Pravomoci komisaře pro informace stanoví článek 58 britského nařízení GDPR, který nezavádí žádné podstatné změny odpovídajícího článku nařízení (EU) 2016/679. Doplňková pravidla pro výkon těchto pravomocí stanoví zákon o ochraně údajů z roku 2018. Komisař má zejména pravomoc: a) nařídit správci a zpracovateli (a za určitých okolností kterékoli jiné osobě), aby poskytli nezbytné informace, výzvou k podání informací (dále jen „výzva k podání informací“) ([91]); b) provádět vyšetřování a audity na základě výzvy k posouzení, která může vyžadovat, aby správce nebo zpracovatel komisaři povolil vstoupit do určených prostor, nahlížet do dokumentů nebo zařízení nebo je kontrolovat, vyslechnout osoby zpracovávající osobní údaje jménem správce atd. (dále jen „oznámení o posouzení“) ([92]); c) získat jiným způsobem přístup k dokumentům atd. správců a zpracovatelů a přístup do jejich prostor v souladu s oddílem 154 zákona o ochraně údajů z roku 2018 (dále jen „pravomoci vstupu a inspekce“); d) vykonávat nápravné pravomoci, a to i formou varování a napomenutí, nebo vydávat příkazy prostřednictvím oznámení o vymáhání, které vyžaduje, aby správci/zpracovatelé provedli určité kroky nebo aby se určitých kroků zdrželi, včetně nařízení správci nebo zpracovateli, aby učinil cokoli podle čl. 58 odst. 2 písm. c) až g) a j) britského nařízení GDPR (dále jen „oznámení o vymáhání“) ([93]); e) a udělovat správní pokuty formou oznámení o sankci (dále jen „oznámení o sankci“) ([94]). Posledně jmenované oznámení lze vydat i v případě, že orgán veřejné moci nedodržel ustanovení britského nařízení GDPR ([95]).

(93) Politika regulačních opatření Úřadu komisaře pro informace stanoví okolnosti, za kterých bude vydávat výzvu k podání informací, oznámení o posouzení, vymáhání nebo sankci ([96]). Oznámení o vymáhání vydané v reakci na selhání správce nebo zpracovatele může ukládat pouze požadavky, které komisař považuje za vhodné pro účely nápravy selhání. Oznámení o vymáhání a sankci mohou být správci nebo zpracovateli vydána v souvislosti s porušeními kapitoly II britského nařízení GDPR (zásady zpracování), článků 12–22 (práva subjektu údajů), článků 25–39 (povinnosti správců a zpracovatelů) a články 44–49 (mezinárodní předání) britského nařízení GDPR. Oznámení o vymáhání lze vydat i v případě, že správce nesplnil požadavek uhradit poplatek stanovený v nařízeních vydaných podle článku 137 zákona o ochraně údajů z roku 2018. Kromě toho může být kontrolnímu subjektu podle článku 41 nebo subjektu vydávajícímu osvědčení zasláno oznámení o vymáhání, pokud neplní své povinnosti podle britského nařízení GDPR. Oznámení o sankci lze rovněž vydat vůči osobě, která nesplnila výzvu k podání informací, oznámení o posouzení nebo oznámení o vymáhání.

(94) Oznámení o sankci vyžaduje, aby daná osoba zaplatila komisaři pro informace částku uvedenou v oznámení. Při rozhodování o tom, zda vůči určité osobě vydat oznámení o sankci, a při určování výše sankce musí komisař pro informace vzít v úvahu záležitosti vyjmenované v čl. 83 odst. 1 a 2 britského nařízení GDPR, které jsou totožné s odpovídajícími pravidly nařízení (EU) 2016/679 ([97]). Podle čl. 83 odst. 4 a 5 činí maximální výše správních pokut v případě nesplnění povinností stanovených v uvedených ustanoveních 8 700 000 GBP, resp. 17 500 000 GBP.

([91]) Článek 142 zákona o ochraně údajů z roku 2018 (s výhradou omezení v článku 143 zákona o ochraně údajů z roku 2018).
([92]) Článek 146 zákona o ochraně údajů z roku 2018 (s výhradou omezení v článku 147 zákona o ochraně údajů z roku 2018).
([93]) Články 149 až 151 zákona o ochraně údajů z roku 2018 (s výhradou omezení v článku 152 zákona o ochraně údajů z roku 2018).
([94]) Článek 155 zákona o ochraně údajů z roku 2018 a článek 83 britského nařízení GDPR.
([95]) To vyplývá z čl. 155 odst. 1 zákona o ochraně údajů z roku 2018 ve spojení s čl. 149 odst. 2 a 5 zákona o ochraně údajů z roku 2018 a z čl. 156 odst. 4 zákona o ochraně údajů z roku 2018, který omezuje vydávání oznámení o sankci, pokud jde o komisaře pro majetek Koruny a správce domácnosti panovníka podle čl. 209 odst. 4 zákona o ochraně údajů z roku 2018.
([96]) Politika regulačních opatření, k dispozici na této adrese: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf
([97]) Včetně povahy a závažnosti porušení (s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, jež jim byla způsobena), toho, zda k porušení došlo úmyslně nebo z nedbalosti, kroků podniknutých správcem či zpracovatelem ke zmírnění škod způsobených subjektům údajů, míry odpovědnosti správce či zpracovatele (s přihlédnutím k technickým a organizačním opatřením, která správce nebo zpracování zavedl), veškerých relevantních předchozích porušení správcem či zpracovatelem; míry spolupráce s komisařem, kategorií osobních údajů dotčených daným porušením, jakékoli jiné přitěžující nebo polehčující okolnosti vztahující se na okolnosti daného případu, jako jsou získaný finanční prospěch či zamezení ztrátám, přímo či nepřímo vyplývající z porušení.

V případě podniku může komisař pro informace ukládat pokuty také jako procento celosvětového ročního obratu, pokud je tato částka vyšší. Stejně jako v rovnocenných ustanoveních nařízení (EU) 2016/679 jsou tyto částky v čl. 83 odst. 4 a 5 stanoveny na 2 %, resp. 4 %. V případě nesplnění výzvy k poskytnutí informací, oznámení o posouzení nebo oznámení o vymáhání je maximální výší pokuty, která může být uložena oznámením o sankci, částka 17 500 000 GBP, nebo v případě podniku 4 % celosvětového ročního obratu, podle toho, která z částek je vyšší.

(95) Britské nařízení GDPR spolu se zákonem o ochraně údajů z roku 2018 posílilo i další pravomoci komisaře pro informace. Komisař například nyní může prostřednictvím oznámení o posouzení provádět povinné audity ve vztahu ke všem správcům a zpracovatelům, zatímco podle předchozí legislativy, zákona o ochraně údajů z roku 1998, měl komisař tuto pravomoc pouze vůči ústředním vládním institucím a organizacím v oblasti zdravotnictví a ostatní subjekty musely s auditem vyslovit souhlas.

(96) Od zavedení nařízení (EU) 2016/679 vyřizuje Úřad komisaře pro informace přibližně 40 000 stížností subjektů údajů ročně ([98]) a kromě toho provádí přibližně 2 000 šetření z moci úřední ([99]). Většina stížností se týká práv přístupu k údajům a zveřejňování údajů. Po svém šetření přijímá komisař donucovací opatření v široké škále odvětví. Přesněji řečeno, podle poslední výroční zprávy Úřadu komisaře pro informace (2019–2020) ([100]) vydala stávající komisařka během sledovaného období 54 výzev k podání informací, osm oznámení o posouzení, sedm oznámení o vymáhání, čtyři výstrahy, osm návrhů na zahájení trestního stíhání a patnáct pokut ([101]).

(97) To zahrnuje několik významných peněžních pokut uložených podle nařízení (EU) 2016/679 a zákona o ochraně údajů z roku 2018. Zejména stávající komisařka pro informace v říjnu 2020 uložila britské letecké společnosti pokutu ve výši 20 milionů GBP za porušení zabezpečení osobních údajů, které se dotklo více než 400 000 zákazníků. Na konci října 2020 byla mezinárodnímu hotelovému řetězci uložena pokuta ve výši 18,4 milionu GBP za to, že nezajistil bezpečnost osobních údajů milionů zákazníků, a v listopadu 2020 britský poskytovatel služeb prodávající na internetu lístky na akce dostal pokutu ve výši 1,25 milionu GBP za to, že nechránil platební údaje zákazníků ([102]).

(98) Kromě donucovacích pravomocí komisaře pro informace popsaných v 92. bodě odůvodnění představují určitá porušení právních předpisů v oblasti ochrany údajů trestné činy, a proto mohou podléhat trestním sankcím (článek 196 zákona o ochraně údajů z roku 2018). Týká se to například vědomého nebo bezohledného získávání nebo zpřístupňování osobních údajů bez souhlasu správce, zajišťování zpřístupnění osobních údajů jiné osobě bez souhlasu správce ([103]), opětovné identifikace údajů, které jsou osobními údaji, jež byly anonymizovány bez souhlasu správce odpovědného za anonymizaci daných osobních údajů ([104]), záměrného maření výkonu pravomocí komisaře v souvislosti s inspekcí osobních údajů v souladu s mezinárodními závazky ([105]), vydávání nepravdivých prohlášení v reakci na výzvu k podání informací nebo ničení údajů v souvislosti s výzvami k podání informací a oznámeními o posouzení ([106]).

([98]) Podle informací, které poskytly orgány Spojeného království, nebylo během období, na které se vztahuje výroční zpráva komisaře pro informace 2019–2020, zjištěno žádné porušení předpisů v přibližně 25 % případů, v přibližně 29 % případů byl subjekt údajů vyzván, aby vůči správci údajů buď nejprve vyjádřil znepokojení, vyčkal na odpověď správce, nebo pokračoval v probíhajícím dialogu se správcem údajů, v přibližně 17 % případů nebylo zjištěno žádné porušení, správci údajů však bylo poskytnuto poradenství, v přibližně 25 % případů stávající komisařka pro informace zjistila porušení předpisů a buď poskytla správci údajů poradenství, nebo byl správce údajů povinen přijmout určitá opatření, přibližně ve 3 % případů bylo zjištěno, že stížnost nespadá do oblasti působnosti nařízení (EU) 2016/679, a přibližně 1 % případů bylo postoupeno jinému orgánu pro ochranu údajů v rámci Evropského sboru pro ochranu osobních údajů.

([99]) Úřad komisaře pro informace může tato šetření zahájit na základě informací obdržených z různých zdrojů, včetně oznámení o porušení zabezpečení osobních údajů, postoupení ze strany jiných orgánů veřejné moci ve Spojeném království nebo zahraničních úřadů pro ochranu osobních údajů a stížností podaných jednotlivci nebo organizacemi občanské společnosti.

([100]) Výroční zpráva a účetní závěrka komisaře pro informace za období 2019–2020 (viz poznámka pod čarou 81).

([101]) Podle předchozí výroční zprávy za období 2018–2019 vydala stávající komisařka pro informace ve sledovaném období 22 oznámení o sankci podle zákona o ochraně údajů z roku 1998, přičemž pokuty dosáhly celkové výše 3 010 610 GBP, včetně dvou pokut ve výši 500 000 GBP (maximální povolená částka podle zákona o ochraně údajů z roku 1998). V roce 2018 provedla komisařka pro informace zejména vyšetřování týkající se používání analýzy dat pro politické účely v návaznosti na odhalení týkající se společnosti Cambridge Analytica. Výsledkem vyšetřování byla politická zpráva, soubor doporučení, pokuta ve výši 500 000 GBP vůči společnosti Facebook a oznámení o vymáhání vůči společnosti Aggregate IQ, kanadské společnosti zprostředkující informace, kterým bylo nařízeno vymazat osobní údaje týkající se občanů a rezidentů Spojeného království, které měla v držení (viz výroční zpráva a účetní závěrka komisaře pro informace za období 2018–2019, k dispozici na adrese https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf)

([102]) Shrnutí přijatých donucovacích opatření je k dispozici na webových stránkách Úřadu komisaře pro informace na této adrese: https://ico.org.uk/action-weve-taken/enforcement/

([103]) Článek 170 zákona o ochraně údajů z roku 2018.

([104]) Článek 171 zákona o ochraně údajů z roku 2018.

([105]) Článek 119 zákona o ochraně údajů z roku 2018.

([106]) Články 144 a 148 zákona o ochraně údajů z roku 2018.

2.6.3 *Dohled nad soudnictvím*

(99) Dohled nad zpracováním osobních údajů soudy a soudní mocí je dvojí. Pokud osoba vykonávající funkci soudce nebo soud nejedná v rámci soudní pravomoci, zajišťuje dohled Úřad komisaře pro informace. Pokud správce jedná v rámci soudní pravomoci, nemůže Úřad komisaře pro informace vykonávat své dozorové funkce ([107]) a dohled provádějí zvláštní subjekty. To odráží přístup zvolený v nařízení (EU) 2016/679 (čl. 55 odst. 3).

(100) Zejména ve druhém scénáři zajišťuje tento dohled nad soudy v Anglii a Walesu a tribunály prvního a vyššího stupně v Anglii a Walesu soudní komise pro ochranu údajů ([108]). Lord nejvyšší soudce (Lord Chief Justice) a vrchní předseda tribunálů vydali oznámení o ochraně osobních údajů ([109]), které stanoví, jak soudy v Anglii a Walesu zpracovávají osobní údaje v rámci soudní funkce. Obdobné oznámení bylo vydáno v rámci soudnictví Severního Irska ([110]) a Skotska ([111]).

(101) Kromě toho v Severním Irsku jmenoval Lord nejvyšší soudce pro Severní Irsko soudce Vrchního soudu soudcem pověřeným dozorem nad ochranou údajů (Data Supervisory Judge) ([112]). Vydal rovněž pokyny pro soudnictví Severního Irska ve věci postupu v případě ztráty nebo potenciální ztráty údajů a řešení jakýchkoli problémů z toho vyplývajících ([113]).

(102) Ve Skotsku jmenoval lord nejvyšší soudce (Lord President) soudce pro dozor nad ochranou údajů, který bude vyšetřovat jakékoli stížnosti z důvodu ochrany údajů. Je to stanoveno v pravidlech pro soudní stížnosti, která odrážejí pravidla stanovená pro Anglii a Wales ([114]).

(103) A konečně, u Nejvyššího soudu je jmenován jeden ze soudců Nejvyššího soudu, aby dohlížel na ochranu údajů.

2.6.4 *Soudní ochrana*

(104) Aby se zajistila odpovídající ochrana, a zejména vymáhání individuálních práv, měla by být subjektu údajů poskytnuta účinná správní a soudní ochrana, včetně náhrady škody.

([107]) Článek 117 zákona o ochraně údajů z roku 2018.

([108]) Komise odpovídá za poskytování poradenství a odborné přípravy soudcům. Zabývá se i stížnostmi subjektů údajů v souvislosti se zpracováním osobních údajů ze strany soudů, tribunálů a jednotlivců jednajících v rámci soudní pravomoci. Cílem komise je poskytnout prostředky, kterými by bylo možné vyřešit jakoukoli stížnost. Pokud stěžovatel nebyl s rozhodnutím komise spokojen a předložil dodatečné důkazy, mohla by komise své rozhodnutí znovu zvážit. Sama komise neukládá finanční sankce, pokud však má za to, že došlo k dostatečně závažnému porušení zákona o ochraně údajů z roku 2018, může stížnost postoupit Úřadu pro vyšetřování jednání soudů (Judicial Conduct Investigation Office), který stížnost prošetří. Je-li stížnosti vyhověno, je věcí lorda kancléře a lorda nejvyššího soudce (nebo vyššího soudce pověřeného jednat v jeho zastoupení), aby rozhodli, jaká opatření by měla být vůči osobě zastávající danou funkci přijata. To by mohlo zahrnovat, v pořadí podle závažnosti: formální doporučení, formální varování a napomenutí a nakonec odvolání z funkce. Pokud je jednotlivec nespokojen s tím, jak Úřad pro vyšetřování jednání soudů stížnost vyšetřoval, může si podat další stížnost veřejnému ochránci práv pro jmenování a jednání soudců (viz https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Veřejný ochránce práv má pravomoc požádat Úřad pro vyšetřování jednání soudů, aby stížnost znovu prošetřil, a může navrhnout, aby bylo stěžovateli vyplaceno odškodnění, pokud je přesvědčen, že následkem nesprávného úředního postupu utrpěl škodu.

([109]) Oznámení Lorda nejvyššího soudce a vrchního předsedy tribunálů o ochraně osobních údajů je k dispozici na této adrese: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([110]) Oznámení Lorda nejvyššího soudce pro Severní Irsko o ochraně osobních údajů je k dispozici na této adrese: https://judiciaryni.uk/data-privacy

([111]) Oznámení o ochraně osobních údajů pro skotské soudy a tribunály je k dispozici na této adrese: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([112]) Soudce pověřený dozorem nad ochranou údajů poskytuje pokyny pro oblast soudnictví a vyšetřuje případy porušení předpisů nebo stížnosti týkající se zpracování osobních údajů ze strany soudů nebo jednotlivců jednajících v rámci soudní pravomoci.

([113]) Jestliže se stížnost nebo případ porušení předpisů považují za závažné, jsou podle kodexu zásad týkajícího se stížností, který vydal lord nejvyšší soudce pro Severní Irsko, postoupeny k dalšímu šetření úředníkovi pro stížnosti v soudnictví. Výsledek takové stížnosti by mohl zahrnovat: žádné další opatření, doporučení, školení nebo mentoring, neformální varování, formální varování, konečné varování, omezení výkonu praxe nebo postoupení zákonnému tribunálu. Kodex zásad týkající se stížností, který vydal lord nejvyšší soudce pro Severní Irsko, je k dispozici na této adrese: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]) Jakákoli opodstatněná stížnost je vyšetřována soudcem pro dozor nad ochranou údajů a postoupena lordu nejvyššímu soudci, který má pravomoc vydat doporučení, formální varování nebo napomenutí, pokud to považuje za nutné. (Rovnocenná pravidla existují pro členy tribunálů a jsou k dispozici na této adrese: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2)

(105) Zaprvé má subjekt údajů právo podat stížnost u komisaře pro informace, pokud má za to, že v souvislosti s jeho osobními údaji došlo k porušení britského nařízení GDPR ([115]). Britské nařízení GDPR zachovává pravidla článku 77 nařízení (EU) 2016/679 týkající se tohoto práva bez podstatných úprav. Totéž platí pro čl. 57 odst. 1 písm. f) a odst. 2, které stanoví úkoly komisaře v souvislosti s vyřizováním stížností. Jak je popsáno v 92. až 98. bodě odůvodnění výše, komisař pro informace má pravomoc posoudit, jak správce a zpracovatel dodržují britské nařízení GDPR a zákon o ochraně údajů z roku 2018, vyžadovat od nich, aby v případě nedodržení předpisů přijali nezbytné kroky nebo se takových kroků zdrželi, a ukládat pokuty.

(106) Zadruhé britské nařízení GDPR a zákon o ochraně údajů z roku 2018 poskytují právo na soudní ochranu vůči komisaři pro informace. Podle čl. 78 odst. 1 britského nařízení GDPR má jednotlivec právo na účinnou soudní ochranu proti právně závaznému rozhodnutí komisaře, které se ho týká. V rámci soudního přezkumu zkoumá soudce rozhodnutí napadené ve stížnosti a zvažuje, zda komisař pro informace jednal zákonným způsobem. Kromě toho čl. 78 odst. 2 britského nařízení GDPR stanoví, že pokud komisař řádně nevyřídí stížnost podanou subjektem údajů ([116]), má stěžovatel přístup k soudní ochraně. Může se obrátit na tribunál prvního stupně, aby nařídil komisaři přijmout vhodná opatření v reakci na stížnost nebo aby stěžovatele informoval o pokroku při vyřizování stížnosti ([117]). Kromě toho se každá osoba, které je doručeno jedno z výše uvedených oznámení (výzva k podání informací, oznámení o posouzení, vymáhání nebo sankci), může odvolat k tribunálu prvního stupně ([118]). Pokud tribunál dospěje k závěru, že rozhodnutí komisaře není v souladu se zákonem, nebo že měl komisař pro informace uplatnit svou diskreční pravomoc jinak, musí tribunál vyhovět opravnému prostředku nebo vydat jiné oznámení nebo přijmout jiné rozhodnutí, které komisař pro informace mohl vydat nebo učinit.

(107) Zatřetí podle článku 79 britského nařízení GDPR a článku 167 zákona o ochraně údajů z roku 2018 mohou jednotlivci získat soudní ochranu vůči správcům a zpracovatelům přímo u soudů. Pokud soud na základě žádosti subjektu údajů dospěje k závěru, že došlo k porušení práv subjektu údajů podle právních předpisů v oblasti ochrany údajů, může soud v souvislosti s daným zpracováním nařídit správci nebo zpracovateli jednajícímu v zastoupení tohoto správce, aby přijal kroky stanovené v soudním příkazu nebo aby se takových kroků zdržel.

(108) Kromě toho článek 82 britského nařízení GDPR a článek 168 zákona o ochraně údajů z roku 2018 stanoví, že kdokoli, kdo v důsledku porušení britského nařízení GDPR utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy. Pravidla pro náhradu újmy a odpovědnost v čl. 82 odst. 1–5 britského nařízení GDPR jsou totožná s odpovídajícími pravidly nařízení (EU) 2016/679. Podle článku 168 zákona o ochraně údajů z roku 2018 zahrnuje nehmotná újma i utrpení. Podle článku 80 britského nařízení GDPR má subjekt údajů také právo pověřit zastupující subjekt nebo organizaci, aby jeho jménem podal(a) stížnost komisaři (podle článku 77 britského nařízení GDPR) a aby jeho jménem uplatnil(a) práva uvedená v článku 78 (právo na účinnou soudní ochranu vůči komisaři), článku 79 (právo na účinnou soudní ochranu vůči správci nebo zpracovateli) a článku 82 (právo na náhradu újmy a odpovědnost) britského nařízení GDPR.

(109) Začtvrté může kromě opravných prostředků popsaných výše každá osoba, která má za to, že orgány veřejné moci porušily její práva, včetně práv na soukromí a ochranu údajů, získat soudní ochranu u soudů Spojeného království podle zákona o lidských právech z roku 1998 ([119]). Jednotlivec, který tvrdí, že orgán veřejné moci jednal (nebo navrhuje jednat) způsobem, který je neslučitelný s právem podle úmluvy, a tudíž je podle čl. 6 odst. 1 zákona o lidských právech z roku 1998 protiprávní, může proti tomuto orgánu podat žalobu u příslušného soudu nebo tribunálu nebo se dovolávat dotčených práv v jakémkoli soudním řízení, pokud tento jednotlivec je (nebo by byl) obětí protiprávního jednání.

(110) Pokud soud shledá jakýkoli akt orgánu veřejné moci protiprávním, může v rámci svých pravomocí poskytnout takový opravný prostředek nebo soudní ochranu nebo vydat takový příkaz, které považuje za spravedlivé a vhodné ([120]). Soud může rovněž prohlásit ustanovení primárního právního předpisu za neslučitelné s právem podle úmluvy.

([115]) Článek 77 britského nařízení GDPR.

([116]) Článek 166 zákona o ochraně údajů z roku 2018 uvádí výslovně tyto situace: a) komisař nepřijme vhodná opatření v reakci na stížnost; b) komisař neposkytne stěžovateli informace o pokroku při vyřizování stížnosti nebo o výsledku stížnosti před koncem tříměsíční lhůty od okamžiku, kdy komisař stížnost obdržel nebo c) pokud komisařovo posouzení stížnosti nebude během této lhůty uzavřeno, neposkytne stěžovateli tyto informace během následné tříměsíční lhůty.

([117]) Ustanovení čl. 78 odst. 2 britského nařízení GDPR a článek 166 zákona o ochraně údajů z roku 2018.

([118]) Ustanovení čl. 78 odst. 1 britského nařízení GDPR a článek 162 zákona o ochraně údajů z roku 2018.

([119]) Ustanovení čl. 7 odst. 1 zákona o lidských právech z roku 1998. Podle čl. 7 odst. 7 je osoba obětí protiprávního jednání, pouze pokud by byla obětí ve smyslu článku 34 Evropské úmluvy o lidských právech, pokud by bylo v souvislosti s tímto činem zahájeno řízení u Evropského soudu pro lidská práva.

([120]) Ustanovení čl. 8 odst. 1 zákona o lidských právech z roku 1998.

(111) A konečně může jednotlivec po vyčerpání vnitrostátních opravných prostředků dosáhnout nápravy u Evropského soudu pro lidská práva za porušení práv zaručených Evropskou úmluvou o lidských právech.

3. PŘÍSTUP K OSOBNÍM ÚDAJŮM PŘEDÁVANÝM Z EVROPSKÉ UNIE A JEJICH POUŽITÍ ORGÁNY VEŘEJNÉ MOCI VE SPOJENÉM KRÁLOVSTVÍ

(112) Komise také posuzovala právní rámec Spojeného království týkající se shromažďování a následného používání osobních údajů předávaných podnikatelským subjektům ve Spojeném království orgány veřejné moci Spojeného království pro účely veřejného zájmu, zejména pro účely prosazování trestního práva a národní bezpečnosti (dále jen „přístup vlády“). Při posuzování toho, zda by podmínky, za nichž by přístup vlády k údajům předávaným do Spojeného království podle tohoto rozhodnutí splňoval test „zásadní rovnocennosti“ podle čl. 45 odst. 1 nařízení (EU) 2016/679, jak je vykládán Soudním dvorem Evropské unie ve světle Listiny základních práv, Komise zohlednila zejména následující kritéria.

(113) Zaprvé musí být jakékoli omezení práva na ochranu osobních údajů stanoveno zákonem a samotný právní základ, který umožňuje zásah do takového práva, musí vymezovat rozsah omezení výkonu dotčeného práva ([121]).

(114) Zadruhé, za účelem splnění požadavku proporcionality, podle kterého musí být výjimky z ochrany osobních údajů a její omezení činěny v mezích toho, co je v demokratické společnosti nezbytně nutné pro splnění konkrétních cílů obecného zájmu rovnocenných cílům uznaným Unií, musí předmětná právní úprava třetí země, která daný zásah povoluje, stanovit jasná a přesná pravidla pro rozsah a použití předmětného opatření a stanovit minimální požadavky, tak aby osoby, jejichž údaje byly předány, měly dostatečné záruky umožňující účinně chránit své osobní údaje proti riziku zneužití ([122]). Právní úprava musí zejména vymezit okolnosti a podmínky, za nichž může být přijato opatření týkající se zpracovávání takových údajů ([123]), jakož i podřizovat plnění takových požadavků nezávislému dohledu ([124]).

(115) Zatřetí musí být tato právní úprava podle vnitrostátního práva právně závazná a tyto právní požadavky musí být pro orgány nejen závazné, ale musí být vůči orgánům dotčené třetí země také vymahatelné u soudu ([125]). Subjekty údajů musí mít zejména možnost podat žalobu k nezávislému a nestrannému soudu pro získání přístupu ke svým osobním údajům nebo pro dosažení opravy nebo výmazu takovýchto údajů ([126]).

3.1 Obecný právní rámec

(116) Jakožto výkon pravomoci orgánu veřejné moci musí být přístup vlády ve Spojeném království prováděn při plném dodržení zákona. Spojené království ratifikovalo Evropskou úmluvu o lidských právech (viz 9. bod odůvodnění) a všechny orgány veřejné moci ve Spojeném království jsou povinny jednat v souladu s úmluvou ([127]). Článek 8 úmluvy stanoví, že jakýkoli zásah do soukromí musí být v souladu se zákonem, v zájmu jednoho z cílů stanovených v čl. 8 odst. 2 a přiměřený s ohledem na tento cíl. Článek 8 rovněž vyžaduje, aby byl zásah „předvídatelný“, tj. aby měl jasný a přístupný právní základ, a aby právní předpis obsahoval vhodné záruky, které zabrání zneužití.

(117) Kromě toho Evropský soud pro lidská práva ve své judikatuře upřesnil, že jakýkoli zásah do práva na soukromí a ochranu údajů by měl podléhat účinnému, nezávislému a nestrannému systému dohledu, který musí zajišťovat buď soudce, nebo jiný nezávislý subjekt ([128]) (např. správní orgán nebo parlamentní orgán).

([121]) Viz rozsudek ve věci Schrems II, body 174–175 a citovaná judikatura. Pokud jde o přístup orgánů veřejné moci členských států, viz také věc C-623/17 Privacy International ECLI:EU:C:2020:790, bod 65 a spojené věci C-511/18, C-512/18 a C-520/18 La Quadrature du Net and Others ECLI:EU:C:2020:791, bod 175.

([122]) Viz rozsudek ve věci Schrems II, body 176 a 181, jakož i citovaná judikatura. Pokud jde o přístup orgánů veřejné moci členských států, viz také věc Privacy International, bod 68; a La Quadrature du Net a další, bod 132.

([123]) Viz rozsudek ve věci Schrems II, bod 176. Pokud jde o přístup orgánů veřejné moci členských států, viz také věc Privacy International, bod 68; a La Quadrature du Net a další, bod 132.

([124]) Viz rozsudek ve věci Schrems II, bod 179.

([125]) Viz rozsudek ve věci Schrems II, body 181–182.

([126]) Viz rozsudek ve věci Schrems I, bod 95 a rozsudek ve věci Schrems II, bod 194. V tomto ohledu SDEU zejména zdůraznil, že dodržování článku 47 Listiny základních práv Evropské unie, který zaručuje právo na účinnou ochranu nezávislým a nestranným soudem nebo tribunálem, „spolutvoří úroveň ochrany vyžadovanou v Unii a [jeho] dodržení musí Komise konstatovat ještě před přijetím rozhodnutí o odpovídající ochraně na základě čl. 45 odst. 1 [nařízení (EU) 2016/679]“ (rozsudek ve věci Schrems II, bod 186).

([127]) Článek 6 zákona o lidských právech z roku 1998.

([128]) Evropský soud pro lidská práva, Klass a ostatní v. Německo, stížnost č. 5029/71, body 17–51.

(118) Kromě toho musí být jednotlivcům poskytnuta účinná právní ochrana a Evropský soud pro lidská práva objasnil, že tuto právní ochranu musí nabídnout nezávislý a nestranný subjekt, který přijal svůj vlastní jednací řád a je složen z členů, kteří musí v současnosti zastávat nebo v minulosti zastávali vysokou soudní funkci nebo být zkušenými právníky, a že k podání stížnosti u tohoto subjektu nesmí být zapotřebí splnit jakékoli důkazní břemeno. Při svém šetření stížnosti jednotlivce by měl mít nezávislý a nestranný subjekt přístup ke všem příslušným informacím, včetně uzavřených materiálů. A konečně by měl mít pravomoc napravit protiprávní jednání ([129]).

(119) Spojené království také ratifikovalo úmluvu Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat (úmluva č. 108) a v roce 2018 podepsalo protokol o změně Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat (označovaný jako úmluva č. 108+) ([130]). Článek 9 úmluvy 108 stanoví, že odchylky od obecných zásad ochrany údajů (článek 5 Kvalita údajů), pravidel upravujících zvláštní skupiny údajů (článek 6 Zvláštní skupiny údajů) a práv subjektu údajů (článek 8 Dodatečné záruky pro subjekt údajů) jsou přípustné pouze v případě, že taková odchylka je stanovena zákonem smluvní strany a představuje nezbytné opatření v demokratické společnosti v zájmu ochrany bezpečnosti státu, veřejné bezpečnosti, měnových zájmů státu nebo potírání trestné činnosti nebo ochrany subjektu údajů nebo práv a svobod jiných osob ([131]).

(120) Prostřednictvím členství v Radě Evropy, dodržování Evropské úmluvy o lidských právech a podrobení se soudní pravomoci Evropského soudu pro lidská práva proto Spojené království podléhá řadě povinností zakotvených v mezinárodním právu, které tvoří rámec jeho systému přístupu vlády na základě zásad, záruk a individuálních práv podobných těm, které jsou zaručeny právními předpisy EU a jsou použitelné v členských státech. Jak je zdůrazněno v 19. bodě odůvodnění, pokračující dodržování těchto nástrojů je proto obzvláště důležitým prvkem posouzení, na němž se zakládá toto rozhodnutí.

(121) Specifické záruky a práva týkající se ochrany údajů dále zaručuje zákon o ochraně údajů z roku 2018 v případech, kdy jsou údaje zpracovávány orgány veřejné moci, včetně donucovacích orgánů a subjektů v oblasti národní bezpečnosti.

(122) Zejména je v části 3 zákona o ochraně údajů z roku 2018, který byl přijat za účelem provedení směrnice (EU) 2016/680 do vnitrostátního práva, stanoven režim zpracování osobních údajů v rámci vymáhání trestního práva. Část 3 zákona o ochraně údajů z roku 2018 se použije na zpracování osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení ([132]).

(123) Pojem „příslušný orgán“ je vymezen v článku 30 zákona o ochraně údajů jako osoba vyjmenovaná v příloze 7 zákona o ochraně údajů z roku 2018, jakož i kterákoli jiná osoba, která má zákonné funkce pro jakékoli účely prosazování práva ([133]). Jak je vysvětleno níže (viz 139. bod odůvodnění), některé příslušné orgány (například Národní kriminální agentura) mohou za určitých podmínek využívat pravomoci, které stanoví zákon o vyšetřovacích pravomocích z roku 2016. V takovém případě se kromě záruk stanovených částí 3 zákona o ochraně údajů z roku 2018 použijí i záruky stanovené zákonem o vyšetřovacích pravomocích z roku 2016. Zpravodajské služby (Tajná zpravodajská služba, Bezpečnostní služba a Vládní ředitelství pro komunikace) nejsou „příslušnými orgány“ ([134]) spadajícími do oblasti působnosti části 3 zákona o ochraně údajů z roku 2018, a proto se na žádnou z jejich činností nepoužijí pravidla stanovená v uvedené části zákona. Zvláštní část zákona o ochraně údajů z roku 2018 (část 4) je věnována zpracování osobních údajů zpravodajskými službami (další podrobnosti viz 125. bod odůvodnění).

([129]) Evropský soud pro lidská práva, Kennedy proti Spojenému království, stížnost č. 26839/05, (dále jen „rozsudek ve věci Kennedy“), body 167 a 190.

([130]) Více informací o Evropské úmluvě o lidských právech a jejím začlenění do práva Spojeného království prostřednictvím zákona o lidských právech z roku 1998 i o úmluvě č. 108 viz (9). bod odůvodnění.

([131]) Obdobně jsou podle článku 11 úmluvy č. 108+ omezení určitých zvláštních práv a povinností vyplývajících z úmluvy, která jsou přijata pro účely národní bezpečnosti nebo prevence, vyšetřování, odhalování a stíhání trestných činů nebo výkonu trestů, přípustná pouze tehdy, je-li takové omezení stanoveno zákonem, respektuje podstatu základních práv a svobod a představuje nezbytné a přiměřené opatření v demokratické společnosti. Činnosti zpracování pro účely národní bezpečnosti a obrany musí rovněž podléhat nezávislému a účinnému přezkumu a dohledu podle vnitrostátních právních předpisů příslušné smluvní strany úmluvy.

([132]) Článek 31 zákona o ochraně údajů z roku 2018.

([133]) Příslušné orgány vyjmenované v příloze 7 zahrnují nejen policejní síly, ale i všechna ministerstva Spojeného království, jakož i jiné orgány s vyšetřovacími funkcemi (např. Commissioner for Her Majesty's Revenue and Customs (orgán daňové a celní správy Spojeného království), National Crime Agency (Národní kriminální agentura), Welsh Revenue Authority (orgán daňové správy ve Walesu), Competition and Markets Authority (Úřad pro hospodářskou soutěž a trhy) nebo Her Majesty's Land Register (Katastrální úřad Spojeného království), státní zastupitelství, další orgány činné v trestním řízení a další držitele funkcí nebo organizace vykonávající činnosti v oblasti prosazování práva (příloha 7 zákona o ochraně údajů z roku 2018 uvádí také ředitele státních zastupitelství, ředitele státního zastupitelství pro Severní Irsko nebo Komisi pro informace).

([134]) Ustanovení čl. 30 odst. 2 zákona o ochraně údajů z roku 2018.

(124) Obdobně jako směrnice (EU) 2016/680 stanoví část 3 zákona o ochraně údajů z roku 2018 zásady zákonnosti a korektnosti ([135]), účelového omezení ([136]), minimalizace údajů ([137]), přesnosti ([138]), omezení uložení ([139]) a zabezpečení ([140]). Tento právní předpis ukládá konkrétní povinnosti týkající se transparentnosti ([141]) a poskytuje jednotlivcům právo na přístup ([142]), opravu a výmaz ([143]) a právo nebýt předmětem automatizovaného rozhodování ([144]). Od příslušných orgánů se rovněž požaduje, aby zavedly záměrnou a standardní ochranu údajů, vedly záznamy o činnostech zpracování a u některých operací zpracování prováděly posouzení vlivu na ochranu osobních údajů a předem konzultovaly komisaře pro informace ([145]). Podle článku 56 zákona o ochraně údajů z roku 2018 jsou povinny prokázat dodržování právních předpisů. Kromě toho jsou povinny zavést vhodná opatření k zajištění bezpečnosti zpracování ([146]) a vztahují se na ně zvláštní povinnosti v případě porušení zabezpečení údajů, včetně oznámení takových porušení komisaři pro informace a subjektům údajů ([147]). Stejně jako v případě směrnice (EU) 2016/680 je rovněž stanoven požadavek, aby správce (pokud se nejedná o soud nebo jiný soudní orgán jednající v rámci soudních pravomocí) jmenoval pověřence pro ochranu osobních údajů ([148]), který je správci nápomocen při dodržování jeho povinností a monitorování tohoto dodržování ([149]). Právní předpisy dále stanoví zvláštní požadavky na mezinárodní předávání osobních údajů třetím zemím nebo mezinárodním organizacím pro účely prosazování práva s cílem zajistit kontinuitu ochrany ([150]). Ke stejnému datu jako toto rozhodnutí Komise přijala rozhodnutí o odpovídající ochraně podle čl. 36 odst. 3 směrnice (EU) 2016/680, v němž konstatuje, že režim ochrany údajů použitelný na zpracování donucovacími orgány ve Spojeném království zajišťuje úroveň ochrany v zásadě rovnocennou úrovni ochrany, kterou zaručuje směrnice (EU) 2016/680.

(125) Část 4 zákona o ochraně údajů z roku 2018 se použije na veškeré zpracování prováděné zpravodajskými službami nebo jejich jménem. Stanovuje zejména hlavní zásady ochrany údajů (zákonnost, korektnost a transparentnost ([151]); účelové omezení ([152]); minimalizaci údajů ([153]); přesnost ([154]); omezení uložení ([155]) a zabezpečení ([156])), ukládá podmínky pro zpracování zvláštních kategorií údajů ([157]), stanoví práva subjektu údajů ([158]), vyžaduje záměrnou

([135]) Článek 35 zákona o ochraně údajů z roku 2018.
([136]) Článek 36 zákona o ochraně údajů z roku 2018.
([137]) Článek 37 zákona o ochraně údajů z roku 2018.
([138]) Článek 38 zákona o ochraně údajů z roku 2018.
([139]) Článek 39 zákona o ochraně údajů z roku 2018.
([140]) Článek 40 zákona o ochraně údajů z roku 2018.
([141]) Článek 44 zákona o ochraně údajů z roku 2018.
([142]) Článek 45 zákona o ochraně údajů z roku 2018.
([143]) Články 46 a 47 zákona o ochraně údajů z roku 2018.
([144]) Články 49 a 50 zákona o ochraně údajů z roku 2018.
([145]) Články 56–65 zákona o ochraně údajů z roku 2018.
([146]) Článek 66 zákona o ochraně údajů z roku 2018.
([147]) Články 67–68 zákona o ochraně údajů z roku 2018.
([148]) Články 69-71 zákona o ochraně údajů z roku 2018.
([149]) Články 67–68 zákona o ochraně údajů z roku 2018.
([150]) Kapitola 5 části 3 zákona o ochraně údajů z roku 2018.
([151]) Podle čl. 86 odst. 6 zákona o ochraně údajů z roku 2018 musí být pro účely určení korektnosti a transparentnosti zpracování zohledněna metoda, jakou je korektnosti a transparentnosti dosaženo. V tomto smyslu je požadavek korektnosti a transparentnosti naplněn, jsou-li údaje získány od osoby, která má zákonné oprávnění nebo povinnost údaje poskytnout.
([152]) Podle článku 87 zákona o ochraně údajů z roku 2018 musí být upřesněny výslovné a oprávněné účely zpracování. Údaje nesmí být zpracovány způsobem, který není slučitelný s účely, pro které jsou shromážděny. Podle čl. 87 odst. 3 zákona o ochraně údajů z roku 2018 může být další slučitelné zpracování osobních údajů přípustné pouze v případě, že je správce ze zákona oprávněn zpracovávat údaje pro daný účel a zpracování je pro tento další účel nezbytné a přiměřené. Zpracování by se mělo považovat za slučitelné, pokud spočívá ve zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely a podléhá příslušným zárukám (čl. 87 odst. 4 zákona o ochraně údajů z roku 2018).
([153]) Osobní údaje musí být přiměřené, přímo související a omezené na nezbytný rozsah (článek 88 zákona o ochraně údajů z roku 2018).
([154]) Osobní údaje musí být přesné a aktuální (článek 89 zákona o ochraně údajů z roku 2018).
([155]) Osobní údaje nesmí být uchovávány po delší než nezbytnou dobu (článek 90 zákona o ochraně údajů z roku 2018).
([156]) Šestá zásada ochrany údajů stanoví, že osobní údaje musí být zpracovávány způsobem, který zahrnuje přijetí vhodných bezpečnostních opatření, pokud jde o rizika, která vyplývají ze zpracování osobních údajů. Mezi tato rizika patří (mimo jiné) náhodný nebo neoprávněný přístup k osobním údajům nebo zničení, ztráta, použití, pozměnění nebo zpřístupnění osobních údajů (článek 91 zákona o ochraně údajů z roku 2018). Článek 107 rovněž stanoví, že 1) každý správce musí zavést vhodná bezpečnostní opatření odpovídající rizikům vyplývajícím ze zpracování osobních údajů a 2) v případě automatizovaného zpracování musí každý správce a každý zpracovatel zavést preventivní nebo zmírňující opatření na základě hodnocení rizik.
([157]) Ustanovení čl. 86 odst. 2 písm. b) a příloha 10 zákona o ochraně údajů z roku 2018.
([158]) Kapitola 3 části 4 zákona o ochraně údajů z roku 2018, zejména tato práva: na přístup, opravu nebo výmaz, právo vznést námitku proti zpracování a právo nebýt předmětem automatizovaného rozhodování, zasáhnout do automatizovaného rozhodování a být o rozhodování informován. Kromě toho musí správce poskytnout subjektu údajů informace o zpracování osobních údajů subjektu. Jak je vysvětleno v pokynech Úřadu komisaře pro informace ke zpracování osobních údajů zpravodajskými službami, jednotlivci mohou vykonávat všechna svá práva (včetně žádosti o opravu) podáním stížnosti u Úřadu komisaře pro informace nebo předložením věci soudu (viz Pokyny Úřadu komisaře pro informace ke zpracování osobních údajů zpravodajskými službami, k dispozici na adrese: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

a standardní ochranu údajů ([159]) a reguluje mezinárodní předávání osobních údajů ([160]). Úřad komisaře pro informace nedávno vydal podrobné pokyny týkající se zpracování údajů zpravodajskými službami podle části 4 zákona o ochraně údajů z roku 2018 ([161]).

(126) Zároveň článek 110 zákona o ochraně údajů z roku 2018 stanoví výjimku z konkrétních ustanovení části 4 zákona o ochraně údajů z roku 2018 ([162]), je-li taková výjimka požadována k zajištění národní bezpečnosti. Tuto výjimku lze využít na základě analýzy jednotlivých případů ([163]). Jak vysvětlily orgány Spojeného království a potvrdila judikatura, „správce musí zvážit, jaké by byly skutečné důsledky pro národní bezpečnost nebo obranu, pokud by musel dodržet konkrétní ustanovení o ochraně údajů, a zda by mohl přiměřeně dodržet obvyklé pravidlo, aniž by to ovlivnilo národní bezpečnost nebo obranu“ ([164]). Otázka toho, zda byla výjimka použita správně, podléhá dohledu Úřadu komisaře pro informace ([165]).

(127) Kromě toho v souvislosti s možností omezit použití těchto výše specifikovaných ustanovení z důvodu ochrany „národní bezpečnosti“ může správce podle článku 111 zákona o ochraně údajů z roku 2018 požádat o osvědčení podepsané ministrem nebo generálním prokurátorem, které potvrzuje, že omezení těchto práv je nezbytným a přiměřeným opatřením k ochraně národní bezpečnosti ([166]).

(128) Vláda Spojeného království vydala pokyny, které mají správcům pomoci při zvažování, zda požádat o osvědčení o omezení z důvodu národní bezpečnosti podle zákona o ochraně údajů z roku 2018, a tyto pokyny zejména zdůrazňují, že jakékoli omezení práv subjektů údajů z důvodu zajištění národní bezpečnosti musí být přiměřené a nezbytné ([167]). Všechna osvědčení o omezení z důvodu národní bezpečnosti musí být zveřejněna na webových stránkách Úřadu komisaře pro informace ([168]).

([159]) Článek 103 zákona o ochraně údajů z roku 2018.

([160]) Článek 109 zákona o ochraně údajů z roku 2018. Předání osobních údajů mezinárodním organizacím nebo zemím mimo Spojené království jsou možná, pokud je předání nezbytným a přiměřeným opatřením prováděným pro účely zákonných funkcí správce nebo pro jiné účely stanovené ve zvláštních článcích zákona o Bezpečnostní službě z roku 1989 a zákona o zpravodajských službách z roku 1994.

([161]) Pokyny Úřadu komisaře pro informace, viz poznámka pod čarou 158.
Článek 30 zákona o ochraně údajů z roku 2018 a příloha 7 zákona o ochraně údajů z roku 2018.

([162]) V čl. 110 odst. 2 zákona o ochraně údajů z roku 2018 jsou vyjmenována ustanovení, z nichž je přípustná výjimka. Zahrnují zásady ochrany údajů (vyjma zásady zákonnosti), práva subjektu údajů, povinnost informovat komisaře pro informace o porušení zabezpečení údajů, inspekční pravomoci komisaře pro informace v souladu mezinárodními závazky, určité donucovací pravomoci komisaře pro informace, ustanovení, podle nichž některá porušení ochrany údajů zakládají trestný čin, a ustanovení týkající se zvláštních účelů zpracování, například novinářské, umělecké, akademické nebo umělecké literární účely.

([163]) Viz rozsudek ve věci Baker v Secretary of State, viz poznámka pod čarou 61.

([164]) Britský vysvětlující rámec pro diskuse o odpovídající ochraně, oddíl H: Ochrana údajů týkajících se národní bezpečnosti a rámec vyšetřovacích pravomocí, s. 15–16 (viz poznámka pod čarou 31). Viz také rozsudek ve věci Baker v Secretary of State (viz poznámka pod čarou 61), kterým soud zrušil osvědčení o omezení z důvodu národní bezpečnosti vydané ministrem vnitra a potvrzující používání výjimky z důvodu národní bezpečnosti, přičemž měl za to, že neexistuje důvod poskytnout plošnou výjimku z povinnosti reagovat na žádosti o přístup a že povolení této výjimky za všech okolností bez analýzy jednotlivých případů překračuje rámec nezbytnosti a přiměřenosti za účelem ochrany národní bezpečnosti.

([165]) Viz Memorandum o porozumění mezi Úřadem komisaře pro informace a agenturou UKIC, podle něhož „Pokud Úřad komisaře pro informace obdrží stížnost subjektu údajů, bude se sám chtít přesvědčit, že záležitost byla vyřízena řádně a případně zda byla jakákoli výjimka uplatněna správně“. Memorandum o porozumění mezi Úřadem komisaře pro informace a zpravodajskými službami Spojeného království, článek 16, k dispozici na této adrese: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf

([166]) Zákon o ochraně údajů z roku 2018 zrušil možnost vydávat osvědčení podle čl. 28 odst. 2 zákona o ochraně údajů z roku 1998. Možnost vydávat „stará osvědčení“ však stále trvá v případech, kdy existuje historický důvod podle zákona z roku 1998 (viz bod 17 části 5 přílohy 20 zákona o ochraně údajů z roku 2018). Tato možnost je však zřejmě velmi vzácná a uplatní se pouze v omezených případech, například pokud subjekt údajů napadne použití výjimky z důvodu národní bezpečnosti v souvislosti se zpracováním osobních údajů orgánem veřejné moci, který provedl zpracování podle zákona z roku 1998. Je třeba upozornit, že v těchto případech se použije článek 28 zákona o ochraně údajů z roku 1998 v celém svém znění, včetně možnosti subjektu údajů napadnout osvědčení před soudem.

([167]) Pokyny vlády Spojeného království týkající se osvědčení o omezení z důvodu národní bezpečnosti podle zákona o ochraně údajů z roku 2018, k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf Podle vysvětlení, které poskytly orgány Spojeného království, je osvědčení nezvratným důkazem, že ačkoli je pro údaje nebo zpracování popsané v osvědčení použitelná výjimka, tato výjimka neruší požadavek, aby správce nutnost použití výjimky posoudil individuálně.

([168]) Podle článku 130 zákona o ochraně údajů z roku 2018 se může Úřad komisaře pro informace rozhodnout nezveřejnit celé znění osvědčení nebo jeho část, pokud by to bylo v rozporu se zájmem národní bezpečnosti nebo by to mohlo ohrozit bezpečnost kterékoli osoby. V těchto případech však Úřad komisaře pro informace zveřejní skutečnost, že dané osvědčení bylo vydáno.

(129) Osvědčení by mělo být vydáno na pevně stanovenou dobu nejvýše pěti let, aby orgán výkonné moci prováděl jeho pravidelný přezkum ([169]). Osvědčení uvádí osobní údaje nebo kategorie osobních údajů, na které se výjimka vztahuje, jakož i ustanovení zákona o ochraně údajů z roku 2018, kterých se výjimka týká ([170]).

(130) Je důležité upozornit, že osvědčení o omezení z důvodu národní bezpečnosti neposkytují další důvod pro omezení práv na ochranu osobních údajů na základě národní bezpečnosti. Jinak řečeno správce nebo zpracovatel může osvědčení uplatnit, pouze pokud dospěl k závěru, že je nutné využít výjimku z důvodu národní bezpečnosti, která – jak je vysvětleno výše – musí být použita individuálně ([171]). I když se na dotčenou záležitost vztahuje osvědčení o omezení z důvodu národní bezpečnosti, může Úřad komisaře pro informace šetřit, zda bylo v konkrétním případě využití výjimky z důvodu národní bezpečnosti opodstatněné ([172]).

(131) Kterákoli osoba, jíž se vydání osvědčení přímo dotýká, může proti osvědčení ([173]) podat opravný prostředek u Vrchního tribunálu ([174]), nebo pokud osvědčení identifikuje údaje prostřednictvím obecného popisu, může napadnout použití osvědčení pro konkrétní údaje ([175]). Tribunál přezkoumá rozhodnutí o vydání osvědčení a rozhodne, zda pro vydání osvědčení existovaly rozumné důvody ([176]). Může zvážit celou řadu otázek, včetně nezbytnosti, přiměřenosti a zákonnosti, pokud jde o dopad na práva subjektů údajů a vyvážení potřeby chránit národní bezpečnost. V důsledku toho může tribunál rozhodnout, že se osvědčení nevztahuje na konkrétní osobní údaje, které jsou předmětem opravného prostředku ([177]).

(132) Jiný soubor možných omezení se týká omezení, která se podle přílohy 11 zákona o ochraně údajů z roku 2018 použijí na určitá ustanovení části 4 zákona o ochraně údajů z roku 2018 ([178]) za účelem ochrany jiných důležitých cílů obecného veřejného zájmu nebo chráněných zájmů, jako jsou například výsady parlamentu, povinnost mlčenlivosti, vedení soudních řízení nebo bojová účinnost ozbrojených sil ([179]). Tato ustanovení se na základě výjimky nepoužijí buď na určité kategorie informací („na základě skupiny“), nebo se nepoužijí v rozsahu, v jakém by jejich použití mohlo poškodit chráněný zájem („na základě újmy“) ([180]). Výjimek na základě újmy se lze domáhat,

([169]) Pokyny vlády Spojeného království týkající se osvědčení o omezení z důvodu národní bezpečnosti, bod 15, viz poznámka pod čarou 167.

([170]) Pokyny vlády Spojeného království týkající se osvědčení o omezení z důvodu národní bezpečnosti, bod 5, viz poznámka pod čarou 167.

([171]) Viz poznámka pod čarou 164.

([172]) Článek 102 zákona o ochraně údajů z roku 2018 vyžaduje, aby byl správce údajů schopen prokázat, že dodržel zákon o ochraně údajů z roku 2018. To znamená, že zpravodajská služba by musela Úřadu komisaře pro informace prokázat, že při využití výjimky zvážila konkrétní okolnosti případu. Úřad komisaře pro informace také zveřejňuje evidenci osvědčení o omezení z důvodu národní bezpečnosti, která je k dispozici na této adrese https://ico.org.uk/about-the-ico/our-information/national-security-certificates/

([173]) Ustanovení čl. 111 odst. 3 zákona o ochraně údajů z roku 2018.

([174]) Vrchní tribunál je soud příslušný projednávat opravné prostředky podané proti rozhodnutím nižších správních tribunálů a má zvláštní pravomoc pro přímé opravné prostředky proti rozhodnutím některých orgánů státní správy.

([175]) Ustanovení čl. 111 odst. 5 zákona o ochraně údajů z roku 2018.

([176]) V rozsudku ve věci Baker v Secretary of State (viz poznámka pod čarou 61) zrušil tribunál pro informace osvědčení o omezení z důvodu národní bezpečnosti vydané ministrem vnitra, přičemž měl za to, že neexistuje důvod poskytnout plošnou výjimku z povinnosti reagovat na žádosti o přístup a že povolení této výjimky za všech okolností bez analýzy jednotlivých případů překračuje rámec nezbytnosti a přiměřenosti za účelem ochrany národní bezpečnosti.

([177]) Pokyny vlády Spojeného království týkající se osvědčení o omezení z důvodu národní bezpečnosti, bod 25, viz poznámka pod čarou 167.

([178]) To zahrnuje: i) zásady ochrany údajů podle části 4, vyjma požadavku zákonnosti zpracování podle první zásady a skutečnosti, že zpracování musí splňovat jednu z příslušných podmínek stanovených v přílohách 9 a 10; ii) práva subjektů údajů a iii) povinnosti týkající se oznamování porušení zabezpečení údajů Úřadu komisaře pro informace.

([179]) Část 4 zákona o ochraně údajů z roku 2018 stanoví právní rámec, který se použije na všechny druhy zpracování osobních údajů prováděného zpravodajskými službami (a nikoli jen na výkon jejich úkolů v oblasti národní bezpečnosti). Část 4 se proto vztahuje také na případy, kdy zpravodajské služby zpracovávají údaje například za účelem řízení lidských zdrojů, v rámci soudních sporů nebo v souvislosti se zadáváním veřejných zakázek. Omezení uvedená v příloze 11 jsou určena především pro použití v těchto dalších souvislostech. Například v souvislosti se soudním sporem se zaměstnancem se lze dovolat omezení pro účely „soudního řízení“ nebo v rámci zadávání veřejných zakázek lze uplatnit omezení pro účely „jednání“ atd. To odrážejí i pokyny Úřadu komisaře pro informace ke zpracování osobních údajů zpravodajskými službami, které zmiňují jednání o vypořádání mezi zpravodajskou službou a bývalým zaměstnancem, který uplatňuje nárok z titulu zaměstnání, jako příklad pro použití omezení podle přílohy 11 (viz poznámka pod čarou 161). Rovněž je třeba poznamenat, že tatáž omezení jsou k dispozici i ostatním orgánům veřejné moci podle přílohy 2 části 2 zákona o ochraně údajů z roku 2018.

([180]) Podle britského vysvětlujícího rámce jsou výjimkami „na základě skupiny“: i) informace o udělování vyznamenání a ocenění Koruny; ii) povinnost mlčenlivosti; iii) důvěrné odkazy na zaměstnání, odbornou přípravu nebo vzdělání a iv) zkušební záznamy a známky. Výjimky „na základě újmy“ se týkají těchto záležitostí: i) prevence nebo odhalování trestné činnosti; zadržování a stíhání pachatelů; ii) výsady parlamentu; iii) soudní řízení; iv) bojová účinnost ozbrojených sil Koruny; v) hospodářský blahobyt Spojeného království; vi) jednání se subjektem údajů; vii) vědecký nebo historický výzkum nebo statistické účely; viii) archivace ve veřejném zájmu. Britský vysvětlující rámec pro diskuse o odpovídající ochraně, oddíl H: Národní bezpečnost, s. 13, viz poznámka pod čarou 31.

pouze pokud by použití uvedeného ustanovení o ochraně údajů pravděpodobně mohlo poškodit dotčený specifický zájem. Použití výjimky musí být proto vždy odůvodněno odkazem na příslušnou újmu, která by v jednotlivém případě pravděpodobně nastala. Výjimky na základě skupiny lze uplatnit pouze pro specifickou úzce definovanou kategorii informací, pro kterou je výjimka udělena. Svým účelem a účinkem jsou podobné několika výjimkám z britského nařízení GDPR (podle přílohy 2 zákona o ochraně údajů z roku 2018), které naopak odrážejí výjimky uvedené v článku 23 nařízení GDPR.

(133) Z výše uvedeného vyplývá, že podle příslušných právních předpisů Spojeného království, jak jsou vykládány také soudy a Komisí pro informace, existují omezení a podmínky, které zajišťují, že tyto výjimky a omezení zůstanou v mezích toho, co je nezbytné a přiměřené k ochraně národní bezpečnosti.

3.2 **Přístup orgánů veřejné moci Spojeného království k osobním údajům a jejich použití těmito orgány pro účely prosazování trestního práva**

(134) Právo Spojeného království ukládá řadu omezení přístupu k osobním údajům a použití těchto údajů pro účely prosazování trestního práva a stanoví v této oblasti dozorové a ochranné mechanismy, které jsou v souladu s požadavky uvedenými v 113. až 115. bodě odůvodnění tohoto rozhodnutí. Podmínky, za kterých lze takový přístup uskutečnit, a záruky týkající se využívání těchto pravomocí jsou podrobně posouzeny v následujících oddílech.

3.2.1 *Právní základy a použitelná omezení / použitelné záruky*

(135) Podle zásady zákonnosti zaručené článkem 35 zákona o ochraně údajů z roku 2018 je zpracování osobních údajů pro jakékoli účely prosazování práva zákonné, pouze pokud vychází ze zákona, přičemž buď subjekt údajů udělil souhlas se zpracováním pro daný účel ([181]), nebo je zpracování nezbytné pro plnění úkolu, který za tímto účelem provádí příslušný orgán.

3.2.1.1 Příkazy k domovní prohlídce a příkazy k předání

(136) V právním rámci Spojeného království je shromažďování osobních údajů od hospodářských subjektů, včetně těch, které by zpracovávaly údaje předané z EU na základě tohoto rozhodnutí o odpovídající ochraně, pro účely prosazování trestního práva přípustné na základě příkazů k domovní prohlídce ([182]) a příkazů k předání ([183]).

(137) Příkazy k domovní prohlídce vydává soud, obvykle na návrh vyšetřovatele. Příkazy povolují vyšetřovateli, aby vstoupil do prostor za účelem hledání materiálů nebo osob významných z hlediska jeho vyšetřování a ponechal si cokoli, co spadá do povoleného rozsahu prohlídky, včetně veškerých příslušných dokumentů nebo materiálů obsahujících osobní údaje ([184]). Příkaz k předání, který musí být rovněž vydán soudem, vyžaduje, aby osoba v něm specifikovaná předložila nebo

([181]) Použití souhlasu zřejmě není ve scénáři odpovídající ochrany významné, neboť při předání údajů nebudou údaje shromážděny donucovacím orgánem Spojeného království přímo od subjektu údajů v EU na základě souhlasu.

([182]) Příslušný právní základ viz článek 8 a násl. zákona o policii a důkazech v trestním řízení z roku 1984 (pro Anglii a Wales), článek 10 a násl. zákona o policii a důkazech v trestním řízení (Severní Irsko) z roku 1989 a pro Skotsko je právní základ dán zvykovým právem (viz článek 46 zákona o trestním soudnictví (Skotsko) z roku 2016) a článek 23B trestního zákona (konsolidované znění) (Skotsko). Právní základ pro příkaz k domovní prohlídce vydaný po zatčení viz článek 18 a násl. zákona o policii a důkazech v trestním řízení z roku 1984 (pro Anglii a Wales), článek 20 a násl. zákona o policii a důkazech v trestním řízení (Severní Irsko) z roku 1989 a pro Skotsko je právní základ dán zvykovým právem (viz článek 46 zákona o trestním soudnictví (Skotsko) z roku 2016). Orgány Spojeného království objasnily, že příkazy k domovní prohlídce vydává soud na návrh vyšetřovatele. Příkazy povolují vyšetřovateli vstup do prostor za účelem hledání materiálů nebo osob významných z hlediska jeho vyšetřování; výkon příkazu k prohlídce bude často vyžadovat součinnost policisty.

([183]) Pokud se vyšetřování týká praní peněz (včetně konfiskace a občanskoprávního vymáhacího řízení), je příslušným právním základem pro návrh na příkaz k předání článek 345 a násl. pro Anglii, Wales a Severní Irsko a článek 380 a násl. zákona o výnosech z trestné činnosti z roku 2002 pro Skotsko. Pokud se vyšetřování týká jiných záležitostí než praní peněz, lze návrh na příkaz k předání vydat na základě článku 9 a přílohy 1 zákona o policii a důkazech v trestním řízení z roku 1984 pro Anglii a Wales a článku 10 a násl. zákona o policii a důkazech v trestním řízení (Severní Irsko) z roku 1989 pro Severní Irsko. Pro Skotsko je právní základ dán zvykovým právem (viz článek 46 zákona o trestním soudnictví (Skotsko) z roku 2016) a článkem 23B trestního zákona (konsolidované znění) (Skotsko). Orgány Spojeného království objasnily, že příkaz k předání vyžaduje, aby v příkazu specifikovaná osoba předložila nebo zpřístupnila materiály, které drží nebo ovládá (viz článek 4 přílohy 1 zákona o policii a důkazech v trestním řízení z roku 1984).

([184]) Například zákon o policii a důkazech v trestním řízení z roku 1984 v článcích 8 a 18 obsahuje pravomoci zabavit a ponechat si cokoli, co spadá do povoleného rozsahu prohlídky.

zpřístupnila materiály, které drží nebo ovládá. Navrhovatel musí soudu odůvodnit, proč je příkaz k domovní prohlídce nebo předložení informací nezbytný, a také proč je ve veřejném zájmu. Existuje několik zákonných pravomocí, které umožňují vydání příkazu k domovní prohlídce a příkazů k předání. Každé ustanovení má svůj vlastní soubor zákonných podmínek, které musí být splněny, aby mohl být příkaz k domovní prohlídce ([185]) nebo příkaz k předání ([186]) vydán.

(138) Příkazy k předání a příkazy k domovní prohlídce mohou být napadeny formou soudního přezkumu ([187]). Pokud jde o záruky, všechny orgány činné v trestním řízení spadající do působnosti části 3 zákona o ochraně údajů z roku 2018 mají přístup k osobním údajům (který představuje formu zpracování) pouze v souladu se zásadami a požadavky stanovenými v zákoně o ochraně údajů z roku 2018 (viz 122. a 124. bod odůvodnění výše). Žádost donucovacího orgánu by proto měla být v souladu se zásadou, podle

([185]) Například články 8 a 18 zákona o policii a důkazech v trestním řízení regulují pravomoc smírčího soudce schválit příkaz k domovní prohlídce, resp. pravomoc police prohledat nemovitost. V prvním případě (článek 8) musí být před vydáním příkazu nejprve smírčí soudce přesvědčen, že existují rozumné důvody domnívat se, že: i) byl spáchán závažný žalovatelný trestný čin; ii) v prostorách se nachází materiál, který pravděpodobně bude mít pro vyšetřování daného trestného činu podstatnou hodnotu (ať už sám o sobě, nebo společně s jinými materiály); iii) materiál bude pravděpodobně relevantním důkazem; iv) materiál netvoří položky podléhající povinnosti mlčenlivosti, vyloučený materiál nebo materiál podléhající zvláštnímu druhu řízení a materiál takové položky nebo materiál ani neobsahuje a v) bez příkazu by nebylo možné dosáhnout vstupu. V druhém případě článek 18 umožňuje policistovi prohledat prostory osoby zatčené pro závažný trestný čin s cílem hledat jiný materiál než materiál podléhající povinnosti mlčenlivosti, pokud má policista důvodné podezření, že v prostorách se nacházejí důkazy související s daným trestným činem nebo s jiným obdobným nebo propojeným trestným činem. Taková prohlídka musí být omezena na nalezení tohoto materiálu a musí být písemně povolena policistou v hodnosti nejméně inspektora, pokud není pro vyšetřování trestného činu nezbytná. V takovém případě musí být policista v hodnosti nejméně inspektora informován co nejdříve po provedení prohlídky. Musí být zaznamenány důvody prohlídky a důkazní prostředky. Kromě toho články 15 a 16 zákona o policii a důkazech v trestním řízení z roku 1984 stanoví zákonné záruky, které je třeba při podávání návrhu na vydání příkazu k domovní prohlídce dodržet. Článek 15 specifikuje požadavky týkající se získání povolení k domovní prohlídce (včetně obsahu návrhu podaného policistou a skutečnosti, že příkaz musí mimo jiné specifikovat právní předpis, podle kterého je vydán, a pokud je to možné, také předměty a osoby, které mají být hledány, a prostory, které mají být prohledány). Článek 16 upravuje, jak musí být prohlídka na základě příkazu provedena (například: čl. 16 odst. 5 stanoví, že policista vykonávající příkaz k domovní prohlídce poskytne uživateli prostor kopii tohoto příkazu; čl. 16 odst. 11 vyžaduje, aby byl příkaz po vykonání uchován po dobu dvanácti měsíců; čl. 16 odst. 12 poskytuje obyvateli prostor právo během této lhůty do příkazu nahlédnout, pokud bude chtít). Uvedené články pomáhají zajistit soulad s článkem 8 EÚLP (viz např. rozsudek ve věci Kent Pharmaceuticals v Director of the Serious Fraud Office [2002] EWHC 3023 (QB) v [30], Lord Woolf CJ). Nesplnění těchto záruk může vést k prohlášení prohlídky za nezákonnou (k příkladům patří rozsudek ve věci R (Brook) v Preston Crown Court [2018] EWHC 2024 (Admin), [2018] ACD 95; R (Superior Import / Export Ltd) v Revenue and Customs Commissioners [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115 a R (F) v Blackfriars Crown Court [2014] EWHC 1541 (Admin)). Články 15 a 16 zákona o policii a důkazech v trestním řízení z roku 1984 doplňuje kodex B tohoto zákona, což je kodex zásad, který upravuje výkon pravomoci policie provádět prohlídky prostor.

([186]) Například při vydávání příkazu k předání podle zákona o výnosech z trestné činnosti z roku 2002 by kromě nutnosti existence rozumných důvodů za účelem splnění podmínek stanovených v čl. 346 odst. 2 zákona o výnosech z trestné činnosti mělo existovat důvodné podezření, že daná osoba má v držení nebo pod kontrolou takto specifikovaný materiál a je pravděpodobné, že materiál má podstatnou hodnotu. Další požadavek týkající se vydání příkazu k předání stanoví, že musí existovat důvodná domněnka, že je ve veřejném zájmu, aby byl materiál předán nebo aby byl k němu umožněn přístup, s ohledem na: a) pravděpodobný přínos pro vyšetřování, který přinese předání materiálu, a b) okolnosti, za nichž osoba, kterou návrh uvádí jako osobu, jež má zřejmě daný v materiál v držení nebo pod kontrolou, tyto informace drží. Podobně soud, který posuzuje návrh na příkaz k předání podle přílohy 1 zákona o policii a důkazech v trestním řízení z roku 1984, musí být přesvědčen, že jsou splněny konkrétní podmínky. Příloha 1 zákona o policii a důkazech v trestním řízení zejména stanoví dva samostatné alternativní soubory podmínek, z nichž jeden musí být splněn, nežli může soudce příkaz k předání vydat. První soubor vyžaduje, aby měl soudce rozumné důvody se domnívat, že i) byl spáchán závažný trestný čin; ii) materiál hledaný v prostorách je tvořen materiálem nebo obsahuje materiál, který podléhá zvláštnímu druhu řízení, ale není vyloučeným materiálem; iii) je pravděpodobné, že materiál bude mít pro vyšetřování podstatnou hodnotu, ať už samostatně, nebo společně s jinými materiály, iv) a je pravděpodobné, že bude relevantním důkazem; v) byly provedeny pokusy o získání materiálu jiným způsobem, nebo nebyly provedeny, neboť by musely selhat, a vi) po zvážení přínosu pro vyšetřování a okolností, za kterých jednotlivec materiál drží, je ve veřejném zájmu, aby byl materiál předán nebo aby byl k němu poskytnut přístup. Druhý soubor podmínek vyžaduje, aby: i) v prostorách byl materiál, který je tvořen materiálem podléhajícím zvláštnímu druhu řízení nebo vyloučeným materiálem; ii) bylo možné vydat příkaz k domovní prohlídce týkající se tohoto materiálu, kdyby nebylo zákazu prohlídek podle právních předpisů přijatých před zákonem o policii a důkazech v trestním řízení pro materiál podléhající zvláštnímu druhu řízení, vyloučený materiál nebo materiál podléhající povinnosti mlčenlivosti, a iii) bylo by vhodné tak učinit.

([187]) Soudní přezkum je soudní řízení, v němž lze napadnout rozhodnutí orgánu veřejné moci u Vrchního soudu. Soudy napadené rozhodnutí „přezkoumají" a s ohledem na pojmy/zásady veřejného práva rozhodnou, zda je prokazatelné, že rozhodnutí má právní vady. Základními důvody pro soudní přezkum jsou zejména protiprávnost, iracionalita, procesní vady, legitimní očekávání a lidská práva. V návaznosti na úspěšný soudní přezkum může soud nařídit řadu různých opravných prostředků; nejběžnějším z nich je prohlášení neplatnosti (kterým se anuluje nebo ruší původní rozhodnutí – tj. rozhodnutí o vydání příkazu k domovní prohlídce) a za určitých okolností to může zahrnovat i přiznání finanční náhrady. Další podrobnosti k soudnímu přezkumu ve Spojeném království jsou k dispozici v publikaci Ministerstva spravedlnosti „Judge Over Your Shoulder – a guide to good decision-making" (Soudce za zády – průvodce dobrým rozhodováním), k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf

níž musí být účely zpracování určité, výslovně vyjádřené a legitimní ([188]) a osobní údaje zpracovávané příslušným orgánem musí být pro tento účel důležité a omezené na nezbytný rozsah ([189]).

3.2.1.2 Vyšetřovací pravomoci pro účely vymáhání práva

(139) Pouze za účelem prevence nebo odhalování závažných trestných činů ([190]) mohou určité donucovací orgány, například Národní kriminální agentura nebo policejní ředitel ([191]), použít cílené vyšetřovací pravomoci podle zákona o vyšetřovacích pravomocích z roku 2016. V takovém případě se kromě záruk stanovených částí 3 zákona o ochraně údajů z roku 2018 použijí i záruky stanovené zákonem o vyšetřovacích pravomocích z roku 2016. Zvláštní vyšetřovací pravomoci, které mohou tyto donucovací orgány využít, zahrnují: cílené odposlechy (část 2 zákona o vyšetřovacích pravomocích z roku 2016), získávání komunikačních údajů (část 3 zákona o vyšetřovacích pravomocích z roku 2016), uchovávání komunikačních údajů (část 4 zákona o vyšetřovacích pravomocích z roku 2016) a cílený vzdálený síťový přístup k zařízení (část 5 zákona o vyšetřovacích pravomocích z roku 2016). Odposlech zahrnuje získávání obsahu komunikace ([192]), zatímco získávání a uchovávání komunikačních údajů není zaměřeno na získání obsahu komunikace, ale na odpovědi na otázky „kdo“, „kdy“, „kde“ a „jak“ ve vztahu k dané komunikaci. Zahrnuje to například čas a dobu trvání komunikace, telefonní číslo nebo e-mailovou adresu původce a příjemce komunikace a někdy i umístění zařízení, z nichž byla komunikace uskutečněna, účastníka telefonní služby nebo vyúčtování rozepsané na jednotlivé položky ([193]). Vzdálený síťový přístup k zařízení je soubor technik používaných k získávání různých dat ze zařízení, která zahrnují počítače, tablety a chytré telefony, jakož i kabely, vodiče a paměťová zařízení ([194]).

(140) Pravomoci cíleného odposlechu lze použít i v případě, že „je to nezbytné pro účely provedení ustanovení nástroje EU pro vzájemnou pomoc nebo mezinárodní dohody o vzájemné pomoci“ (tzv. příkaz ke vzájemné pomoci ([195])). Příkazy ke vzájemné pomoci se vydávají pouze ve vztahu k odposlechu, nikoli k získávání komunikačních údajů nebo vzdálenému síťovému přístupu k zařízení. Tyto cílené pravomoci upravuje zákon o vyšetřovacích pravomocích z roku 2016 ([196]), který společně se zákonem o úpravě vyšetřovacích pravomocí z roku 2000 pro Anglii, Wales a Severní Irsko a zákonem o úpravě vyšetřovacích pravomocí (Skotsko) z roku 2000 pro Skotsko stanoví právní základ a stanoví příslušná omezení a záruky pro použití těchto pravomocí. Zákon o vyšetřovacích pravomocích z roku 2016 rovněž stanoví režim pro použití hromadných vyšetřovacích pravomocí, donucovací orgány však tyto pravomoci nemají (mohou je využívat pouze zpravodajské služby) ([197]).

([188]) Ustanovení čl. 36 odst. 1 britského zákona o ochraně údajů z roku 2018.

([189]) Článek 37 britského zákona o ochraně údajů z roku 2018.

([190]) Ustanovení čl. 263 odst. 1 zákona o vyšetřovacích pravomocích z roku 2016 uvádí, že „závažným trestným činem“ se rozumí trestný čin, u něhož lze důvodně předpokládat, že dospělá osoba, která dosud nebyla soudně trestána, bude odsouzena k trestu odnětí svobody v délce nejméně tří let, nebo dané jednání zahrnuje použití násilí, vede k podstatnému finančnímu zisku nebo se ho účastní velký počet osob. Kromě toho pro účely získávání komunikačních údajů stanoví čl. 87 odst. 10B části 4 zákona o vyšetřovacích pravomocích z roku 2016, že „závažným trestným činem“ se rozumí trestný čin, za který lze uložit trest odnětí svobody v délce nejméně dvanácti měsíců, nebo trestný čin spáchaný osobou, která není fyzickou osobou, nebo trestný čin, jehož nedílnou součástí je odeslání komunikačního sdělení nebo porušení práva na soukromí osoby.

([191]) Konkrétně mohou návrh na cílený příkaz k odposlechu podat tyto donucovací orgány: generální ředitel Národní kriminální agentury (Director General of the National Crime Agency), ředitel Metropolitní policie (Commissioner of Police of the Metropolis), ředitel policie v Severním Irsku (Chief Constable of the Police Service of Northern Ireland), ředitel policie ve Skotsku (Chief Constable of the Police Service of Scotland), ředitel daňové a celní správy (Commissioner for Her Majesty's Revenue and Customs), náčelník Obranné zpravodajské služby (Chief of Defence Intelligence) a osoba, která je příslušným orgánem země nebo území Spojeného království pro účely nástroje EU pro vzájemnou pomoc nebo dohody o mezinárodní vzájemné pomoci (čl. 18 odst. 1 zákona o vyšetřovacích pravomocích z roku 2016).

([192]) Viz článek 4 zákona o vyšetřovacích pravomocích z roku 2016.

([193]) Viz čl. 261 odst. 5 zákona o vyšetřovacích pravomocích z roku 2016 a kodex zásad pro hromadné získávání komunikačních údajů (Code of Practice on Bulk Acquisition of Communications Data) k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, článek 2.9.

([194]) Code of Practice on Equipment Interference (kodex zásad pro vzdálený síťový přístup k zařízení), k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, bod 2.2.

([195]) Příkaz ke vzájemné pomoci opravňuje orgán Spojeného království poskytnout pomoc orgánu mimo území Spojeného království při odposlechu a zpřístupnění zachyceného materiálu tomuto orgánu v souladu s mezinárodním nástrojem vzájemné pomoci (čl. 15 odst. 4 zákona o vyšetřovacích pravomocích z roku 2016).

([196]) Zákon o vyšetřovacích pravomocích z roku 2016 (viz: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) nahradil různé zákony týkající se odposlechu komunikace, vzdáleného síťového přístupu k zařízení a získávání komunikačních údajů, zejména část I zákona o úpravě vyšetřovacích pravomocí z roku 2000, které stanovil předchozí obecný legislativní rámec pro použití vyšetřovacích pravomocí donucovacími a vnitrostátními bezpečnostními orgány.

([197]) Ustanovení čl. 138 odst. 1, čl. 158 odst. 1, čl. 178 odst. 1, čl. 199 odst. 1 zákona o vyšetřovacích pravomocích z roku 2016.

(141) K výkonu těchto pravomocí musí orgány získat příkaz ([198]) vydaný příslušným orgánem ([199]) a schválený nezávislým soudním komisařem ([200]) (tzv. postup dvojitého zámku). Získání takového příkazu podléhá testu nezbytnosti a přiměřenosti ([201]). Jelikož jsou tyto cílené vyšetřovací pravomoci poskytované zákonem o vyšetřovacích pravomocích z roku 2016 stejné jako ty, které mají k dispozici národní bezpečnostní služby, podrobně se podmínkám, omezením a zárukám použitelným na tyto pravomoci věnuje část týkající se přístupu a používání osobních údajů orgány veřejné moci Spojeného království pro účely národní bezpečnosti (viz 177. bod odůvodnění a násl.).

3.2.2 *Další použití shromážděných informací*

(142) Sdílení údajů donucovacím orgánem s jiným orgánem pro jiné účely, než pro které byly údaje původně shromážděny (tzv. další sdílení), podléhá určitým podmínkám.

(143) Obdobně jako čl. 4 odst. 2 směrnice (EU) 2016/680 umožňuje čl. 36 odst. 3 zákona o ochraně údajů z roku 2018, aby osobní údaje shromážděné příslušným orgánem pro účely vymáhání práva mohly být dále zpracovávány (ať už původním správcem, nebo jiným správcem) pro jakýkoli jiný účel vymáhání práva, pokud je správce ze zákona oprávněn zpracovávat údaje pro tento jiný účel a zpracování je nezbytné a přiměřené tomuto účelu ([202]). V tomto případě se na zpracování prováděné přijímajícím orgánem vztahují všechny záruky stanovené v části 3 zákona o ochraně údajů z roku 2018 uvedené ve 122. a 124. bodě odůvodnění.

(144) V právním řádu Spojeného království takové další sdílení výslovně umožňují různé zákony. Zejména i) zákon o digitální ekonomice z roku 2017 umožňuje sdílení mezi orgány veřejné moci z několika důvodů, například v případě jakéhokoli podvodu vůči veřejnému sektoru, který by pro orgány veřejné moci znamenal ztrátu nebo riziko ztráty ([203]), nebo v případě dluhu vůči orgánu veřejné moci nebo Koruně ([204]); ii) zákon o trestní činnosti a soudech z roku 2013, který umožňuje sdílení informací s Národní kriminální agenturou (National Crime Agency) ([205]) pro účely boje proti závažné a organizované trestné činnosti, jejího vyšetřování a stíhání; iii) zákon o závažné trestné činnosti z roku 2007, který orgánům veřejné moci umožňuje zpřístupňovat informace organizacím pro boj proti podvodům za účelem předcházení podvodům ([206]).

(145) Tyto zákony výslovně stanoví, že sdílení informací by mělo být v souladu se zásadami, které stanoví zákon o ochraně údajů z roku 2018. Kromě toho College of Policing (instituce pro vzdělávání policistů) vydala povolený odborný postup pro sdílení informací ([207]), který má policii pomoci při

([198]) Kapitola 2 části 2 zákona o vyšetřovacích pravomocích z roku 2016 stanoví omezený počet případů, kdy lze odposlech provádět bez příkazu. To zahrnuje: odposlech se souhlasem odesílatele nebo příjemce, odposlech pro správní nebo donucovací účely, odposlech probíhající v určitých institucích (věznice, psychiatrické léčebny a zajišťovací zařízení pro přistěhovalce), jakož i odposlech prováděný v souladu s příslušnou mezinárodní dohodou.

([199]) Ve většině případů je orgánem, který vydává příkazy podle zákona o vyšetřovacích pravomocích z roku 2016, ministr, přičemž skotští ministři jsou oprávněni vydávat příkazy k cílenému odposlechu, příkaz ke vzájemné pomoci a příkazy k cílenému vzdálenému síťovému přístupu k zařízení, pokud se osoby nebo prostory, u nichž má být prováděn odposlech, a zařízení, do něhož se má vstupovat, nacházejí ve Skotsku (viz články 22 a 103 zákona o vyšetřovacích pravomocích z roku 2016). V případě cíleného vzdáleného síťového přístupu k zařízení může příkaz vydat ředitel donucovacího orgánu (uvedený v části 1 a části 2 přílohy 6 zákona o vyšetřovacích pravomocích z roku 2016), a to za podmínek stanovených v článku 106 tohoto zákona.

([200]) Soudní komisaři jsou nápomocni komisaři pro kontrolu vyšetřovacích pravomocí, což je nezávislý orgán, který vykonává funkce dohledu nad využíváním vyšetřovacích pravomocí zpravodajskými službami (další podrobnosti viz (162). bod odůvodnění a násl.).

([201]) Viz zejména články 19 a 23 zákona o vyšetřovacích pravomocích z roku 2016.

([202]) Ustanovení čl. 36 odst. 3 zákona o ochraně údajů z roku 2018.

([203]) Článek 56 zákona o digitální ekonomice z roku 2017, k dispozici na této adrese: https://www.legislation.gov.uk/ukpga/2017/30/section/56

([204]) Článek 48 zákona o digitální ekonomice z roku 2017.

([205]) Článek 7 zákona o trestné činnosti a soudech z roku 2013, k dispozici na této adrese: https://www.legislation.gov.uk/ukpga/2013/22/section/7

([206]) Článek 68 zákona o závažné trestné činnosti z roku 2007, k dispozici na této adrese: https://www.legislation.gov.uk/ukpga/2007/27/contents

([207]) Authorised Professional Practice on Information Sharing (povolený odborný postup pro sdílení informací), k dispozici na této adrese: https://www.app.college.police.uk/app-content/information-management/sharing-police-information

plnění jejích povinností v oblasti ochrany údajů podle britského nařízení GDPR, zákona o ochraně údajů a zákona o lidských právech z roku 1998. Soulad sdílení s platným právním rámcem pro ochranu údajů samozřejmě podléhá soudnímu přezkumu ([208]).

(146) Kromě toho, podobně jako článek 9 směrnice (EU) 2016/680 stanoví zákon o ochraně údajů z roku 2018, že osobní údaje shromážděné pro jakékoli účely vymáhání práva mohou být zpracovávány za účelem, který nespočívá ve vymáhání práva, pokud je zpracování povoleno zákonem ([209]).

(147) Tento typ sdílení zahrnuje dva scénáře: 1) když orgán činný v trestním řízení sdílí údaje s donucovacím orgánem činným v oblasti mimo trestní řízení, který není zpravodajskou službou (např. s finančním nebo daňovým úřadem, úřadem pro hospodářskou soutěž, úřadem pro péči o mládež atd.); 2) když orgán činný v trestním řízení sdílí údaje se zpravodajskou službou. V prvním scénáři bude zpracování osobních údajů spadat do oblasti působnosti britského nařízení GDPR, jakož i části 2 zákona o ochraně údajů z roku 2018. Ve 12. až 111. bodě odůvodnění posoudila Komise záruky poskytované britským nařízením GDPR a částí 2 zákona o ochraně údajů z roku 2018 a dospěla k závěru, že Spojené království zajišťuje odpovídající úroveň ochrany osobních údajů předávaných v rámci oblasti působnosti nařízení (EU) 2016/679 z Evropské unie do Spojeného království.

(148) Ve druhém scénáři, pokud jde o sdílení údajů, které shromáždil orgán činný v trestním řízení, se zpravodajskou službou pro účely národní bezpečnosti, je právním základem, který takové sdílení povoluje, článek 19 zákona o boji proti terorismu z roku 2008 ([210]). Podle tohoto zákona může kterákoli osoba poskytovat informace kterékoli ze zpravodajských služeb za účelem výkonu kterékoli z funkcí této služby, včetně „národní bezpečnosti".

(149) Pokud jde o podmínky, za nichž lze údaje sdílet pro účely národní bezpečnosti, zákon o zpravodajských službách ([211]) a zákon o Bezpečnostní službě ([212]) omezují možnost zpravodajských služeb získávat údaje na to, co je nezbytné k výkonu jejich zákonem stanovených funkcí. Donucovací orgány, které chtějí sdílet údaje se zpravodajskými službami, budou muset kromě zákonných funkcí agentur stanovených zákonem o zpravodajských službách a zákonem o Bezpečnostní službě ([213]) zohlednit řadu faktorů/omezení. Článek 20 zákona o boji proti terorismu z roku 2008 objasňuje, že jakékoli sdílení údajů podle článku 19 musí splňovat i právní předpisy o ochraně údajů; což znamená, že se použijí všechna omezení a požadavky podle části 3 zákona o ochraně údajů z roku 2018. Kromě toho vzhledem k tomu, že příslušnými orgány jsou orgány veřejné moci pro účely zákona o lidských právech z roku 1998, musí tyto orgány zajistit, aby jednaly v souladu s právy podle úmluvy, včetně článku 8 EÚLP. Tato omezení zajišťují, že veškeré sdílení údajů mezi donucovacími orgány a zpravodajskými službami bude v souladu s právními předpisy o ochraně údajů a EÚLP.

([208]) Viz například věc M, R v the Chief Constable of Sussex Police [2019] EWHC 975 (Admin), v níž byl Vrchní soud požádán, aby posoudil sdílení údajů mezi policií a Business Crime Reduction Partnership (BCRP), organizací zmocněnou ke správě programů vyloučení vstupu, které zakazují osobám vstup do komerčních prostor členů organizace. Soud přezkoumal sdílení údajů, které se uskutečnilo na základě dohody za účelem ochrany veřejnosti a předcházení trestné činnosti, a dospěl k závěru, že většina aspektů sdílení údajů byla zákonná, s výjimkou některých citlivých informací sdílených mezi policií a organizací BCRP. Jiným příkladem je rozsudek ve věci Cooper v NCA [2019] EWCA Civ 16, v němž odvolací soud potvrdil sdílení údajů mezi policií a Agenturou pro závažnou trestnou činnost (Serious Organised Crime Agency), donucovacím orgánem, který je nyní součástí Národní kriminální agentury.

([209]) Ustanovení čl. 36 odst. 4 zákona o ochraně údajů z roku 2018.

([210]) Zákon o boji proti terorismu z roku 2008, k dispozici na této adrese: https://www.legislation.gov.uk/ukpga/2008/28/section/19

([211]) Zákon o zpravodajských službách z roku 1994, k dispozici na této adrese: https://www.legislation.gov.uk/ukpga/1994/13/contents

([212]) Zákon o Bezpečnostní službě z roku 1989, k dispozici na této adrese: https://www.legislation.gov.uk/ukpga/1989/5/contents

([213]) Ustanovení čl. 2 odst. 2 zákona o zpravodajských službách z roku 1994 stanoví, že „náčelník zpravodajské služby odpovídá za účinnost této služby a je jeho povinností zajistit a) aby existovala opatření, jež zajistí, že zpravodajská služba nebude získávat žádné informace ve větší míře, než jaká je nezbytná pro řádné plnění funkcí služby, a že služba nebude zpřístupňovat žádné informace, pokud to nebude nezbytné: i) pro tento účel; ii) v zájmu národní bezpečnosti; iii) za účelem prevence nebo odhalování závažné trestné činnosti nebo iv) pro účely trestního řízení, a b) aby zpravodajská služba neprováděla žádné kroky k prosazování zájmů žádné politické strany ve Spojeném království", přičemž čl. 2 odst. 2 zákona o Bezpečnostní službě z roku 1989 stanoví, že „generální ředitel odpovídá za účinnost služby a je jeho povinností zajistit, aby a) existovala opatření, jež zajistí, že služba nebude získávat žádné informace ve větší míře, než jaká je nezbytná pro řádné plnění funkcí služby, a nebude zpřístupňovat žádné informace, pokud to nebude nezbytné pro tento účel nebo pro účely prevence nebo odhalování] závažné trestné činnosti nebo pro účely trestního řízení], a b) aby služba neprováděla žádné kroky k prosazování zájmů žádné politické strany ve Spojeném království a c) aby existovala ujednání dohodnutá s generálním ředitelem Národní kriminální agentury, pokud jde o koordinaci činností služby podle čl. 1 odst. 4 tohoto zákona s činnostmi policejních sil, Národní kriminální agentury a ostatních donucovacích orgánů".

(150) Pokud příslušný orgán hodlá sdílet osobní údaje zpracovávané podle části 3 zákona o ochraně údajů z roku 2018 s donucovacími orgány třetí země, platí zvláštní požadavky ([214]). Zejména se tato předání mohou uskutečnit tehdy, jsou-li založena na nařízeních o odpovídající ochraně vydaných ministrem, nebo pokud taková nařízení neexistují, musí být zajištěny vhodné záruky. Článek 75 zákona o ochraně údajů z roku 2018 stanoví, že vhodné záruky jsou zavedeny tehdy, pokud jsou stanoveny právním nástrojem závazným pro zamýšleného příjemce nebo pokud správce po posouzení všech okolností souvisejících s předáním tohoto druhu osobních údajů třetí zemi nebo mezinárodní organizaci dojde k závěru, že k ochraně údajů existují vhodné záruky.

(151) Pokud předání není založeno na nařízení o odpovídající ochraně, může k němu dojít pouze za určitých specifikovaných okolností, označovaných jako „zvláštní okolnosti" ([215]). Ty existují v případě, že je předání nezbytné: a) k ochraně životně důležitých zájmů subjektu údajů nebo jiné osoby; b) k ochraně oprávněných zájmů subjektu údajů; c) aby se zabránilo bezprostřednímu a závažnému ohrožení veřejné bezpečnosti v některém členském státě nebo třetí zemi; d) v jednotlivých případech pro jakékoli účely vymáhání práva nebo e) v jednotlivých případech pro právní účely (například v souvislosti se soudním řízením nebo s cílem získat právní poradenství). Lze upozornit, že písmena d) a e) se nepoužijí, pokud práva a svobody subjektu údajů převažují nad veřejným zájmem na předání. Tento soubor okolností odpovídá konkrétním situacím a podmínkám, které lze kvalifikovat jako „výjimky" podle článku 38 směrnice (EU) 2016/680.

(152) Kromě toho, pokud je do třetí země předáván materiál získaný donucovacími orgány na základě příkazu, který povoluje použití odposlechu nebo vzdáleného síťového přístupu k zařízení, ukládá zákon o vyšetřovacích pravomocích z roku 2016 další záruky. Zejména je takové zpřístupnění, definované jako „zahraniční zpřístupnění", povoleno za předpokladu, že vydávající orgán má za to, že existuje zvláštní vhodný režim, který omezuje počet osob, kterým jsou údaje zpřístupněny, rozsah, v jakém je jakýkoli materiál poskytnut nebo zpřístupněn, stejně jako rozsah, v jakém je jakákoli část materiálu kopírována, a počet pořízených kopií. Vydávající orgán se také může domnívat, že jsou zapotřebí vhodná opatření k zajištění toho, aby každá kopie jakékoli části tohoto materiálu byla zničena, jakmile pominou příslušné důvody pro její uchování (pokud již nebyla zničena dříve) ([216]).

(153) A v neposlední řadě by se v budoucnu mohly uskutečňovat zvláštní formy dalšího předávání ze Spojeného království do Spojených států na základě „Dohody mezi vládou Spojeného království Velké Británie a Severního Irska a vládou Spojených států amerických o přístupu k elektronickým údajům za účelem boje proti závažné trestné činnosti (dále jen „dohoda mezi Spojeným královstvím a USA" nebo „dohoda") ([217]), která byla uzavřena v říjnu 2019 ([218]). Zatímco dohoda mezi Spojeným královstvím a USA dosud nevstoupila v platnost v době přijetí tohoto rozhodnutí, její předvídatelný vstup v platnost může ovlivnit další předávání údajů, které byly nejprve předány do Spojeného království na základě tohoto rozhodnutí, do USA. Přesněji řečeno, jakmile dohoda vstoupí v platnost, mohly by údaje předané z EU poskytovatelům služeb ve Spojeném království podléhat příkazům k předání elektronických důkazů vydaným příslušnými donucovacími orgány v USA, které jsou na základě uvedené dohody použitelné ve Spojeném království. Z těchto důvodů je pro toto rozhodnutí významné posouzení podmínek a záruk, za nichž lze takové příkazy vydávat a vykonávat.

([214]) Viz kapitola 5 části 3 zákona o ochraně údajů z roku 2018.

([215]) Článek 76 zákona o ochraně údajů z roku 2018.

([216]) Články 54 a 130 zákona o vyšetřovacích pravomocích z roku 2016. Vydávající orgány musí u materiálu předávaného zahraničním orgánům posoudit nezbytnost uložení zvláštních ochranných opatření, aby se ujistily, že pro údaje platí záruky týkající se uchovávání, ničení a zpřístupňování údajů obdobné těm, které ukládají články 53 a 129 zákona o vyšetřovacích pravomocích z roku 2016.

([217]) Dohoda mezi vládou Spojeného království Velké Británie a Severního Irska a vládou Spojených států amerických o přístupu k elektronickým údajům za účelem boje proti závažné trestné činnosti, k dispozici na této adrese: 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]) Toto je první dohoda dosažená podle zákona USA o objasnění zákonného zahraničního použití údajů (Clarifying Lawful Overseas Use of Data (CLOUD)). Zákon CLOUD je americký federální zákon, který byl přijat dne 23. března 2018 a prostřednictvím novely zákona o uložených komunikacích z roku 1986 objasňuje, že poskytovatelé služeb v USA jsou povinni plnit v USA vydané příkazy ke zpřístupnění obsahových a neobsahových údajů bez ohledu na to, kde jsou tyto údaje uloženy. Zákon CLOUD také umožňuje uzavírat se zahraničními vládami dohody o provádění, na jejichž základě by američtí poskytovatelé služeb mohli poskytovat obsahové údaje přímo těmto zahraničním vládám (znění zákona CLOUD je k dispozici na této adrese: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf)

(154) V tomto ohledu je třeba upozornit, že zaprvé je z hlediska věcné působnosti dohoda použitelná pouze na trestné činy, za které je možné uložit trest odnětí svobody v délce nejméně tří let (definované jako „závažné trestné činy“) ([219]), včetně „teroristické činnosti“. Zadruhé lze podle této dohody získat údaje zpracovávané v jiné jurisdikci pouze na základě „příkazu […] podléhajícího přezkumu nebo dohledu podle vnitrostátního práva vydávající strany zajištěného soudem, soudcem, smírčím soudcem nebo jiným nezávislým orgánem před řízením ve věci výkonu nařízení nebo v průběhu takového řízení“ ([220]). Zatřetí se musí jakýkoli příkaz „opírat o požadavky na přiměřené odůvodnění založené na pojmenovatelných a důvěryhodných skutečnostech, podrobnosti, zákonnosti a závažnosti, pokud jde o vyšetřované jednání“ ([221]) a musí „být zaměřen na konkrétní účty, jakož i určovat konkrétní osobu, účet, adresu nebo osobní zařízení nebo jakýkoli jiný specifický identifikátor“ ([222]). Začtvrté jsou údaje získané v rámci této dohody předmětem ochranných opatření rovnocenných zvláštním zárukám, která poskytuje tzv. zastřešující dohoda mezi EU a USA ([223]) (komplexní dohoda o ochraně údajů uzavřená v prosinci 2016 mezi EU a USA, která stanoví záruky a práva týkající se předávání údajů v oblasti spolupráce při vymáhání práva), jež jsou do této dohody obdobně začleněna odkazem, a zejména mají zohlednit specifickou povahu těchto předání (tj. předání od soukromých hospodářských subjektů donucovacím orgánům, nikoli předání mezi donucovacími orgány) ([224]). Dohoda mezi Spojeným královstvím a USA výslovně stanoví, že ochranná opatření rovnocenná těm, která poskytuje zastřešující dohoda mezi EU a USA, se použijí „na všechny osobní údaje předané v rámci výkonu příkazů, které jsou předmětem této dohody, aby zajistila rovnocennou ochranu“ ([225]).

(155) Údaje předané orgánům USA podle dohody mezi Spojeným královstvím a USA by proto měly požívat ochrany poskytované nástrojem práva EU, a to s nezbytnými úpravami, které mají odrážet povahu dotčených předání. Orgány Spojeného království dále potvrdily, že ochranná opatření podle zastřešující dohody se budou vztahovat na všechny osobní údaje předané nebo uchovávané na základě této dohody, bez ohledu na povahu nebo druh dožadujícího orgánu (např. federální i státní donucovací orgány v USA), ve všech případech musí být tudíž poskytována rovnocenná ochrana. Orgány Spojeného království však rovněž vysvětlily, že podrobnosti konkrétního provádění záruk ochrany údajů jsou dosud předmětem jednání mezi Spojeným královstvím a USA. V souvislosti s rozhovory s útvary Evropské komise na téma tohoto rozhodnutí orgány Spojeného království potvrdily, že nechají dohodu vstoupit v platnost až poté, co se přesvědčí, že její provádění je v souladu s právními závazky, které jsou v ní stanoveny, včetně jasnosti ohledně dodržování standardů ochrany údajů, pokud jde o jakékoli údaje požadované podle této dohody. Jelikož případný vstup dohody v platnost může mít dopad na úroveň ochrany posuzovanou v tomto rozhodnutí, mělo by Spojené království Evropské komisi sdělit jakékoli informace a budoucí objasnění týkající se způsobu, jakým budou Spojené státy plnit své závazky vyplývající z dohody, jakmile bude toto objasnění k dispozici a v každém případě před vstupem dohody v platnost, aby bylo zajištěno řádné sledování tohoto rozhodnutí v souladu s čl. 45 odst. 4 nařízení (EU) 2016/679. Zvláštní pozornost bude věnována použití a přizpůsobení ochranných opatření v rámci zastřešující dohody pro konkrétní druhy předání, na které se vztahuje dohoda mezi Spojeným královstvím a USA.

(156) Obecněji bude jakýkoli relevantní vývoj, pokud jde o vstup dohody v platnost a její uplatňování, náležitě zohledněn v rámci nepřetržitého sledování tohoto rozhodnutí, a to i s ohledem na nezbytné důsledky, které budou vyvozeny v případě jakékoli známky toho, že již není zajištěna v zásadě rovnocenná úroveň ochrany.

3.2.3 *Dohled*

(157) V závislosti na pravomocích, které příslušné orgány používají při zpracování osobních údajů pro účely vymáhání práva (ať už podle zákona o ochraně údajů z roku 2018, nebo podle zákona o vyšetřovacích pravomocích z roku 2016), zajišťují dohled nad využíváním těchto pravomocí různé subjekty. Zejména na zpracování osobních údajů

([219]) Ustanovení čl. 1 odst. 14 dohody.
([220]) Ustanovení čl. 5 odst. 2 dohody.
([221]) Ustanovení čl. 5 odst. 1 dohody.
([222]) Ustanovení čl. 4 odst. 5 dohody. Pokud jde o odposlech v reálném čase, platí dodatečný a přísnější standard: příkazy musí být časově omezené na dobu, která nesmí být delší než doba přiměřeně nezbytná k dosažení účelů příkazu, a mohou být vydány pouze v případě, že stejné informace nelze rozumně získat méně rušivým způsobem (čl. 5 odst. 3 dohody).
([223]) Dohoda mezi Spojenými státy americkými a Evropskou unií o ochraně osobních informací v souvislosti s prevencí, vyšetřováním, odhalováním a stíháním trestných činů. Úř. věst. L 336, 10.12.2016, s. 3, k dispozici na této adrese: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN
([224]) Ustanovení čl. 9 odst. 1 dohody.
([225]) Ustanovení čl. 9 odst. 1 dohody.

dohlíží komisař pro informace, pokud zpracování spadá do oblasti působnosti části 3 zákona o ochraně údajů z roku 2018 ([226]). Nezávislý a soudní dohled nad využíváním vyšetřovacích pravomocí podle zákona o vyšetřovacích pravomocích z roku 2016 zajišťuje Úřad komisaře pro kontrolu vyšetřovacích pravomocí ([227]) (této části se věnují 250. až 255. bod odůvodnění). Kromě toho je další dohled zaručen ze strany parlamentu Spojeného království, jakož i jiných orgánů.

3.2.3.1 Dohled podle části 3 zákona o ochraně údajů z roku 2018

(158) Obecné funkce komisaře pro informace (jehož nezávislost a organizace jsou vysvětleny v 87. bodě odůvodnění), pokud jde o zpracování osobních údajů spadajících do oblasti působnosti části 3 zákona o ochraně údajů z roku 2018, jsou stanoveny v příloze 13 zákona o ochraně údajů z roku 2018. Hlavním úkolem Úřadu komisaře pro informace je sledovat a vymáhat část 3 zákona o ochraně údajů z roku 2018 a také zvyšovat povědomí veřejnosti, poskytovat doporučení parlamentu Spojeného království, vládě a dalším institucím a subjektům. V zájmu zachování nezávislosti soudnictví není komisař pro informace oprávněn vykonávat své funkce v souvislosti se zpracováním osobních údajů jednotlivcem, který jedná v rámci soudních pravomocí, nebo soudem či tribunálem jednajícím v rámci své soudní pravomoci. Za těchto okolností by funkce dohledu vykonávaly jiné orgány, jak je vysvětleno v 99. až 103. bodě odůvodnění.

(159) Pokud jde o zpracování osobních údajů, na které se použije část 3, má komisař obecné vyšetřovací, nápravné, povolovací a poradenské pravomoci. Komisař má zejména pravomoc oznamovat správci nebo zpracovateli údajné porušení části 3 zákona o ochraně údajů z roku 2018, vydávat varování nebo napomenutí správci nebo zpracovateli, který porušil ustanovení části 3 zákona, jakož i z vlastního podnětu nebo na žádost vydávat pro parlament Spojeného království, vládu nebo jiné instituce a subjekty, jakož i pro veřejnost stanoviska k jakékoli otázce týkající se ochrany osobních údajů ([228]).

(160) Kromě toho má komisař pravomoc vydávat výzvy k podání informací ([229]), oznámení o posouzení ([230]) a oznámení o vymáhání ([231]), jakož i pravomoc získat přístup k dokumentům správců a zpracovatelů, vstupovat do jejich prostor ([232]) a udělovat správní pokuty formou oznámení o sankci ([233]). Politika regulačních opatření Úřadu komisaře pro informace stanoví okolnosti, za nichž komisař vydává výzvy k podání informací, oznámení o posouzení, vymáhání a o sankci ([234]) (viz také 93. bod odůvodnění a 101.–102. bod odůvodnění směrnice (EU) 2016/680 týkající se rozhodnutí o odpovídající ochraně).

(161) Podle posledních výročních zpráv Úřadu (2018–2019 ([235]), 2019–2020 ([236])) vedla komisařka pro informace řadu vyšetřování a přijala donucovací opatření v souvislosti se zpracováním údajů donucovacími orgány. Komisařka například provedla šetření a v říjnu 2019 zveřejnila stanovisko týkající se používání technologie rozpoznávání obličeje na veřejných místech pro účely vymáhání práva. Šetření se zaměřilo zejména na využití zařízení pro rozpoznávání obličeje v reálném čase policií jižního Walesu a metropolitní policií. Komisařka pro informace rovněž vyšetřovala tzv. matici gangů ([237]) metropolitní policie a zjistila řadu závažných porušení právních předpisů v oblasti ochrany údajů, která by mohla narušit důvěru veřejnosti v matici a ve způsob, jakým jsou údaje využívány. V listopadu 2018 vydala komisařka pro informace oznámení o vymáhání a metropolitní policie následně přijala potřebné kroky, aby zvýšila zabezpečení a odpovědnost zajistila přiměřené využívání údajů. Dalším příkladem opatření k vymáhání v této oblasti je pokuta ve výši 325 000 GBP,

([226]) Článek 116 zákona o ochraně údajů z roku 2018.
([227]) Viz zákon o vyšetřovacích pravomocích z roku 2016, zejména část 8 kapitoly 1.
([228]) Bod 2 přílohy 13 zákona o ochraně údajů z roku 2018.
([229]) Výzva nařizující správci a zpracovateli (a za určitých okolností kterékoli jiné osobě), aby poskytli nezbytné informace článek 142 zákona o ochraně údajů z roku 2018).
([230]) Oznámení umožňující provádět vyšetřování a audit, která mohou vyžadovat, aby správce nebo zpracovatel komisaři povolil vstoupit do určených prostor, nahlížet do dokumentů nebo zařízení nebo je kontrolovat, vyslechnout osoby zpracovávající osobní údaje jménem správce (článek 146 zákona o ochraně údajů z roku 2018).
([231]) Oznámení povolující výkon nápravných pravomocí, které vyžaduje, aby správci/zpracovatelé provedli určité kroky nebo aby se určitých kroků zdrželi (článek 149 zákona o ochraně údajů z roku 2018).
([232]) Článek 154 zákona o ochraně údajů z roku 2018.
([233]) Článek 155 zákona o ochraně údajů z roku 2018.
([234]) Politika regulačních opatření, viz poznámka pod čarou 96.
([235]) Výroční zpráva a účetní závěrka komisaře pro informace za období 2018–2019, viz poznámka pod čarou 101.
([236]) Výroční zpráva a účetní závěrka komisaře pro informace za období 2019–2020, viz poznámka pod čarou 82.
([237]) Databáze, která evidovala zpravodajské informace týkající se údajných členů gangů a obětí trestných činů souvisejících s gangy.

kterou komisařka uložila v květnu 2018 úřadu státního zástupce za ztrátu nezašifrovaných DVD obsahujících záznamy policejních výslechů. Komisařka pro informace rovněž vedla vyšetřování v rámci obecnějších témat, například v první polovině roku 2020 šetřila získávání údajů z mobilních telefonů pro policejní účely a zpracování údajů obětí ze strany policie. Kromě toho komisařka v současné době vyšetřuje případ, který zahrnuje přístup donucovacích orgánů k údajům uchovávaným subjektem soukromého sektoru, společností Clearview AI Inc ([238]).

(162) Vedle donucovacích pravomocí komisaře pro informace popsaných ve 160. a 161. bodě odůvodnění představují určitá porušení právních předpisů v oblasti ochrany údajů trestné činy, a proto mohou podléhat trestním sankcím (článek 196 zákona o ochraně údajů z roku 2018). Jde například o získávání, zpřístupňování nebo uchovávání osobních údajů bez souhlasu správce a zajišťování zpřístupnění osobních údajů jiné osobě bez souhlasu správce ([239]); opětovnou identifikaci údajů, které jsou osobními údaji, jež byly anonymizovány, bez souhlasu správce odpovědného za anonymizaci daných osobních údajů ([240]); záměrné maření výkonu pravomocí komisaře v souvislosti s inspekcí osobních údajů v souladu s mezinárodními závazky ([241]), vydávání nepravdivých prohlášení v reakci na výzvu k podání informací nebo ničení údajů v souvislosti s výzvami k podání informací a oznámeními o posouzení ([242]).

3.2.3.2 Další orgány dohledu v oblasti vymáhání trestního práva

(163) Vedle komisaře pro informace existuje několik orgánů dohledu v oblasti vymáhání trestního práva se zvláštními mandáty relevantními pro otázky ochrany údajů. K nim patří například komisař pro uchovávání a používání biometrických materiálů (dále jen „komisař pro biometriku“) ([243]) a komisař pro sledovací kamerové systémy ([244]).

3.2.3.3 Parlamentní dohled v oblasti vymáhání trestního práva

(164) Zvláštní parlamentní výbor pro vnitřní záležitosti (Home Affairs Select Committee) zajišťuje parlamentní dohled v oblasti vymáhání práva. Výbor se skládá z jedenácti poslanců parlamentu Spojeného království vybraných ze tří největších politických stran. Úkolem výboru je zkoumat výdaje, správu a politiku Ministerstva vnitra a přidružených veřejných subjektů, tj. včetně policie a Národní kriminální agentury, jejichž práci může výbor výhradně zkoumat ([245]).

([238]) Viz prohlášení Úřadu komisaře pro informace, k dispozici na této adrese: 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]) Článek 170 zákona o ochraně údajů z roku 2018.

([240]) Článek 171 zákona o ochraně údajů z roku 2018.

([241]) Ustanovení čl. 119 odst. 6 zákona o ochraně údajů z roku 2018.

([242]) Během účetního období od 1. dubna 2019 do 31. března 2020 vedla vyšetřování Úřadu komisaře pro informace ke čtyřem výstrahám a osmi trestním stíháním. Trestní stíhání v těchto případech bylo vedeno podle článku 55 zákona o ochraně údajů z roku 1998, článku 77 zákona o svobodě informací z roku 2000 a článku 170 zákona o ochraně údajů z roku 2018. V 75 % případů předložili obžalovaní přiznání viny, čímž zmizela nutnost zdlouhavých soudních řízení a s nimi spojených nákladů. (Výroční zpráva a účetní závěrka komisaře pro informace za období 2019/2020, viz poznámka pod čarou 87, s. 40).

([243]) Funkce komisaře pro biometriku byla zřízena zákonem o ochraně svobod z roku 2012 (viz: https://www.legislation.gov.uk/ukpga/2012/9/contents). Kromě jiných funkcí rozhoduje komisař pro biometriku také o tom, zda policie může či nesmí uchovávat záznamy profilu DNA a otisky prstů získané od osob, které byly zatčeny, ale nebyly obviněny ze závažného trestného činu (článek 63G zákona o policii a důkazech v trestním řízení z roku 1984). Komisař pro biometriku má navíc obecnou odpovědnost za kontrolu uchovávání a používání DNA a otisků prstů a uchovávání z důvodu národní bezpečnosti (čl. 20 odst. 2 zákona o ochraně svobod z roku 2012). Komisař pro biometriku je jmenován podle Kodexu pro jmenování do veřejných funkcí (kodex je k dispozici na adrese: https://www.gov.uk/government/publications/governance-code-for-public-appointments) a podmínky jeho jmenování jasně uvádějí, že jej z funkce může odvolat pouze ministr vnitra za přesně vymezeného souboru okolností; jedná se například o neplnění povinností komisaře po dobu tří měsíců, odsouzení za trestný čin nebo nedodržení podmínek jmenování komisaře.

([244]) Funkce komisaře pro sledovací kamerové systémy byla zřízena zákonem o ochraně svobod z roku 2012 a úlohou komisaře je podporovat dodržování kodexu zásad pro sledovací kamerové systémy; přezkoumávat fungování kodexu a poskytovat doporučení ministrům ohledně nutnosti případné změny kodexu. Komisař je jmenován podle stejných pravidel jako komisaři pro biometriku a má obdobné pravomoci, zdroje a ochranu proti odvolání.

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

(165) Výbor může v mezích svých pravomocí zvolit svůj vlastní předmět šetření, včetně konkrétních případů, pokud v dané věci není soudně rozhodnuto. Výbor může rovněž požadovat písemné a ústní důkazy od celé řady příslušných skupin a jednotlivců. Vypracovává zprávy o svých zjištěních a vydává doporučení vládě ([246]). Vláda by měla reagovat na každé z doporučení ve zprávě a musí odpovědět do 60 dnů ([247]).

(166) V oblasti sledování výbor rovněž vypracoval zprávu týkající se zákona o úpravě vyšetřovacích pravomocí z roku 2000 ([248]), která došla k závěru, že zákon o úpravě vyšetřovacích pravomocí z roku 2000 neodpovídá svému účelu. Zpráva výboru byla zohledněna při nahrazování významných částí zákona o úpravě vyšetřovacích pravomocí z roku 2000 zákonem o vyšetřovacích pravomocích z roku 2016. Úplný seznam šetření lze nalézt na webových stránkách výboru ([249]).

(167) Úkoly zvláštního parlamentního výboru pro vnitřní záležitosti ve Skotsku plní Justiční podvýbor pro činnost policie a v Severním Irsku Výbor pro spravedlnost ([250]).

3.2.4 *Soudní ochrana*

(168) Pokud jde o zpracování údajů donucovacími orgány, jsou k dispozici ochranné mechanismy podle části 3 zákona o ochraně údajů z roku 2018 a podle zákona o vyšetřovacích pravomocích z roku 2016, jakož i podle zákona o lidských právech z roku 1998.

(169) Tato série mechanismů poskytuje subjektům údajů účinné prostředky správní a soudní ochrany, které jim umožňují zejména zajistit jejich práva včetně práva na přístup k jejich osobním údajům nebo dosáhnout opravy nebo výmazu těchto údajů.

(170) Zaprvé má podle článku 165 zákona o ochraně údajů z roku 2018 subjekt údajů právo podat stížnost u komisaře pro informace, pokud má za to, že v souvislosti s jeho osobními údaji došlo k porušení části 3 zákona o ochraně údajů z roku 2018 ([251]). Komisař pro informace má pravomoc posoudit, jak správce a zpracovatel dodržují zákon o ochraně údajů z roku 2018, vyžadovat od nich, aby v případě nedodržení předpisů přijali nezbytné kroky, a ukládat pokuty.

([246]) Zvláštní parlamentní výbory včetně zvláštního parlamentního výboru pro vnitřní záležitosti podléhají jednacímu řádu Dolní sněmovny. Jednací řád tvoří pravidla schválená Dolní sněmovnou, která upravují způsob činnosti parlamentu. Působnost vybraných výborů je široká, přičemž čl. 152 odst. 1 jednacího řádu stanoví, že „zvláštní parlamentní výbory jsou jmenovány k přezkoumání výdajů, správy a politiky hlavních útvarů vlády, jak je uvedeno v článku 2 tohoto řádu, a souvisejících veřejných subjektů“. To umožňuje zvláštnímu parlamentnímu výboru pro vnitřní záležitosti zkoumat jakoukoli politiku, která přísluší Ministerstvu vnitra, což zahrnuje politiky (a související právní předpisy) týkající se vyšetřovacích pravomocí. Ustanovení čl. 152 odst. 4 jednacího řádu navíc objasňuje, že výbory mají různé pravomoci, včetně možnosti požadovat po osobách, aby poskytly důkazy nebo dokumenty týkající se konkrétní záležitosti, a vypracovávat zprávy. Probíhající a předchozí šetření výboru jsou k dispozici na této adrese https://committees.parliament.uk/committee/83/home-affairs-committee/.

([247]) Pravomoci zvláštního parlamentního výboru pro vnitřní záležitosti v Anglii a Walesu stanoví jednací řád Dolní sněmovny, který je k dispozici na této adrese: https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

([248]) K dispozici na této adrese: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm

([249]) K dispozici na této adrese: https://committees.parliament.uk/committee/83/home-affairs-committee

([250]) Jednací řád Justičního podvýboru pro činnost policie ve Skotsku je k dispozici na této adrese https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx a jednací řád Výboru pro spravedlnost v Severním Irsku je uveden na této adrese: http://www.niassembly.gov.uk/assembly-business/standing-orders/]

([251]) Poslední výroční zpráva Úřadu komisaře pro informace uvádí členění podle povahy obdržených a uzavřených stížností. Konkrétně počet přijatých stížností týkajících se „činnosti policie a trestního rejstříku“ činí 6 % z celkového počtu přijatých stížností (s nárůstem o 1 % ve srovnání s předchozím rozpočtovým rokem). Výroční zpráva rovněž ukazuje, že stížnosti týkající se žádostí subjektů údajů o přístup představují nejvyšší počet (46 % z celkového počtu stížností, což znamená nárůst o 8 % ve srovnání s předchozím účetním obdobím). (Výroční zpráva Úřadu komisaře pro informace za období 2019–2020, strana 55; viz poznámka pod čarou 88).

(171) Zadruhé zákon o ochraně údajů z roku 2018 stanoví právo na nápravu vůči komisaři pro informace, pokud komisař řádně nevyřídí stížnost subjektu údajů. Přesněji řečeno, pokud komisař „nedosahuje pokroku“ ([252]) ve věci stížnosti podané subjektem údajů, má stěžovatel přístup k soudnímu opravnému prostředku, neboť se může obrátit na tribunál prvního stupně ([253]), aby ten komisaři nařídil přijmout vhodná opatření k vyřízení stížnosti nebo informovat stěžovatele o pokroku ve věci stížnosti ([254]). Kromě toho se každá osoba, které je doručeno jedno z výše uvedených oznámení komisaře (výzva k podání informací, oznámení o posouzení, vymáhání nebo sankci), může odvolat k tribunálu prvního stupně. Pokud tribunál dospěje k závěru, že rozhodnutí komisaře není v souladu se zákonem, nebo že měl komisař pro informace uplatnit svou diskreční pravomoc jinak, musí tribunál vyhovět opravnému prostředku nebo vydat jiné oznámení nebo přijmout jiné rozhodnutí, které komisař pro informace mohl vydat nebo učinit ([255]).

(172) Zatřetí mohou jednotlivci soudní ochrany vůči správcům a zpracovatelům dosáhnout přímo u soudů. Zejména může subjekt údajů podle článku 167 zákona o ochraně údajů z roku 2018 podat u soudu žalobu pro porušení svých práv podle právních předpisů o ochraně údajů a soud může formou příkazu požádat správce, aby v zájmu souladu zpracování se zákonem o ochraně údajů z roku 2018 přijal jakékoli opatření (nebo se jakéhokoli opatření zdržel). Kromě toho podle článku 169 zákona o ochraně údajů z roku 2018 má každá osoba, která utrpěla škodu v důsledku porušení požadavku právních předpisů o ochraně údajů (včetně části 3 zákona o ochraně údajů z roku 2018), kromě britského nařízení GDPR, nárok na náhradu této škody od správce nebo zpracovatele, s výjimkou případů, kdy správce nebo zpracovatel prokáže, že správce nebo zpracovatel není nijak odpovědný za událost, která vedla ke vzniku škody. Škoda zahrnuje jak finanční ztrátu, tak nefinanční újmu, například utrpení.

(173) A konečně kterákoli osoba, která se domnívá, že její práva včetně práv na ochranu soukromí a ochranu údajů byla porušena orgány veřejné moci, může dosáhnout nápravy u soudů Spojeného království podle zákona o lidských právech z roku 1998 ([256]) a osoba, nevládní organizace a skupiny jednotlivců mohou po vyčerpání vnitrostátních opravných prostředků dosáhnout nápravy u Evropského soudu pro lidská práva, pokud jde o porušení práv zaručených Evropskou úmluvou o lidských právech ([257]) (viz 111. bod odůvodnění).

3.2.4.1 Ochranné mechanismy podle zákona o vyšetřovacích pravomocích z roku 2016

(174) Jednotlivci mohou dosáhnout nápravy v případě porušení zákona o vyšetřovacích pravomocích z roku 2016 u tribunálu pro kontrolu vyšetřovacích pravomocí. Možnosti nápravy dostupné podle zákona o vyšetřovacích pravomocích z roku 2016 jsou popsány ve 263. až 269. bodě odůvodnění níže.

([252]) Článek 166 zákona o ochraně údajů z roku 2018 uvádí výslovně tyto situace: a) komisař nepřijme vhodná opatření v reakci na stížnost; b) komisař neposkytne stěžovateli informace o pokroku při vyřizování stížnosti nebo o výsledku stížnosti před koncem tříměsíční lhůty od okamžiku, kdy komisař stížnost obdržel nebo c) pokud komisařovo posouzení stížnosti nebude během této lhůty uzavřeno, neposkytne stěžovateli tyto informace během následné tříměsíční lhůty.

([253]) Tribunál prvního stupně je soud příslušný projednávat opravné prostředky podané proti rozhodnutím regulačních orgánů státní správy. V případě rozhodnutí komisaře pro informace je příslušným soudním orgánem „obecný regulační senát“ se soudní pravomocí pro celé Spojené království.

([254]) Článek 166 zákona o ochraně údajů z roku 2018. Příkladem úspěšných žalob proti Úřadu komisaře pro informace u tribunálu je věc, v níž Úřadu komisaře pro informace potvrdil přijetí stížnosti od subjektu údajů, ale neuvedl, jaký postup hodná uplatnit, a proto mu bylo nařízeno, aby do 21 kalendářních dnů potvrdil, zda hodlá stížnosti vyšetřovat, a pokud ano, aby poté informoval stěžovatele o postupu vyšetřování nejméně každých 21 kalendářních dnů (rozsudek dosud není zveřejněn), a věc, kdy měl tribunál prvního stupně za to, že není jasné, zda odpověď Úřadu komisaře pro informace stěžovateli představovala řádný „výstup“ stížnosti (viz Susan Milne v. The Information Commissioner [2020], rozsudek k dispozici na této adrese: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf)

([255]) Články 162 a 163 zákona o ochraně údajů z roku 2018.

([256]) Viz například věc Brown v Commissioner of Police of the Metropolis & Anor [2019] EWCA Civ 1724, kdy byla přiznána náhrada škody ve výši 9 000 GBP podle zákona o ochraně údajů z roku 1998 a zákona o lidských právech z roku 1998 za nezákonné získání a neoprávněné použití osobních údajů, a věc R (on the application of Bridges) v Chief Constable of South Wales [2020] EWCA Civ 1058, kde odvolací soud prohlásil za nezákonné použití systému pro rozpoznávání obličeje policií ve Walesu, neboť bylo v rozporu s článkem 8 EÚLP a posouzení vlivu na ochranu osobních údajů, které vypracoval správce údajů, nebylo v souladu se zákonem o ochraně údajů z roku 2018.

([257]) Článek 34 Evropské úmluvy o lidských právech stanoví: „Soud může přijímat stížnosti od každé fyzické osoby, nevládní organizace nebo skupiny jednotlivců považujících se za oběti v důsledku porušení práv přiznaných Úmluvou a jejími Protokoly jednou z Vysokých smluvních stran. Vysoké smluvní strany se zavazují, že nebudou nijak bránit účinnému výkonu tohoto práva“.

3.3 **Přístup orgánů veřejné moci Spojeného království k osobním údajům pro účely národní bezpečnosti**

(175) V právním řádu Spojeného království jsou zpravodajskými službami zmocněnými ke shromažďování elektronických informací uchovávaných správci nebo zpracovateli z důvodů národní bezpečnosti v situacích, které jsou příslušné pro scénář odpovídající ochrany, Security Service (Bezpečnostní služba, MI5) ([258]), Secret Intelligence Service (Tajná zpravodajská služba, SIS) ([259]) a Government Communications Headquarters (Vládní ředitelství pro komunikace, GCHQ) ([260]) ([261]).

3.3.1 *Právní základy, omezení a záruky*

(176) Ve Spojeném království jsou pravomoci zpravodajských služeb stanoveny v zákoně o vyšetřovacích pravomocích z roku 2016 a v zákoně o úpravě vyšetřovacích pravomocí z roku 2000 a tyto zákony spolu se zákonem o ochraně údajů z roku 2018 vymezují věcnou a osobní působnost těchto pravomocí, jakož i omezení a záruky pro jejich použití. V následujících oddílech jsou tyto pravomoci, jakož i omezení a záruky, které se na ně vztahují, podrobně posouzeny.

3.3.1.1 Vyšetřovací pravomoci vykonávané v kontextu národní bezpečnosti

(177) Zákon o vyšetřovacích pravomocích z roku 2016 poskytuje právní rámec pro použití vyšetřovacích pravomocí, tj. pravomoc odposlechů, přístupu ke komunikačním údajům a vzdáleného síťového přístupu k zařízení. Zákon o vyšetřovacích pravomocích z roku 2016 zavádí obecný zákaz použití technik, které umožňují přístup k obsahu komunikace, přístup ke komunikačním údajům nebo vzdálený síťový přístup k zařízení bez zákonného oprávnění, a toto jednání kvalifikuje jako trestný čin ([262]). To se odráží ve skutečnosti, že použití těchto vyšetřovacích pravomocí je zákonné pouze tehdy, je-li prováděno na základě příkazu nebo povolení ([263]).

(178) Zákon o vyšetřovacích pravomocích z roku 2016 stanoví podrobná pravidla upravující oblast působnosti a použití každé z vyšetřovacích pravomocí, jakož i jejich zvláštní omezení a záruky. Platí různá pravidla v závislosti na druhu vyšetřovací pravomoci (odposlech komunikace, získávání a uchovávání komunikačních

([258]) (MI5) spadá do oblasti pravomoci ministra vnitra. Zákon o Bezpečnostní službě z roku 1989 stanovuje funkce MI5: ochrana národní bezpečnosti (včetně ochrany před hrozbou špionáže, terorismu a sabotáže, před činností agentů cizích mocností a akcemi určenými ke svržení nebo podkopání parlamentní demokracie politickými, průmyslovými nebo násilnými prostředky), ochrana hospodářského blahobytu Spojeného království proti vnějším hrozbám a podpora činnosti policejních sil a jiných donucovacích orgánů při prevenci a odhalování závažné trestné činnosti.

([259]) SIS spadá do pravomoci ministra zahraničí a její funkce jsou vymezeny v zákoně o zpravodajských službách z roku 1994. Těmito funkcemi je získávat a poskytovat informace týkající se jednání nebo úmyslů osob mimo Britské ostrovy a plnit další úkoly související s jednáním nebo úmysly těchto osob. Tyto funkce lze vykonávat pouze v zájmu národní bezpečnosti, v zájmu hospodářského blahobytu Spojeného království nebo na podporu prevence nebo odhalování závažné trestné činnosti.

([260]) GCHQ spadá do pravomoci ministra zahraničí a její funkce jsou vymezeny v zákoně o zpravodajských službách z roku 1994. Těmito funkcemi jsou a) monitorovat a využívat, popř. rušit elektromagnetické a jiné vyzařování a zařízení, které je zdrojem takového záření, získávat a poskytovat informace získané z takových vyzařování nebo zařízení nebo informace s nimi související a informace ze šifrovaných materiálů; b) poskytovat doporučení a pomoc v jazykové oblasti, včetně terminologie používané pro technické záležitosti a kryptografii a pro další záležitosti související s ochranou informací, a to ozbrojeným silám, vládě nebo jiným organizacím nebo osobám považovaným za způsobilé. Tyto funkce lze vykonávat pouze v zájmu národní bezpečnosti, v zájmu hospodářského blahobytu Spojeného království ve vztahu k jednání nebo úmyslům osob mimo Britské ostrovy nebo na podporu prevence nebo odhalování závažné trestné činnosti.

([261]) Dalšími veřejnými orgány vykonávajícími funkce související s národní bezpečností jsou Defence Intelligence (Obranná zpravodajská služba), National Security Council and Secretariat (Rada a sekretariát pro národní bezpečnost), Joint Intelligence Organisation (Společná zpravodajská organizace) a Joint Intelligence Committee (Společný zpravodajský výbor). Ani Společný zpravodajský výbor, ani Společná zpravodajská organizace však nemohou využívat vyšetřovacích pravomocí podle zákona o vyšetřovacích pravomocích z roku 2016, zatímco Obranná zpravodajská služba má pro využití svých pravomocí omezenou oblast působnosti.

([262]) Zákaz se vztahuje na veřejné i soukromé komunikační sítě, jakož i na veřejnou poštovní službu, pokud je odposlech prováděn ve Spojeném království. Zákaz se nevztahuje na správce údajů v soukromé síti, pokud správce vydal výslovný nebo konkludentní souhlas s provedením odposlechu (článek 3 zákona o vyšetřovacích pravomocích z roku 2016).

([263]) Ve zvláštních omezených případech je zákonný odposlech možný bez příkazu, tj. při provádění odposlechu se souhlasem odesílatele nebo příjemce (článek 44 zákona o vyšetřovacích pravomocích z roku 2016), v případě omezených správních nebo donucovacích účelů (články 45 až 48 zákona o vyšetřovacích pravomocích), v určitých zvláštních institucích (články 49 až 51 zákona o vyšetřovacích pravomocích z roku 2016) a v souladu se zahraničními žádostmi (článek 52 zákona o vyšetřovacích pravomocích z roku 2016).

údajů a vzdálený síťový přístup k zařízení) ([264]), jakož i na tom, zda je pravomoc vykonávána vůči konkrétnímu cíli nebo hromadně. Podrobnosti o oblasti působnosti, zárukách a omezeních každého opatření podle zákona o vyšetřovacích pravomocích z roku 2016 jsou popsány ve zvláštním oddíle níže.

(179) Zákon o vyšetřovacích pravomocích z roku 2016 je navíc doplněn řadou zákonných kodexů zásad, které vydal ministr a schválily obě komory Parlamentu Spojeného království ([265]) a které jsou použitelné v celé zemi a poskytují pokyny k využívání uvedených pravomocí ([266]). Zatímco subjekty údajů mohou při výkonu svých práv vycházet přímo z ustanovení zákona o vyšetřovacích pravomocích z roku 2016, bod 5 přílohy 7 zákona o vyšetřovacích pravomocích z roku 2016 stanoví, že kodexy zásad jsou přípustné jako důkazy v občanskoprávních a trestních řízeních a soud, tribunál nebo dozorčí orgán může vzít jakékoli nedodržení kodexů v úvahu při rozhodování o příslušné otázce v soudním řízení ([267]). V rámci svého posouzení „kvality práva" týkajícího se předchozího právního předpisu Spojeného království v oblasti dozoru, zákona o úpravě vyšetřovacích pravomocí z roku 2000, velký senát Evropského soudu pro lidská práva výslovně uznal příslušnost britských kodexů zásad a připustil, že jejich ustanovení lze zohlednit při posuzování předvídatelnosti právních předpisů umožňujících sledování ([268]).

(180) Je třeba také poznamenat, že cílené pravomoci (cílené odposlechy ([269]), získávání komunikačních údajů ([270]), uchovávání komunikačních údajů ([271]) a cílený vzdálený síťový přístup k zařízení ([272])) jsou dostupné národním bezpečnostním službám a určitým donucovacím orgánům ([273]), zatímco hromadné pravomoci (tj. hromadný odposlech ([274]), hromadné získávání komunikačních údajů ([275]), hromadný vzdálený síťový přístup k zařízení ([276]) a hromadné soubory osobních údajů ([277])) mohou využívat pouze zpravodajské služby.

(181) Při rozhodování o tom, která vyšetřovací pravomoc by měla být použita, musí zpravodajská služba dodržovat „obecné povinnosti týkající se soukromí" vyjmenované v čl. 2 odst. 2 písm. a) zákona o vyšetřovacích pravomocích z roku 2016, které zahrnují test nezbytnosti a přiměřenosti. Přesněji řečeno, podle tohoto ustanovení musí orgán veřejné moci, který má v úmyslu využít vyšetřovací pravomoc, zvážit: i) zda by bylo možné cíle, kterého má být

([264]) Pokud jde například o oblast působnosti těchto opatření, v rámci části 3 a části 4 (uchovávání a získávání komunikačních údajů) je oblast působnosti opatření důsledně vázána na definici „provozovatelů telekomunikačních služeb", údaje jejichž uživatelů jsou předmětem opatření. Další příklad lze uvést ve vztahu k použití „hromadných" pravomocí. V tomto případě je oblast působnosti těchto pravomocí omezena na „komunikaci odesílanou nebo přijímanou jednotlivci mimo Britské ostrovy".

([265]) Příloha 7 zákona o vyšetřovacích pravomocích z roku 2016 určuje oblast působnosti kodexů, postup pro jejich vydávání, pravidla jejich revize a účinek kodexů.

([266]) Kodexy zásad podle zákona o vyšetřovacích pravomocích z roku 2016 jsou k dispozici na této adrese: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

([267]) Soudy a tribunály používají kodexy zásad k posouzení zákonnosti postupu orgánů. Viz například: věc Dias v Cleveland Police, [2017] UKIPTrib15_586-CH, kdy tribunál pro kontrolu vyšetřovacích pravomocí odkázal na konkrétní části kodexu zásad pro komunikační údaje, aby porozuměl definici důvodu spočívajícího v „předcházení nebo odhalování trestné činnosti nebo předcházení porušování pořádku", který byl využit pro získání komunikačních údajů. Kodex byl zahrnut do odůvodnění s cílem zjistit, zda byl uvedený důvod použit nesprávně. Soud dospěl k závěru, že napadená jednání byla protiprávní. Soudy rovněž provedly hodnocení úrovně záruk dostupných v kodexech, viz například věc Just for Law Kids v Secretary of State for the Home Department [2019] EWHC 1772 (Admin), v níž Vrchní soud shledal, že primární a sekundární právní předpisy spolu s interními pokyny poskytovaly dostatečné záruky, nebo R (National Council for Civil Liberties) v Secretary of State for the Home Department & Others [2019] EWHC 2057 (Admin), v níž soud shledal, že jak zákon o vyšetřovacích pravomocích z roku 2016, tak kodex zásad pro vzdálený síťový přístup k zařízení obsahovaly dostatečná ustanovení o nezbytné specifičnosti příkazů.

([268]) V rozsudku ve věci Big Brother Watch velký senát Evropského soudu pro lidská práva uvedl, že „kodex zásad pro odposlechy komunikace je veřejným dokumentem schváleným oběma komorami parlamentu Spojeného království, který vláda zveřejnila on-line a v tištěném vydání a k němuž musí přihlížet jak subjekty, které vykonávají funkce odposlechu, tak soudy (viz body 93–94 výše). V důsledku toho tento soud připustil, že ustanovení kodexu lze zohlednit při posuzování předvídatelnosti režimu podle zákona o úpravě vyšetřovacích pravomocí (viz Kennedy, cit. výše, bod 157). Soud by tudíž připustil, že vnitrostátní právo bylo přiměřeně „dostupné"." (Viz Evropský soud pro lidská práva (velký senát), rozsudek ve věci Big Brother Watch a ostatní proti Spojenému království, stížnosti č. 58170/13, 62322/14 a 24960/15, ze dne 25. května 2021, bod 366).

([269]) Část 2 zákona o vyšetřovacích pravomocích z roku 2016.

([270]) Část 3 zákona o vyšetřovacích pravomocích z roku 2016.

([271]) Část 4 zákona o vyšetřovacích pravomocích z roku 2016.

([272]) Část 5 zákona o vyšetřovacích pravomocích z roku 2016.

([273]) Seznam příslušných donucovacích orgánů, které mohou uplatňovat cílené vyšetřovací pravomoci podle zákona o vyšetřovacích pravomocích z roku 2016 viz poznámka pod čarou (139).

([274]) Článek 136 zákona o vyšetřovacích pravomocích z roku 2016.

([275]) Článek 158 zákona o vyšetřovacích pravomocích z roku 2016.

([276]) Článek 176 zákona o vyšetřovacích pravomocích z roku 2016.

([277]) Článek 199 zákona o vyšetřovacích pravomocích z roku 2016.

příkazem, povolením nebo oznámením dosaženo, rozumně dosáhnout jinými, méně rušivými prostředky; ii) zda je úroveň ochrany, která se má uplatnit v souvislosti s jakýmkoli získáváním informací na základě příkazu, povolení nebo oznámení, vyšší z důvodu zvláštní citlivosti daných informací; iii) veřejný zájem na integritě a bezpečnosti telekomunikačních systémů a poštovních služeb a iv) jakékoli další aspekty veřejného zájmu na ochraně soukromí ([278]).

(182) Způsob, jakým by měla být tato kritéria uplatňována (a způsob, jakým je jejich dodržování posuzováno v rámci povolení použití uvedených pravomocí ministrem a nezávislými soudními komisaři), je dále upřesněn v příslušných kodexech zásad. Zejména musí být použití kterékoli z těchto vyšetřovacích pravomocí vždy „přiměřené cíli, kterého má být dosaženo, [což] zahrnuje vyvážení závažnosti zásahu do soukromí (a dalších aspektů uvedených v čl. 2 odst. 2) vůči nezbytnosti dané činnosti z hlediska vyšetřovacího, operativního nebo kapacitního“. To zejména znamená, že „by mělo nabízet reálnou vyhlídku na dosažení očekávaného přínosu a nemělo by být nepřiměřené nebo svévolné“ a „[ž]ádný zásah do soukromí by neměl být považován za přiměřený, pokud by požadované informace mohly být rozumně získány jinými, méně rušivými prostředky“ ([279]). Přesněji řečeno, dodržování zásady přiměřenosti musí být posouzeno s ohledem na tato kritéria: „i) rozsah navrhovaného zásahu do soukromí v poměru k cíli, kterého má být dosaženo; ii) jak a proč metody, které mají být přijaty, způsobí co nejmenší možný zásah do soukromí dané osoby a ostatních; iii) zda činnost představuje odpovídající použití zákona a po zvážení všech rozumných alternativ i přiměřený způsob dosažení požadovaného cíle; iv) jaké případné další metody buď nebyly provedeny, nebo byly použity, ale bez použití navrhované vyšetřovací pravomoci jsou hodnoceny jako nedostatečné ke splnění operativních cílů“ ([280]).

(183) Jak vysvětlily orgány Spojeného království, v praxi se tím zajišťuje, že zpravodajská služba nejprve stanoví operativní cíl (a tím vymezí rozsah shromažďování údajů, např. účel spočívající v mezinárodní protiteroristické činnosti v konkrétní zeměpisné oblasti) a následně na základě tohoto operativního cíle bude muset zvážit, která technická možnost (např. cílený nebo hromadný odposlech, vzdálený síťový přístup k zařízení, získávání komunikačních údajů) je nejpřiměřenější (tj. nejméně narušující soukromí, viz čl. 2 odst. 2 zákona o vyšetřovacích pravomocích) cíli, kterého má být dosaženo, a proto ji lze povolit podle jednoho z dostupných právních základů.

(184) Stojí za zmínku, že toto využití standardů nezbytnosti a přiměřenosti zaznamenal a uvítal i Joseph Cannataci, zvláštní zpravodaj OSN pro právo na soukromí, který v souvislosti se systémem zavedeným zákonem o vyšetřovacích pravomocích z roku 2016 uvedl, že „[p]ostupy zavedené jak ve zpravodajských službách, tak v donucovacích orgánech zřejmě systematicky vyžadují posouzení nezbytnosti a přiměřenosti opatření nebo operace v oblasti sledování předtím, než je opatření nebo operace doporučena k povolení, jakož i přezkum opatření nebo operace z týchž důvodů“ ([281]). Rovněž poznamenal, že na svém setkání se zástupci donucovacích orgánů a národních bezpečnostních služeb „získal konsenzuální názor, že při každém rozhodování o opatřeních v oblasti sledování musí být primárně zohledněno právo na soukromí. Všichni chápali a oceňovali nezbytnost a přiměřenost jako základní zásady, které je třeba vzít v úvahu“.

([278]) Kodex zásad pro odposlech komunikace stanoví, že dalšími prvky testu přiměřenosti jsou: „i) rozsah navrhovaného zásahu do soukromí v poměru k cíli, kterého má být dosaženo; ii) jak a proč metody, které mají být přijaty, způsobí co nejmenší možný zásah do soukromí dané osoby a ostatních; iii) zda činnost představuje odpovídající použití zákona a po zvážení všech rozumných alternativ i přiměřený způsob dosažení požadovaného cíle; iv) jaké případné další metody buď nebyly provedeny, nebo byly použity, ale bez použití navrhované vyšetřovací pravomoci jsou hodnoceny jako nedostatečné ke splnění operativních cílů“. Code of Practice on Interception of Communications (Kodex zásad pro odposlech komunikace), bod 4.16, k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

([279]) Viz Code of Practice on Interception of Communications (kodex zásad pro odposlech komunikace), body 4.12 a 4.15, k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

([280]) Viz kodex zásad pro odposlech komunikace, bod 4.16.

([281]) End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland (Prohlášení po skončení mise zvláštního zpravodaje pro právo na soukromí týkající se skončení jeho mise do Spojeného království Velké Británie a Severního Irska), k dispozici na této adrese: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, bod 1.a.

(185) Zvláštní kritéria pro vydávání jednotlivých příkazů, jakož i omezení a záruky stanovené zákonem o vyšetřovacích pravomocích z roku 2016 pro každou vyšetřovací pravomoc jsou podrobně uvedeny ve 186. až 243. bodě odůvodnění.

3.3.1.1.1 Cílené odposlechy a šetření

(186) Existují tři druhy příkazů týkající se cíleného odposlechu: příkaz k cílenému odposlechu ([282]), příkaz k cílenému šetření a příkaz k vzájemné pomoci ([283]). Podmínky pro získání těchto příkazů i příslušné záruky jsou stanoveny v části 2 kapitole 1 zákona o vyšetřovacích pravomocích z roku 2016.

(187) Příkaz k cílenému odposlechu povoluje odposlech komunikace popsané v příkazu během přenosu a získávání dalších údajů významných pro tuto komunikaci ([284]), včetně sekundárních údajů ([285]). Příkaz k cílenému šetření opravňuje určitou osobu k provedení výběru pro šetření obsahu odposlechu získaného na základě příkazu k hromadnému odposlechu ([286]).

(188) Jakýkoli příkaz podle části 2 zákona o vyšetřovacích pravomocích z roku 2016 může vydat ministr ([287]) a schválit soudní komisař ([288]). Ve všech případech je doba platnosti jakéhokoli typu cíleného příkazu omezena na šest měsíců ([289]) a pro jeho úpravy ([290]) a prodloužení platí zvláštní pravidla ([291]).

(189) Před vydáním příkazu musí ministr provést posouzení nezbytnosti a přiměřenosti ([292]). Zvláště v případě příkazu k cílenému odposlechu a příkazu k cílenému šetření by měl ministr ověřit, zda je opatření nezbytné z jednoho z těchto důvodů: zájem národní bezpečnosti; prevence nebo odhalování trestné činnosti nebo zájmy hospodářského blahobytu Spojeného království ([293]), pokud jsou tyto zájmy významné i z hlediska zájmů národní bezpečnosti ([294]). Na druhé straně příkaz k vzájemné pomoci (viz 139. bod odůvodnění výše) lze vydat pouze v případě, že má ministr za to, že existují okolnosti rovnocenné okolnostem, za nichž by vydal příkaz za účelem prevence a/nebo odhalování závažné trestné činnosti ([295]).

(190) Ministr by měl navíc posoudit, zda je opatření přiměřené cíli, kterého má být dosaženo ([296]). Posouzení přiměřenosti požadovaných opatření musí zohledňovat obecné povinnosti týkající se soukromí stanovené v čl. 2 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016, zejména potřebu posoudit, zda by bylo možné cíle, kterého má být

([282]) Ustanovení čl. 15 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016.
([283]) Ustanovení čl. 15 odst. 4 zákona o vyšetřovacích pravomocích z roku 2016.
([284]) Ustanovení čl. 15 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016.
([285]) Sekundární údaje jsou údaje připojené k odposlechnuté komunikaci nebo s ní logicky spojené, které od ní lze logicky oddělit, a pokud by byly takto odděleny, neodhalily by nic z toho, co by bylo možné rozumně považovat za smysl dané komunikace (pokud existuje). K příkladům sekundárních údajů patří konfigurace routeru nebo firewallu nebo doba, po kterou byl router aktivní v síti, pokud jsou tyto údaje součástí odposlechnuté komunikace, jsou k ní připojeny nebo s ní logicky spojeny. Další podrobnosti viz definice v článku 16 zákona o vyšetřovacích pravomocích z roku 2016 a v bodě 2.19 kodexu zásad pro odposlech komunikace, viz poznámka pod čarou 278.
([286]) Toto šetření se provádí jako výjimka z ustanovení čl. 152 odst. 4 zákona o vyšetřovacích pravomocích z roku 2016, který stanoví zákaz snahy o ztotožnění komunikace osob, které se nacházejí na Britských ostrovech. Viz (229). bod odůvodnění.
([287]) Skotský ministr povoluje příkaz, pokud se týká závažné trestné činnosti ve Skotsku (viz články 21 a 22 zákona o vyšetřovacích pravomocích z roku 2016), přičemž ministr může pověřit vyššího úředníka k vydání příkazu k vzájemné pomoci, pokud vyjde najevo, že odposlech se bude týkat osoby nebo prostor nacházejících se mimo Spojené království (článek 40 zákona o vyšetřovacích pravomocích z roku 2016).
([288]) Články 19 a 23 zákona o vyšetřovacích pravomocích z roku 2016.
([289]) Článek 32 zákona o vyšetřovacích pravomocích z roku 2016.
([290]) Článek 39 zákona o vyšetřovacích pravomocích z roku 2016. Určené osoby mohou provést omezené úpravy příkazů za podmínek stanovených v zákoně o vyšetřovacích pravomocích z roku 2016. Osoba, která příkaz vydala, jej může kdykoli zrušit. Musí tak učinit, pokud příkaz již není z jakýchkoli relevantních důvodů nezbytný nebo pokud jednání povolené příkazem již není přiměřené cíli, kterého má být dosaženo.
([291]) Článek 33 zákona o vyšetřovacích pravomocích z roku 2016. Rozhodnutí o prodloužení příkazu musí schválit soudní komisař.
([292]) Článek 19 zákona o vyšetřovacích pravomocích z roku 2016.
([293]) K pojmu „zájmy hospodářského blahobytu Spojeného království, pokud jsou tyto zájmy významné i z hlediska zájmů národní bezpečnosti“ velký senát Evropského soudu pro lidská práva ve věci Big Brother Watch a ostatní proti Spojenému království (viz poznámka pod čarou 268 výše) v bodě 371 konstatoval, že tento pojem je dostatečně zaměřen na národní bezpečnost. Jakkoli zjištění soudu v této věci souviselo s použitím uvedeného pojmu v zákoně o úpravě vyšetřovacích pravomocí z roku 2000, tentýž pojem je použit i v zákoně o vyšetřovacích pravomocích z roku 2016.
([294]) Ustanovení čl. 20 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016.
([295]) Ustanovení čl. 20 odst. 3 zákona o vyšetřovacích pravomocích z roku 2016.
([296]) Ustanovení čl. 19 odst. 1 písm. b), čl. 19 odst. 2 písm. b) a čl. 19 odst. 3 písm. b) zákona o vyšetřovacích pravomocích z roku 2016.

příkazem, povolením nebo oznámením dosaženo, rozumně dosáhnout jinými, méně rušivými prostředky a zda je úroveň ochrany, která se má uplatnit v souvislosti s jakýmkoli získáváním informací na základě příkazu vyšší z důvodu zvláštní citlivosti daných informací (viz 181. bod odůvodnění výše).

(191) Za tímto účelem bude ministr muset vzít v úvahu všechny prvky návrhu poskytnuté dožadujícím orgánem, a to zejména ty, které se týkají osob, které mají být odposlouchávány, a významu opatření pro vyšetřování. Tyto prvky jsou vyjmenovány v kodexu zásad pro odposlech komunikace a musí být popsány s určitou mírou specifičnosti ([297]). Kromě toho článek 17 zákona o vyšetřovacích pravomocích z roku 2016 vyžaduje, aby jakýkoli příkaz vydaný podle kapitoly 2 uvedeného zákona musel jmenovat nebo popisovat konkrétní osobu nebo skupinu osob, organizaci nebo prostory, které mají být odposlouchávány (tedy „cíl“). Příkaz k cílenému odposlechu nebo příkaz k cílenému šetření se může vztahovat také na skupinu osob, více než jednu osobu nebo organizaci nebo více než jeden soubor prostor (také označovaný jako „tematický příkaz“) ([298]). V těchto případech by měl příkaz popisovat společný účel nebo činnost sdílenou danou skupinou osob nebo operaci/vyšetřování a měl by pojmenovat nebo popsat co nejvíce z těchto osob/organizací nebo soubor prostor, je-li to přiměřeně proveditelné ([299]). A konečně také musí všechny příkazy vydané podle části 2 zákona o vyšetřovacích pravomocích z roku 2016 specifikovat adresy, čísla, přístroje, faktory nebo kombinaci faktorů, které mají být použity k identifikaci komunikace ([300]). V tomto ohledu kodex zásad pro odposlech komunikace stanoví, že v případě příkazu k cílenému odposlechu a příkazu k cílenému šetření „musí příkaz specifikovat (nebo popisovat) faktory nebo kombinaci faktorů, které mají být použity pro identifikaci komunikace. Pokud má být komunikace identifikována odkazem na telefonní číslo (například), musí být číslo specifikováno uvedením v celém rozsahu. Pokud však mají být k identifikaci komunikace použity velmi složité nebo neustále se měnící internetové selektory, měly by být tyto selektory popsány v maximálním možném rozsahu“ ([301]).

(192) Důležitou zárukou v této souvislosti je to, že posouzení provedené ministrem pro účely vydání příkazu musí být schváleno nezávislým soudním komisařem ([302]), který zejména ověří, zda je rozhodnutí o vydání příkazu v souladu se zásadami nezbytnosti a přiměřenosti ([303]) (status a úloha soudních komisařů viz 251. až 256. bod odůvodnění níže). Zákon o vyšetřovacích pravomocích z roku 2016 rovněž objasňuje, že při provádění této kontroly musí soudní komisař uplatňovat stejné zásady, jaké by uplatňoval soud při podání návrhu na soudní přezkum ([304]). Tím je zajištěno, že v každém případě a před uskutečněním přístupu k údajům bude soulad se zásadou nezbytnosti a přiměřenosti systematicky kontrolován nezávislým subjektem.

(193) Zákon o vyšetřovacích pravomocích z roku 2016 stanoví několik málo specifických a úzce vymezených výjimek pro provádění cílených odposlechů bez příkazu. Omezené případy jsou podrobně popsány v zákoně ([305]) a kromě případu založeného na „souhlasu“ odesílatele/příjemce provádějí odposlech jiné osoby (soukromé nebo veřejné subjekty) než národní bezpečnostní služby. Kromě toho se tento druh odposlechů provádí za jiným účelem, než je shromažďování „zpravodajských informací“ ([306]), a u některých z nich je velmi nepravděpodobné, že by shromažďování údajů mohlo probíhat v kontextu scénáře „předávání“ (například v případě odposlechu

([297]) Požadované informace zahrnují podrobnosti o pozadí (popis osob / organizací / souboru prostor, komunikace, která má být odposlouchávána) a o tom, jak získání těchto informací prospěje vyšetřování, jakož i popis jednání, které má být povoleno. V případě, že není možné popsat osoby/organizaci/prostory, je třeba uvést vysvětlení, proč to nebylo možné nebo proč byl uveden pouze obecný popis (kodex zásad pro odposlech komunikace, body 5.32 a 5.34, viz poznámka pod čarou 278).

([298]) Ustanovení čl. 17 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016. Viz také kodex zásad pro odposlech komunikace, body 5.11 a násl., viz poznámka pod čarou 278.

([299]) Ustanovení čl. 31 odst. 4 a 5 zákona o vyšetřovacích pravomocích z roku 2016.

([300]) Ustanovení čl. 31 odst. 8 zákona o vyšetřovacích pravomocích z roku 2016.

([301]) Kodex zásad pro odposlech komunikace, body 5.37 a 5.38, viz poznámka pod čarou 278.

([302]) Schválení soudním komisařem se nevyžaduje, pokud má ministr za to, že vydání příkazu je naléhavě nutné (čl. 19 odst. 1 zákona o vyšetřovacích pravomocích). Soudní komisař však musí být co nejdříve informován a musí rozhodnout, zda příkaz schválí, nebo neschválí. Pokud jej neschválí, ztratí příkaz účinnost (články 24 a 25 zákona o vyšetřovacích pravomocích z roku 2016).

([303]) Ustanovení čl. 23 odst. 1 zákona o vyšetřovacích pravomocích z roku 2016.

([304]) Ustanovení čl. 23 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016.

([305]) Viz články 44–51 zákona o vyšetřovacích pravomocích z roku 2016 a oddíl 12 kodexu zásad pro odposlech komunikace (viz poznámka pod čarou 278).

([306]) Jedná se například o případ, kdy je zapotřebí odposlech ve věznici nebo v psychiatrické léčebně (ke kontrole chování zadržené osoby nebo pacienta), nebo například odposlech u provozovatele poštovních nebo telekomunikačních služeb za účelem zjištění urážlivého obsahu.

prováděného v psychiatrické léčebně nebo ve věznici). S ohledem na povahu subjektu, na který se tyto specifické případy vztahují (kterým nejsou národní bezpečnostní služby), použijí se všechny záruky stanovené v části 2 zákona o ochraně údajů z roku 2018 a v britském nařízení GDPR, včetně dohledu Úřadu komisaře pro informace a dostupných ochranných mechanismů. Kromě toho kromě záruk poskytnutých zákonem o ochraně údajů z roku 2018 zákon o vyšetřovacích pravomocích z roku 2016 v určitých případech stanoví také následný dohled ze strany Úřadu komisaře pro kontrolu vyšetřovacích pravomocí ([307]).

(194) Při provádění odposlechu platí další omezení a záruky s ohledem na konkrétní status odposlouchávané osoby / odposlouchávaných osob ([308]). Například odposlech záležitostí podléhajících povinnosti mlčenlivosti je povolen pouze za výjimečných a naléhavých okolností, osoba vydávající příkaz musí brát ohled na veřejný zájem na důvěrnosti záležitostí podléhajících povinnosti mlčenlivosti a na to, že existují zvláštní požadavky týkající se manipulace s takovým materiálem, jeho uchovávání a zpřístupňování ([309]).

(195) Zákon o vyšetřovacích pravomocích z roku 2016 dále stanoví specifické záruky týkající se zabezpečení, uchovávání a zpřístupňování, které by měl ministr vzít v úvahu před vydáním cíleného příkazu ([310]). Ustanovení čl. 53 odst. 5 zákona o vyšetřovacích pravomocích z roku 2016 zejména vyžaduje, aby každá kopie kteréhokoli z těchto materiálů shromážděných na základě příkazu byla uložena bezpečně a byla zničena, jakmile již nebudou existovat žádné relevantní důvody pro její uchovávání, zatímco čl. 53 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016 vyžaduje, aby počet osob, kterým je materiál zpřístupněn, a rozsah, v jakém je jakýkoli materiál zveřejněn, zpřístupněn, zpřístupňován nebo kopírován, byl omezen na minimum, které je pro zákonné účely nezbytné.

(196) A konečně, pokud má být materiál, který byl zachycen na základě příkazu k cílenému odposlechu nebo příkazu k vzájemné pomoci, předán třetí zemi („zahraniční zpřístupnění"), zákon o vyšetřovacích pravomocích z roku 2016 stanoví, že ministr se musí ujistit, že existuje vhodný režim, který zaručí, že v této třetí zemi budou existovat obdobné záruky zabezpečení, uchovávání a zpřístupňování ([311]). Kromě toho čl. 109 odst. 2 zákona o ochraně údajů z roku 2018 stanoví, že zpravodajské služby mohou předávat osobní údaje na území mimo Spojené království pouze v případě, že je předání nezbytné a přiměřené pro účely zákonných funkcí správce nebo pro jiné účely stanovené v čl. 2 odst. 2 písm. a) zákona o Bezpečnostní službě z roku 1989 nebo v čl. 2 odst. 2 písm. a) a čl. 4 odst. 2 písm. a) zákona o zpravodajských službách z roku 1994 ([312]). Důležité je, že tyto požadavky se použijí i v případech, v nichž je uplatněna výjimka z důvodu národní bezpečnosti podle článku 110 zákona o ochraně údajů z roku 2018, neboť článek 110 zákona o ochraně údajů z roku 2018 neuvádí článek 109 zákona o ochraně údajů z roku 2018 jako jedno z ustanovení, které se nemusí použít, pokud je pro účely ochrany národní bezpečnosti nutná výjimka z určitých ustanovení.

3.3.1.1.2 Cílené získávání a uchovávání komunikačních údajů

(197) Zákon o vyšetřovacích pravomocích z roku 2016 umožňuje ministrovi požadovat, aby provozovatelé telekomunikačních služeb uchovávali komunikační údaje za účelem cíleného přístupu řady orgánů veřejné moci, včetně donucovacích orgánů a zpravodajských služeb. Část 4 zákona o vyšetřovacích pravomocích z roku 2016 stanoví uchovávání komunikačních údajů, zatímco část 3 upravuje cílené získávání komunikačních údajů. Část 3 a část 4 zákona o vyšetřovacích pravomocích z roku 2016 rovněž vymezují konkrétní omezení použití těchto pravomocí a stanoví zvláštní záruky.

([307]) Viz *a contrario* čl. 229 odst. 4 zákona o vyšetřovacích pravomocích.

([308]) Články 26–29 zákona o vyšetřovacích pravomocích z roku 2016 zavádějí omezení pro získání příkazu k cílenému odposlechu a cílenému šetření v souvislosti s odposlechem komunikace zasílané nebo určené osobě, která je poslancem parlamentu (kteréhokoli parlamentu ve Spojeném království), s odposlechem záležitostí podléhajících povinnosti mlčenlivosti, odposlechem komunikace, o které má odposlouchávající orgán za to, že bude obsahovat důvěrné novinářské materiály, a pokud je účelem příkazu identifikovat nebo potvrdit zdroj novinářských informací.

([309]) Článek 26 zákona o vyšetřovacích pravomocích z roku 2016.

([310]) Ustanovení čl. 19 odst. 1 zákona o vyšetřovacích pravomocích z roku 2016.

([311]) Článek 54 zákona o vyšetřovacích pravomocích z roku 2016. Záruky týkající se zpřístupňování materiálu zahraničním orgánům jsou dále upřesněny v kodexech zásad: viz zejména bod 9.26 a násl. a bod 9.87 kodexu zásad pro odposlech komunikace a bod 9.33 a násl. a bod 9.41 kodexu zásad pro vzdálený síťový přístup k zařízení (viz poznámka pod čarou 278).

([312]) Těmito účely jsou: pro Bezpečnostní službu prevence nebo odhalování závažné trestné činnosti nebo jakékoli trestní řízení (čl. 2 odst. 2 písm. a) zákona o Bezpečnostní službě z roku 1989), pro zpravodajskou službu zájmy národní bezpečnosti, prevence nebo odhalování závažné trestné činnosti nebo jakékoli trestní řízení (čl. 2 odst. 2 písm. a) zákona o zpravodajských službách z roku 1994) a pro GCHQ jakékoli trestní řízení (čl. 4 odst. 2 písm. a) zákona o zpravodajských službách z roku 1994). Viz také vysvětlivky k zákonu o ochraně údajů z roku 2018, k dispozici na této adrese: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(198) Výraz „komunikační údaje“ v rámci určité komunikace zahrnuje „kdo“, „kdy“, „kde“ a „jak“, nikoli však obsah komunikace, tj. co bylo řečeno nebo napsáno. Na rozdíl od odposlechu není získávání a uchovávání komunikačních údajů zaměřeno na získání obsahu komunikace, ale na získání informací, například určení účastníka telefonní služby nebo vyúčtování rozepsaného na jednotlivé položky. Údaje by mohly zahrnovat čas a dobu trvání komunikace, telefonní číslo nebo e-mailovou adresu původce a příjemce a někdy i umístění zařízení, z nichž byla komunikace uskutečněna ([313]).

(199) Je třeba upozornit, že uchovávání a získávání komunikačních údajů se obvykle nebude týkat osobních údajů subjektů údajů z EU předávaných podle tohoto rozhodnutí do Spojeného království. Povinnost uchovávat nebo zpřístupňovat komunikační údaje podle částí 3 a 4 zákona o vyšetřovacích pravomocích z roku 2016 zahrnuje údaje, které shromažďují provozovatelé telekomunikačních služeb ve Spojeném království přímo od uživatelů telekomunikační služby ([314]). Tento druh zpracování „v přímém vztahu k zákazníkovi“ obvykle nezahrnuje předání na základě tohoto rozhodnutí, tj. předání správcem/zpracovatelem v EU správci/zpracovateli ve Spojeném království.

(200) Pro úplnost jsou však v následujících bodech odůvodnění analyzovány podmínky a záruky, kterými se tyto režimy získávání a uchovávání řídí.

(201) Jako základní premisu je třeba uvést, že uchovávání a cílené získávání komunikačních údajů mohou využít jak národní bezpečnostní služby, tak některé donucovací orgány ([315]). Podmínky požadavku na uchovávání a/nebo získávání komunikačních údajů se mohou lišit v závislosti na důvodu pro požadování daného opatření, konkrétně na účelu týkajícího se národní bezpečnosti nebo vymáhání práva.

(202) Zejména, zatímco nový režim zavedl obecný požadavek předem vydaného povolení nezávislého orgánu, který se použije ve všech případech, v nichž jsou uchovávány a/nebo získávány komunikační údaje (buď pro účely vymáhání práva, nebo pro účely národní bezpečnosti), v návaznosti na rozsudek Evropského soudního dvora ve věci Tele2/Watson ([316]) byly zavedeny zvláštní záruky v případech, v nichž je opatření požadováno pro účely vymáhání práva. Zejména, je-li uchování nebo získání komunikačních údajů požadováno pro účely vymáhání práva, musí předem vydané povolení vždy vystavit komisař pro kontrolu vyšetřovacích pravomocí. Není tomu tak vždy, pokud je opatření požadováno z důvodu národní bezpečnosti, neboť v určitých případech může být takový druh opatření povolen jinou „schvalující osobou“, jak je popsáno níže. Nový režim kromě toho zvýšil prahovou hodnotu, u níž lze povolit uchovávání a získávání komunikačních údajů, na „závažné trestné činy“ ([317]).

([313]) Komunikační údaje definuje čl. 261 odst. 5 zákona o vyšetřovacích pravomocích z roku 2016. Komunikační údaje se člení na „údaje týkající se události“ (jakékoli údaje, které identifikují nebo popisují událost, ať s odkazem, či bez odkazu na místo události, která nastala v telekomunikačním systému nebo prostřednictvím telekomunikačního systému, přičemž událost zahrnuje jeden nebo více subjektů zapojených do konkrétní činnosti v konkrétní dobu) a „údaje týkající se subjektu“ (jakékoli údaje, které a) se týkají i) subjektu, ii) souvislosti mezi telekomunikační službou a subjektem nebo iii) souvislosti mezi jakoukoli částí telekomunikačního systému a subjektem; b) jsou tvořeny údaji, které identifikují nebo popisují subjekt (ať s odkazem, či bez odkazu na umístění subjektu) a c) nejsou údaji týkajícími se událostí).

([314]) To vyplývá z definice komunikačních údajů uvedené v čl. 261 odst. 5 zákona o vyšetřovacích pravomocích z roku 2016, podle nichž jsou komunikační údaje uchovávány nebo získávány poskytovatelem telekomunikačních služeb a buď se týkají uživatele telekomunikační služby a vztahují se k poskytování této služby, nebo jsou obsaženy v určité komunikaci, zahrnuty jako součást komunikace, připojeny ke komunikaci nebo s komunikací logicky spojeny (viz také kodex zásad pro komunikační údaje, k dispozici na této adrese: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). Definice poskytovatele telekomunikačních služeb uvedená v čl. 261 odst. 10 zákona o vyšetřovacích pravomocích z roku 2016 navíc vyžaduje, aby poskytovatelem telekomunikačních služeb byla osoba, která nabízí nebo poskytuje telekomunikační službu osobám ve Spojeném království nebo která ovládá nebo poskytuje telekomunikační systém, který se (zcela nebo zčásti) nachází ve Spojeném království nebo je ze Spojeného království ovládán. Tyto definice objasňují, že povinnosti podle zákona o vyšetřovacích pravomocích z roku 2016 nelze uložit poskytovatelům telekomunikačních služeb, jejichž zařízení se nenachází ve Spojeném království nebo není ze Spojeného království ovládáno, a kteří nenabízejí ani neposkytují služby osobám ve Spojeném království (viz také kodex zásad pro komunikační údaje, bod 2.1). Pokud účastníci z EU (ať se nacházejí v EU, nebo ve Spojeném království) využívají služeb ve Spojeném království, veškerá komunikace související s poskytováním této služby by byla shromažďována přímo poskytovatelem služeb ve Spojeném království a nebyla by předávána z EU.

([315]) Příslušné orgány jsou uvedeny v příloze 4 zákona o vyšetřovacích pravomocích z roku 2016 a zahrnují policejní síly, zpravodajské služby, některá ministerstva a vládní útvary, Národní kriminální agenturu, Celní a daňovou správu, Úřad pro hospodářskou soutěž a trhy, komisaře pro informace, zdravotní záchrannou službu, hasičský sbor a záchranářskou službu a orgány působící například v oblasti zdraví a bezpečnosti potravin.

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

([317]) Získávání komunikačních údajů viz čl. 61 odst. 7 písm. b) a uchovávání komunikačních údajů viz článek 87 odst. 10A.

i) *Oprávnění k získávání komunikačních údajů*

(203) Podle části 3 zákona o vyšetřovacích pravomocích z roku 2016 jsou příslušné orgány veřejné moci oprávněny získávat komunikační údaje od poskytovatele telekomunikačních služeb nebo kterékoli osoby, která může takové údaje získat a zpřístupnit. Povolení nemusí umožňovat odposlech obsahu komunikace ([318]) a pozbývá účinnosti po uplynutí jednoho měsíce ([319]) s možností prodloužení, bude-li vydáno další povolení ([320]). Získání komunikačních údajů vyžaduje povolení komisaře pro kontrolu vyšetřovacích pravomocí ([321]) (status a pravomoci komisaře pro kontrolu vyšetřovacích pravomocí viz 250. až 251. bod odůvodnění níže). Je tomu tak ve všech případech, kdy o získání komunikačních údajů žádá příslušný donucovací orgán. Avšak jsou-li údaje získány v zájmu národní bezpečnosti nebo hospodářského blahobytu Spojeného království, pokud je to důležité pro národní bezpečnost nebo pokud žádost podá člen zpravodajské služby podle čl. 61 odst. 7 písm. b) ([322]), může podle článku 61 zákona o vyšetřovacích pravomocích z roku 2016 získání alternativně ([323]) povolit komisař pro kontrolu vyšetřovacích pravomocí nebo určený vyšší úředník ([324]). Určený úředník musí být nezávislý na dotčeném vyšetřování nebo dotčené operaci a musí mít pracovní znalost zásad a právních předpisech v oblasti lidských práv, zejména zásad nezbytnosti a přiměřenosti ([325]). Rozhodnutí určeného úředníka bude podléhat následnému dohledu ze strany komisaře pro kontrolu vyšetřovacích pravomocí (další podrobnosti o funkcích následného dohledu komisaře pro kontrolu vyšetřovacích pravomocí viz 254. bod odůvodnění níže).

(204) Povolení k získání komunikačních údajů je založeno na posouzení nezbytnosti a přiměřenosti opatření. Přesněji řečeno, nezbytnost opatření se posuzuje s ohledem na důvody vyjmenované v právních předpisech ([326]). S ohledem na cílenou povahu tohoto opatření musí být opatření také nezbytné pro konkrétní vyšetřování nebo operaci ([327]). Další požadavky na posouzení nezbytnosti opatření jsou stanoveny v kodexu zásad pro komunikační údaje ([328]). Tento kodex zejména stanoví, že návrh podaný dožadujícím orgánem by měl identifikovat tři minimální prvky odůvodňující jeho nezbytnost: i) vyšetřovanou událost, jako je trestný čin nebo místo, kde se nachází zranitelná pohřešovaná osoba; ii) osobu, jejíž údaje jsou požadovány, například podezřelého, svědka nebo pohřešované osoby, a způsob, jakým je osoba s událostí spojena, a iii) požadovaná komunikační data, jako je telefonní číslo nebo IP adresa, a vztah těchto údajů k dané osobě a události ([329]).

(205) Získání komunikačních údajů by navíc mělo být přiměřené cíli, kterého má být dosaženo ([330]). Kodex zásad pro komunikační údaje objasňuje, že při provádění takového posouzení by měl schvalující jednotlivec posoudit vyvážení „míry zásahu do práv a svobod jednotlivce vůči konkrétnímu prospěchu pro vyšetřování nebo operaci prováděnou příslušným orgánem veřejné moci ve veřejném zájmu“ a uvážit, že při zohlednění všech aspektů

([318]) Ustanovení čl. 60A odst. 6 zákona o vyšetřovacích pravomocích z roku 2016.

([319]) Tato lhůta se zkracuje na tři dny, pokud je povolení vydáno z naléhavých důvodů (čl. 65 odst. 3A zákona o vyšetřovacích pravomocích z roku 2016).

([320]) Podle článku 65 zákona o vyšetřovacích pravomocích z roku 2016 bude prodloužené povolení platné po dobu jednoho měsíce ode dne vypršení platnosti stávajícího povolení. Osoba, která povolení vydala, může povolení kdykoli zrušit, pokud bude mít za to, že požadavky již nejsou plněny.

([321]) Ustanovení čl. 60A odst. 1 zákona o vyšetřovacích pravomocích z roku 2016. Tuto funkci jménem komisaře pro kontrolu vyšetřovacích pravomocí plní Úřad pro povolování v oblasti komunikačních údajů (Office for Communications Data Authorisations, OCDA) (viz kodexy zásad pro komunikační údaje, bod 5.6).

([322]) Návrh podle čl. 61 odst. 7 písm. b) zákona o vyšetřovacích pravomocích z roku 2016 se podává za „příslušným účelem souvisejícím s trestnou činností“, což podle čl. 61 odst. 7A zákona o vyšetřovacích pravomocích z roku 2016 znamená: „pokud jsou komunikační údaje zcela nebo zčásti tvořeny údaji týkajícími se událostí, účel spočívající v prevenci nebo odhalování závažné trestné činnosti; ve všech ostatních případech účel prevence nebo odhalování trestné činnosti nebo předcházení porušování pořádku“.

([323]) Kodex zásad pro komunikační údaje stanoví: „Pokud by bylo možné podat návrh týkající se národní bezpečnosti podle článku 60A nebo článku 61, rozhodnutí o tom, který postup vydání povolení je v daném případě nejvhodnější, je věcí jednotlivých orgánů veřejné moci. Orgány veřejné moci, které hodlají použít postup prostřednictvím určeného vyššího úředníka, by měly mít zavedeny jasné pokyny, kdy je tento postup povolení vhodný.“ (kodex zásad pro komunikační údaje, bod 5.19, k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

([324]) Ustanovení čl. 70 odst. 3 zákona o vyšetřovacích pravomocích z roku 2016 uvádí definici „určeného úředníka“, která se liší podle příslušného orgánu veřejné správy (jejichž výčet uvádí příloha 4 zákona o vyšetřovacích pravomocích z roku 2016).

([325]) Další podrobnosti o nezávislosti určeného vyššího úředníka uvádí kodex zásad pro komunikační údaje (kodex zásad pro komunikační údaje, body 4.12–4.17, viz poznámka pod čarou 323).

([326]) Těmito důvody jsou: i) národní bezpečnost; ii) předcházení nebo odhalování trestné činnosti nebo předcházení porušování pořádku (v případě „údajů týkajících se událostí“ pouze závažné trestné činnosti); iii) zájmy hospodářského blahobytu Spojeného království, pokud jsou tyto zájmy významné i z hlediska zájmů národní bezpečnosti; iv) zájmy veřejné bezpečnosti; v) předcházení úmrtí či zranění nebo jakékoli újmě na fyzickém či psychickém zdraví určité fyzické osoby nebo zmírnění jakéhokoli zranění nebo újmy na fyzickém či psychickém zdraví určité fyzické osoby; vi) pomoc při vyšetřování údajných justičních omylů nebo vii) určení totožnosti zemřelé osoby nebo osoby, která se z důvodu určitého zdravotního stavu není schopna identifikovat sama (čl. 61 odst. 7 zákona o vyšetřovacích pravomocích z roku 2016).

([327]) Ustanovení čl. 60A odst. 1 zákona o vyšetřovacích pravomocích z roku 2016.

([328]) Kodex zásad pro komunikační údaje, body 3.3 a násl., viz poznámka pod čarou 323.

([329]) Kodex zásad pro komunikační údaje, bod 3.13, viz poznámka pod čarou 323.

([330]) Ustanovení čl. 60 odst. 1 písm. c) zákona o vyšetřovacích pravomocích z roku 2016.

konkrétního případu „nemusí být zásah do práv jednotlivce přesto odůvodněn, neboť nepříznivý dopad na práva jiného jednotlivce nebo skupiny jednotlivců je příliš závažný“. Za účelem konkrétního posouzení přiměřenosti opatření kodex vyjmenovává řadu prvků, které by měl obsahovat návrh podaný dožadujícím orgánem ([331]). Dále je třeba věnovat zvláštní pozornost druhu komunikačních údajů (údaje týkající se „subjektu“ nebo „událostí“ ([332])), které mají být získány, a musí být upřednostněno použití méně rušivé kategorie údajů ([333]). Kodex zásad pro komunikační údaje také obsahuje konkrétní pokyny pro povolení týkající se komunikačních údajů osob v určitých profesích (například lékařů, advokátů, novinářů, poslanců nebo kněží) ([334]), na které se vztahují další záruky ([335]).

ii) *Oznámení vyžadující uchovávání komunikačních údajů*

(206) Část 4 zákona o vyšetřovacích pravomocích z roku 2016 stanoví pravidla pro uchovávání komunikačních údajů, a zejména kritéria umožňující ministrovi vydat výzvu k uchovávání údajů ([336]). Záruky zavedené zákonem o vyšetřovacích pravomocích jsou stejné, pokud jsou údaje uchovávány buď pro účely vymáhání práva, nebo v zájmu národní bezpečnosti.

(207) Vydání těchto výzev k uchovávání údajů má zajistit, aby provozovatelé telekomunikačních služeb po dobu maximálně 12 měsíců uchovávali relevantní komunikační údaje, které by jinak byly vymazány, jakmile již nebudou pro obchodní účely zapotřebí ([337]). Uchované údaje mají zůstat k dispozici po požadovanou dobu pro případ, že by bylo následně nezbytné, aby je orgán veřejné moci získal na základě povolení k cílenému získání komunikačních údajů podle části 3 zákona o vyšetřovacích pravomocích z roku 2016 a popisu ve 203. až 205. bodě odůvodnění.

(208) Výkon pravomoci vyžadovat uchovávání určitých údajů podléhá řadě omezení a záruk. Ministr může výzvu k uchovávání údajů jednomu nebo více provozovatelům ([338]) vydat pouze v případě, že má za to, že požadavek na uchování údajů je nezbytný pro jeden ze zákonných účelů ([339]) a je přiměřený cíli, kterého má být dosaženo ([340]). Jak je objasněno v samotném zákoně o vyšetřovacích pravomocích

([331]) Tyto povinně uváděné informace musí obsahovat: i) nástin toho, jak získání údajů přinese prospěch vyšetřování nebo operaci; ii) vysvětlení významu požadovaných lhůt, včetně toho, jak jsou tyto lhůty přiměřené vyšetřované události; iii) vysvětlení toho, jak je míra narušení soukromí oprávněná s ohledem na přínos údajů pro vyšetřování (toto odůvodnění by mělo zahrnovat posouzení toho, zda by pro dosažení cíle mohlo být provedeno méně rušivé vyšetřování); iv) posouzení práv jednotlivce (zejména na soukromí a v příslušných případech svobody projevu) a vyvážení těchto práv s přínosem pro vyšetřování; v) podrobnosti o případném vedlejším narušení soukromí a o tom, jak požadované lhůty ovlivní vedlejší narušení soukromí (kodex zásad pro komunikační údaje, body 3.22–3.26, viz poznámka pod čarou 323).

([332]) Viz poznámka pod čarou 313.

([333]) Pokud jsou požadovány komunikační údaje s větším narušením soukromí (tj. týkající se událostí), kodex stanoví, že je vhodnější nejprve získat údaje týkající se subjektu nebo přímo získat data týkající se událostí v omezených případech zvláštní naléhavosti (kodex zásad pro komunikační údaje, body 6.10–6.14, viz poznámka pod čarou 323).

([334]) Kodex zásad pro komunikační údaje, body 8.8–8.44, viz poznámka pod čarou 323.

([335]) Kodex zásad stanoví, že „schvalující osoba musí posuzování těchto návrhů věnovat zvláštní pozornost, včetně dodatečného zvážení toho, zda by návrhy mohly mít nezamýšlené důsledky a zda daný návrh nejlépe slouží veřejnému zájmu“ (kodex zásad pro komunikační údaje, bod 8.8). Kromě toho musí být o tomto druhu návrhů vedeny záznamy a při příští inspekci by tyto návrhy měly být označeny upozorněním komisaři pro kontrolu vyšetřovacích pravomocí (kodex zásad pro komunikační údaje, bod 8.10, viz poznámka pod čarou 323).

([336]) Články 87 až 89 zákona o vyšetřovacích pravomocích z roku 2016.

([337]) Podle článku 90 zákona o vyšetřovacích pravomocích z roku 2016 může poskytovatel telekomunikačních služeb, kterému je vydána výzva k uchovávání údajů, požádat ministra, který výzvu vydal, o její přezkum.

([338]) Podle čl. 87 odst. 2 písm. a) zákona o vyšetřovacích pravomocích z roku IPA 2016 může výzva k uchovávání údajů „souviset s konkrétním poskytovatelem nebo určitým druhem poskytovatelů“.

([339]) Těmito účely jsou: i) zájmy národní bezpečnosti; ii) „příslušný účel související s trestnou činností“ (ve smyslu čl. 87 odst. 10A zákona o vyšetřovacích pravomocích z roku 2016); iii) zájmy hospodářského blahobytu Spojeného království, pokud jsou tyto zájmy významné i z hlediska zájmů národní bezpečnosti; iv) zájmy veřejné bezpečnosti; v) předcházení úmrtí či zranění nebo jakékoli újmě na fyzickém či psychickém zdraví určité osoby nebo zmírnění jakéhokoli zranění nebo újmy na fyzickém či psychickém zdraví určité osoby nebo vi) pomoc při vyšetřování údajných justičním omylů (článek 87 zákona o vyšetřovacích pravomocích).

([340]) Článek 87 zákona o vyšetřovacích pravomocích z roku 2016. Kromě toho se podle příslušného kodexu zásad k posouzení přiměřenosti výzvy k uchovávání údajů použijí kritéria, která stanoví čl. 2 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016, jmenovitě povinnost posoudit, zda by bylo možné cíle, kterého má být výzvou dosaženo, rozumně dosáhnout jinými, méně rušivými prostředky. Podobně jako při posouzení přiměřenosti získání komunikačních údajů kodex zásad pro komunikační údaje objasňuje, že toto posouzení zahrnuje „vyvážení míry zásahu do práva jednotlivce na respektování jeho soukromého života vůči konkrétnímu prospěchu pro vyšetřování“ (kodex zásad pro komunikační údaje, bod 16.3, viz poznámka pod čarou 323).

z roku 2016 ([341]), ministr musí před vydáním výzvy k uchovávání údajů zohlednit: pravděpodobné přínosy výzvy ([342]); popis telekomunikačních služeb; vhodnost omezení údajů, které mají být uchovávány, s odkazem na místo nebo popisy osob, kterým jsou poskytovány telekomunikační služby ([343]); pravděpodobný počet uživatelů (je-li znám) jakékoli telekomunikační služby, které se výzva týká ([344]); technickou proveditelnost vyhovění výzvě; pravděpodobné náklady na vyhovění výzvě a jakýkoli jiný vliv výzvy na poskytovatele telekomunikačních služeb (nebo popis poskytovatelů), kterého se týká ([345]). Jak je dále upřesněno v kapitole 17 kodexu zásad pro komunikační údaje, všechny výzvy k uchovávání údajů musí specifikovat každý druh údajů, který má být uchováván, a to, jak daný druh údajů splňuje nezbytné testy pro uchování.

(209) Ve všech případech (pro účely národní bezpečnosti i pro účely vymáhání práva) musí rozhodnutí ministra vydat výzvu k uchovávání údajů schválit nezávislý soudní komisař v rámci tzv. postupu dvojitého zámku, a tento komisař musí zejména přezkoumat, zda je výzva k uchovávání příslušných komunikačních údajů nezbytná a přiměřená pro jeden nebo více zákonných účelů ([346]).

3.3.1.1.3 Vzdálený síťový přístup k zařízení

(210) Vzdálený síťový přístup k zařízení je soubor technik používaných k získávání různých údajů ze zařízení ([347]), která zahrnují počítače, tablety a chytré telefony, jakož i kabely, vodiče a paměťová zařízení ([348]). Vzdálený síťový přístup k zařízení umožňuje získat jak obsah komunikace, tak údaje týkající se zařízení ([349]).

(211) V souladu s čl. 13 odst. 1 zákona o vyšetřovacích pravomocích z roku 2016 vyžaduje použití vzdáleného síťového přístupu k zařízení zpravodajskou službou povolení formou příkazu podle postupu „dvojitého zámku“ ve smyslu zákona o vyšetřovacích pravomocích z roku 2016, za předpokladu, že existuje „spojení s Britskými ostrovy“ ([350]). Podle vysvětlení, která poskytly orgány Spojeného království, by v situacích, kdy jsou údaje předávány z Evropské

([341]) Viz článek 88 zákona o vyšetřovacích pravomocích z roku 2016.

([342]) Přínosy mohou být existující nebo plánované a musí být v souladu se zákonnými účely, pro které lze údaje uchovávat (kodex zásad pro komunikační údaje, bod 17.17, viz poznámka pod čarou 323).

([343]) Tyto úvahy budou zahrnovat určení toho, zda je plný zeměpisný dosah výzvy k uchovávání údajů nezbytný a přiměřený a zda je nezbytné a přiměřené zahrnout nebo vyloučit konkrétní popisy osob (kodex zásad pro komunikační údaje, bod 17.17, viz poznámka pod čarou 323).

([344]) To ministrovi pomůže posoudit míru narušení soukromí zákazníků i pravděpodobné přínosy údajů, které mají být uchovávány (kodex zásad pro komunikační údaje, bod 17.17, viz poznámka pod čarou 323).

([345]) Článek 88 zákona o vyšetřovacích pravomocích z roku 2016.

([346]) Článek 89 zákona o vyšetřovacích pravomocích z roku 2016.

([347]) Podle čl. 135 odst. 1 a čl. 198 odst. 1 zákona o vyšetřovacích pravomocích z roku 2016 „zařízení“ zahrnuje zařízení produkující elektromagnetické, akustické nebo jiné emise a jakýkoli přístroj, který lze ve spojení s takovým zařízením použít.

([348]) Code of Practice on Equipment Interference (kodex zásad pro vzdálený síťový přístup k zařízení), k dispozici na této adrese: 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 o zařízení jsou definovány v článku 100 zákona o vyšetřovacích pravomocích z roku 2016 jako systémová data a údaje, které jsou a) obsaženy v určité komunikaci nebo jakékoli jiné jednotlivé informaci, zahrnuty jako součást komunikace/informace, připojeny ke komunikaci/informaci nebo s komunikací/informací logicky spojeny (ať už odesílatelem nebo jinak); b) je možné je logicky oddělit od zbytku komunikace nebo jednotlivé informace a c) pokud by byly takto odděleny, neodhalily by nic z toho, co by bylo možné rozumně považovat za smysl dané komunikace nebo jednotlivé informace (pokud existuje).

([350]) Aby byl požadavek příkazu povinný, čl. 13 odst. 1 zákona o vyšetřovacích pravomocích z roku 2016 rovněž vyžaduje, aby jednání, které je předmětem šetření zpravodajské služby, zakládalo jeden nebo více trestných činů podle článku 1 až 3A zákona o zneužití počítačů z roku 1990, což by nastalo v drtivé většině situací, viz kodex zásad pro vzdálený síťový přístup k zařízení, body 3.32 a 3.6 až 3.9). Podle čl. 13 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016 „spojení s Britskými ostrovy“ existuje, pokud a) k jakékoli části jednání došlo na Britských ostrovech (bez ohledu na umístění zařízení, které by bylo nebo mohlo být předmětem přístupu); b) zpravodajská služba je přesvědčena, že kterékoli ze zařízení, které by bylo nebo mohlo být předmětem přístupu, by bylo nebo mohlo být na Britských ostrovech v době, kdy ke vzdálenému síťovému přístupu k zařízení dojde, nebo c) účelem vzdáleného síťového přístupu k zařízení je získat i) komunikaci zaslanou osobou nebo osobě, která se skutečně nebo podle přesvědčení zpravodajské služby aktuálně nachází na Britských ostrovech; ii) soukromé informace týkající se jednotlivce, který se skutečně nebo podle přesvědčení zpravodajské služby aktuálně nachází na Britských ostrovech, nebo iii) údaje o zařízení, které tvoří součást komunikace nebo soukromých informací podle pododstavce i) nebo ii) nebo jsou s takovou komunikací nebo soukromými informacemi spojeny.

unie do Spojeného království v rámci působnosti tohoto rozhodnutí, vždy existovalo „spojení s Britskými ostrovy“ a jakýkoli vzdálený síťový přístup k zařízení zahrnující takové údaje by proto podléhal požadavku povinného příkazu podle čl. 13 odst. 1 zákona o vyšetřovacích pravomocích z roku 2016 ([351]).

(212) Pravidla týkající se příkazů k cílenému vzdálenému síťovému přístupu k zařízení jsou stanovena v části 5 zákona o vyšetřovacích pravomocích z roku 2016. Podobně jako cílený odposlech se cílený vzdálený síťový přístup k zařízení musí vztahovat ke konkrétnímu „cíli“, který musí být v příkazu vymezen ([352]). Podrobnosti o tom, jak musí být „cíl“ identifikován, závisí na dané záležitosti a druhu zařízení, do něhož se má přístup uskutečnit. Zejména čl. 115 odst. 3 zákona o vyšetřovacích pravomocích specifikuje prvky, které by měly být v příkazu obsaženy (např. jméno osoby nebo organizace, popis místa), v závislosti například na tom, zda se přístup týká zařízení, které náleží určité osobě nebo organizaci nebo skupině osob, používá je určitá osoba nebo organizace nebo skupina osob nebo je zařízení v držení určité osoby nebo organizace nebo skupiny osob, nachází se na konkrétním místě atd. ([353]) Účely, pro které lze vydat příkazy k cílenému vzdálenému síťovému přístupu k zařízení, závisí na orgánu veřejné moci, který vydá návrh na vydání příkazu ([354]).

(213) Obdobně jako u cíleného odposlechu musí vydávající orgán zvážit, zda je opatření nezbytné k dosažení konkrétního účelu a zda je přiměřené cíli, kterého má být dosaženo ([355]). Kromě toho by měl rovněž zvážit, zda existují záruky, pokud jde o zabezpečení, uchovávání a zpřístupňování, jakož i pokud jde o „zahraniční zpřístupnění“ ([356])(viz 196. bod odůvodnění).

(214) Pokud se nejedná o naléhavý případ, musí příkaz schválit soudní komisař ([357]). Pokud jde o naléhavý případ, musí být soudní komisař o vydání příkazu informován a musí jej schválit do tří pracovních dnů. Pokud soudní komisař odmítne příkaz schválit, pozbude příkaz účinnosti a nesmí být obnoven ([358]). Soudní komisař má také pravomoc vyžadovat, aby byly jakékoli údaje získané na základě příkazu vymazány ([359]). Skutečnost, že byl zatykač vydán za naléhavých okolností, nemá vliv na následný dohled (viz 244. až 255. bod odůvodnění), ani na možnosti jednotlivců požadovat nápravu (viz 260. až 270. bod odůvodnění). Jednotlivci mohou obvyklým způsobem podat stížnost u Úřadu komisaře pro informace nebo uplatnit nárok týkající se jakéhokoli údajného jednání u tribunálu pro kontrolu vyšetřovacích pravomocí. Ve všech případech soudní komisař při rozhodování o schválení či neschválení příkazu použije test nezbytnosti a přiměřenosti použitelný na žádosti o cílené odposlechy ([360]) (viz 192. bod odůvodnění výše).

([351]) Pro úplnost je třeba upozornit, že i v situacích, kdy neexistuje „spojení s Britskými ostrovy“ a použití vzdáleného síťového přístupu k zařízení proto nepodléhá požadavku povinného příkazu podle č. 13 odst. 1 zákona o vyšetřovacích pravomocích z roku 2016, by zpravodajská služba, která hodlá provozovat činnost, pro kterou může získat příkaz k hromadnému vzdálenému síťovému přístupu k zařízení, měla tento příkaz podle obecné politiky získat (viz kodex zásad pro vzdálený síťový přístup k zařízení, bod 3.24). I v případě, že příkaz ke vzdálenému síťovému přístupu k zařízení podle zákona o vyšetřovacích pravomocích z roku 2016 není ze zákona vyžadován, ani získáván podle obecné politiky, podléhají kroky zpravodajských služeb řadě podmínek a omezení podle článku 7 zákona o zpravodajských službách z roku 1994. To zahrnuje zejména požadavek povolení vydaného ministrem, který musí být přesvědčen, že žádné opatření nepřekračuje rámec toho, co je nezbytné pro řádný výkon funkcí zpravodajské služby.

([352]) Článek 115 zákona o vyšetřovacích pravomocích z roku 2016 upravuje obsah příkazu a stanoví, že příkaz musí obsahovat jméno nebo popis osob, organizací, místa nebo skupiny osob, které představují „cíl“, popis povahy vyšetřování a popis činností, pro které se zařízení používá. Musí také popisovat druh zařízení a jednání, k němuž je osoba, které je příkaz adresován, oprávněna.

([353]) Viz také kodex zásad pro vzdálený síťový přístup k zařízení, bod 5.7, viz poznámka pod čarou 348.

([354]) Národní bezpečnostní služby mohou o příkaz k vzdálenému síťovému přístupu k zařízení požádat, pokud je to nezbytné pro účely národní bezpečnosti, pro účely odhalování závažné trestné činnosti a/nebo v zájmech hospodářského blahobytu Spojeného království, pokud jsou tyto zájmy významné i z hlediska zájmů národní bezpečnosti (články 102–103 zákona o vyšetřovacích pravomocích z roku 2016). Podle dané služby může být příkaz k vzdálenému síťovému přístupu k zařízení požadován pro účely vymáhání práva, pokud je to nezbytné pro odhalování nebo prevenci závažné trestné činnosti nebo pro předcházení úmrtí či zranění nebo jakékoli újmě na fyzickém či psychickém zdraví určité fyzické osoby nebo zmírnění jakéhokoli zranění nebo újmy na fyzickém či psychickém zdraví určité fyzické osoby (viz čl. 106 odst. 1 a čl. 106 odst. 3 zákona o vyšetřovacích pravomocích z roku 2016).

([355]) Ustanovení čl. 102 odst. 1 zákona o vyšetřovacích pravomocích z roku 2016.

([356]) Články 129–131 zákona o vyšetřovacích pravomocích z roku 2016.

([357]) Článek 109 zákona o vyšetřovacích pravomocích z roku 2016.

([358]) Ustanovení čl. 109 odst. 4 zákona o vyšetřovacích pravomocích z roku 2016.

([359]) Ustanovení čl. 110 odst. 3 písm. b) zákona o vyšetřovacích pravomocích z roku 2016. Podle bodu 5.67 kodexu zásad pro vzdálený síťový přístup k zařízení je naléhavost určena tím, zda by bylo přiměřeně proveditelné požádat soudního komisaře o souhlas s vydáním příkazu v době, která je k dispozici pro naplnění potřeby v oblasti operativní činnosti nebo vyšetřování. Naléhavé příkazy by měly spadat do jedné nebo obou následujících kategorií: i) bezprostřední ohrožení života nebo hrozba závažné újmy, například pokud byla osoba unesena a má se za to, že je bezprostředně ohrožen její život, nebo ii) příležitost k získání zpravodajských informací nebo vyšetřování, která má časové omezení,– například pokud má do Spojeného království vstoupit zásilka drog třídy A a donucovací orgány chtějí získat informace o pachatelích závažné trestné činnosti, aby provedly zatčení. Viz poznámka pod čarou 348.

([360]) Článek 108 zákona o vyšetřovacích pravomocích z roku 2016.

(215) A konečně se také na vzdálený síťový přístup k zařízení vztahují zvláštní záruky použitelné na cílené odposlechy, pokud jde o dobu platnosti, prodloužení a úpravu příkazu, jakož i o odposlech poslanců parlamentu Spojeného království, záležitostí podléhajících povinnosti mlčenlivosti a novinářských materiálů (další podrobnosti viz 193. bod odůvodnění).

3.3.1.1.4 Výkon hromadných pravomocí

(216) Hromadné pravomoci upravuje část 6 zákona o vyšetřovacích pravomocích z roku 2016. Další podrobnosti týkající se použití hromadných pravomocí stanoví i kodexy zásad. Ačkoli v právu Spojeného království neexistuje definice „hromadné pravomoci", v kontextu zákona o vyšetřovacích pravomocích z roku 2016 byla popsána jako shromažďování a uchovávání velkého množství údajů získaných vládou různými prostředky (tj. pravomoci hromadného odposlechu, hromadného získávání, hromadného vzdáleného síťového přístupu k zařízení a hromadných souborů osobních údajů), k nimž mohou mít následně orgány přístup. Tento popis je objasněn srovnáním s tím, co „hromadná pravomoc" není: nerovná se „plošnému sledování" bez omezení nebo záruk. Naopak, jak je vysvětleno níže, zahrnuje omezení a záruky, jejichž cílem je zajistit, aby přístup k údajům nebyl poskytován nerozlišujícím nebo neodůvodněným způsobem ([361]). Hromadné pravomoci lze použít pouze zejména v případě, že je stanoveno spojení mezi technickým opatřením, které národní zpravodajská služba hodlá použít, a operačním cílem, pro který je takové opatření požadováno.

(217) Hromadné pravomoci jsou navíc k dispozici pouze zpravodajským službám a vždy vyžadují příkaz vydaný ministrem zahraničí a schválený soudním komisařem. Při volbě prostředků pro shromažďování zpravodajských informací je třeba zvážit, zda lze dotyčného cíle dosáhnout „méně rušivými prostředky" ([362]). Tento přístup vyplývá z rámce právních předpisů, který se opírá o zásadu přiměřenosti, a proto upřednostňuje cílené shromažďování před hromadným.

3.3.1.1.4.1 Hromadný odposlech a hromadný vzdálený síťový přístup k zařízení

(218) Režim pro hromadný odposlech je uveden v kapitole 1 části 6 zákona o vyšetřovacích pravomocích z roku 2016, zatímco kapitola 3 téže části upravuje hromadný vzdálený síťový přístup k zařízení. Tyto režimy jsou v podstatě stejné, podmínky a další záruky použitelné na tyto příkazy jsou tudíž analyzovány společně.

i) *Podmínky a kritéria pro vydání příkazu*

(219) Příkaz k hromadnému odposlechu se omezuje na odposlech komunikace v průběhu přenosu této komunikace odesílané nebo přijímané osobami mimo Britské ostrovy ([363]), tzv. komunikace související se zahraničím ([364]),

([361]) Podle zprávy o hromadných pravomocích, kterou přednesl Lord David Anderson, nezávislý recenzent právních předpisů v oblasti boje proti terorismu, před schválením zákona o vyšetřovacích pravomocích z roku 2016, *„by mělo být zřejmé, že hromadné shromažďování a uchovávání údajů se nerovná „plošnému sledování". Jakýkoli právní systém hodný svého názvu bude obsahovat omezení a záruky navržené právě k tomu, aby zajistily, že přístup k úložištím citlivých údajů (…) nebude poskytován nerozlišujícím nebo neodůvodněným způsobem. Takováto omezení a záruky v návrhu zákona nepochybně existují."* Lord David Anderson, Zpráva o přezkumu hromadných pravomocí, srpen 2016, bod 1.9 (zvýraznění doplněno), k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF

([362]) Ustanovení čl. 2 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016. Viz například kodex zásad pro hromadné získávání komunikačních údajů, bod 4.11, k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf

([363]) „Britské ostrovy" zahrnují Spojené království, britské Normanské ostrovy a Ostrov Man a jsou definovány v příloze 1 výkladového zákona z roku 1978, k dispozici na této adrese: https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

([364]) Podle článku 136 zákona o vyšetřovacích pravomocích z roku 2016 se „komunikacemi souvisejícími se zahraničím" rozumí: i) sdělení zasílaná osobami, které se nacházejí mimo Britské ostrovy, nebo ii) sdělení přijímaná osobami, které se nacházejí mimo Britské ostrovy. Tento režim, jak potvrdily orgány Spojeného království, zahrnuje také komunikaci mezi dvěma osobami, které se obě nacházejí mimo Britské ostrovy. Velký senát Evropského soudu pro lidská práva ve věci Big Brother Watch and others v United Kingdom (viz poznámka pod čarou 279 výše) v bodě 376 konstatoval, že pokud jde o podobné omezení komunikace (s odkazem na „externí komunikaci"), kterou lze zachytit hromadným odposlechem podle zákona o úpravě vyšetřovacích pravomocí z roku 2000, bylo toto omezení dostatečně vymezené a předvídatelné.

jakož i další související údaje a následný výběr zachyceného materiálu pro šetření ([365]). Příkaz k hromadnému vzdálenému síťovému přístupu k zařízení ([366]) opravňuje adresáta k zajištění přístupu do jakéhokoli zařízení za účelem získání komunikací souvisejících se zahraničím (včetně čehokoli, co zahrnuje řeč, hudbu, zvuky, vizuální obrazy nebo data jakéhokoli popisu), údajů o zařízení (údajů, které umožňují nebo usnadňují fungování poštovní služby; telekomunikačního systému; telekomunikační služby) nebo jakékoli jiné informace ([367]).

(220) Ministr může vydat hromadný příkaz pouze na návrh podaný ředitelem zpravodajské služby ([368]). Příkaz povolující hromadný odposlech nebo vzdálený síťový přístup k zařízení musí být vydán pouze v případě, že je to nezbytné v zájmu národní bezpečnosti a pro další účel prevence nebo odhalování závažné trestné činnosti nebo v zájmu hospodářského blahobytu Spojeného království, pokud je tento zájem významný pro národní bezpečnost ([369]). Kromě toho čl. 142 odst. 7 zákona o vyšetřovacích pravomocích z roku 2016 vyžaduje, aby byl příkaz k hromadnému odposlechu specifikován podrobněji než pouhým odkazem na „zájmy národní bezpečnosti", „hospodářský blahobyt Spojeného království" a „předcházení závažné trestné činnosti a její potírání", ale aby byla stanovena spojitost mezi požadovaným opatřením a jedním nebo více operativními účely, které musí být v příkazu uvedeny.

(221) Volba operativního účelu je výsledkem vícevrstvého procesu. Ustanovení čl. 142 odst. 4 stanoví, že operativní účely uvedené v příkazu musí být upřesněny v seznamu vedeném vedoucími představiteli zpravodajských služeb jakožto účely, které považují za operativní účely, pro které mohou být zachycený obsah nebo sekundární údaje získané na základě příkazů k hromadnému odposlechu vybrány k šetření. Seznam operativních účelů musí schválit ministr. Ministr může takový souhlas udělit pouze za předpokladu, že je přesvědčen, že operativní účel je specifikován podrobněji než obecné důvody pro povolení příkazu (národní bezpečnost nebo národní bezpečnost a hospodářský blahobyt nebo prevence závažné trestné činnosti) ([370]). Na konci každého příslušného tříměsíčního období musí ministr předat kopii seznamu operativních účelů parlamentnímu výboru pro zpravodajské služby a bezpečnost. A konečně také musí seznam operativních účelů alespoň jednou ročně přezkoumat předseda vlády ([371]). Jak uvedl Vrchní soud, „[t]ato opatření nelze považovat za nevýznamné záruky, protože společně vytvářejí složitý soubor režimů odpovědnosti, do nichž je zapojen Parlament Spojeného království i členové vlády na nejvyšší úrovni" ([372]).

(222) Tyto operativní účely také omezují rozsah výběru zachyceného materiálu pro fázi šetření. Výběr jakéhokoli materiálu shromážděného v rámci příkazu k hromadnému odposlechu k šetření musí být odůvodněn s ohledem na operativní účel(y). Jak vysvětlily orgány Spojeného království, znamená to, že ministr musí posoudit praktický režim šetření již ve fázi vydávání příkazu a musí být uvedeny dostatečné podrobnosti ke splnění zákonných povinností podle článků 152 a 193 zákona o vyšetřovacích pravomocích z roku 2016 ([373]). Podrobnosti poskytnuté ministrovi v souvislosti s těmito režimy by musely zahrnovat například (případné) informace o tom, jak se mohou měnit režimy filtrování v době účinnosti příkazu ([374]). Další podrobnosti o postupu a zárukách použitých pro fáze filtrování a šetření viz 229. bod odůvodnění níže.

([365]) Ustanovení čl. 136 odst. 4 zákona o vyšetřovacích pravomocích z roku 2016. Podle vysvětlení obdržených od vlády Spojeného království lze hromadné odposlechy použít například k identifikaci dříve neznámých hrozeb pro národní bezpečnost Spojeného království, a to filtrováním a analýzou zachyceného materiálu za účelem identifikace komunikace zpravodajské hodnoty (britský vysvětlující rámec, oddíl H: Národní bezpečnost, s. 27–28, viz poznámka pod čarou 29). Jak vysvětlily orgány Spojeného království, tyto nástroje lze použít k určení spojení mezi známými zájmovými subjekty, jakož i k hledání stop činnosti jednotlivců, kteří dosud nemusí být známi, ale objeví se v průběhu vyšetřování, a k identifikaci vzorců činnosti, které mohou naznačovat hrozbu pro Spojené království.

([366]) V souladu s čl. 13 odst. 1 zákona o vyšetřovacích pravomocích z roku 2016 vyžaduje použití vzdáleného síťového přístupu k zařízení zpravodajskou službou povolení formou příkazu podle zákona o vyšetřovacích pravomocích z roku 2016, pokud existuje „spojení s Britskými ostrovy" viz (211). bod odůvodnění.

([367]) Článek 176 zákona o vyšetřovacích pravomocích z roku 2016. Příkaz k hromadnému vzdálenému síťovému přístupu k zařízení nesmí povolit jednání, které by (pokud by nebylo provedeno ze zákona oprávněným orgánem) zakládalo protiprávní odposlech (s výjimkou uchovávané komunikace). Podle britského vysvětlujícího rámce by získané informace mohly být nezbytné pro identifikaci zájmových subjektů a obvykle by šlo o vhodné operace velkého rozsahu (britský vysvětlující rámec, oddíl H: Národní bezpečnost, s. 28, viz poznámka pod čarou 29).

([368]) Ustanovení čl. 138 odst. 1 a čl. 178 odst. 1 zákona o vyšetřovacích pravomocích z roku 2016.

([369]) Ustanovení čl. 138 odst. 2 a čl. 178 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016.

([370]) Podle vysvětlení, které poskytly orgány Spojeného království, může například operativní účel omezovat oblast působnosti opatření na existenci hrozby v konkrétní zeměpisné oblasti.

([371]) Ustanovení čl. 142 odst. 4–10 zákona o vyšetřovacích pravomocích z roku 2016.

([372]) Vrchní soud, rozsudek ve věci Liberty, [2019] EWHC 2057 (Admin), bod 167.

([373]) Články 152 a 193 zákona o vyšetřovacích pravomocích z roku 2016 vyžadují: a) výběr pro šetření se provádí pouze pro operativní účely upřesněné v příkazu; b) výběr pro šetření je za všech okolností nezbytný a přiměřený a c) výběr pro šetření neporušuje zákaz výběru materiálu a identifikace komunikace, která byla odeslána jednotlivci nebo je určena jednotlivcům, o nichž je známo, že se v dané době nacházejí na Britských ostrovech.

([374]) Viz kodex zásad pro odposlech komunikace, bod 6.6, viz poznámka pod čarou 278.

(223) Hromadnou pravomoc lze povolit, pouze pokud je přiměřená cíli, kterého má být dosaženo ([375]). Jak je stanoveno v kodexu zásad pro odposlech, každé posouzení přiměřenosti zahrnuje „vyvážení závažnosti zásahu do soukromí (a dalších aspektů uvedených v čl. 2 odst. 2) vůči nezbytnosti dané činnosti z hlediska vyšetřovacího, operativního nebo kapacitního. Povolené jednání by mělo nabízet reálnou vyhlídku na dosažení očekávaného přínosu a nemělo by být nepřiměřené nebo svévolné“ ([376]). Jak již bylo zmíněno, v praxi to znamená, že test přiměřenosti je založen na testu rovnováhy mezi tím, čeho má být dosaženo („operativní účel(y)“), a dostupnými technickými možnostmi (např. cílené nebo hromadné odposlechy, vzdálený síťový přístup k zařízení, získávání komunikačních údajů), přičemž se upřednostňují nejméně rušivé prostředky (viz 181. a 182. bod odůvodnění výše). Pokud je pro daný cíl vhodné více než jedno opatření, musí být upřednostněny méně rušivé prostředky.

(224) Dodatečná záruka při posuzování přiměřenosti požadovaného opatření je zajištěna tím, že ministr musí obdržet příslušné informace potřebné k řádnému provedení jeho posouzení. Kodex zásad pro odposlech a kodex zásad pro vzdálený síťový přístup k zařízení zejména vyžadují, aby návrh podaný příslušným orgánem uváděl souvislosti žádosti, popis komunikace, která má být odposlouchávána, a poskytovatele telekomunikačních služeb, kteří mají být nápomocni, popis jednání, které má být povoleno, operativní účely a vysvětlení, proč je dané jednání nezbytné a přiměřené ([377]).

(225) A v neposlední řadě je důležité, že rozhodnutí ministra vydat příkaz musí být schváleno nezávislým soudním komisařem, který posoudí hodnocení nezbytnosti a přiměřenosti navrhovaného opatření, a to za použití stejných zásad, jaké by použil soud u návrhu na soudní přezkum ([378]). Konkrétně soudní komisař přezkoumá závěry ministra z hlediska toho, zda je příkaz nezbytný a zda je jednání přiměřené z hlediska zásad stanovených v čl. 2 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016 (obecné povinnosti týkající se soukromí). Soudní komisař rovněž přezkoumá závěry ministra, pokud jde o to, zda je každý z operativních účelů uvedených v příkazu účelem, který vyžaduje nebo může vyžadovat výběr. Pokud soudní komisař odmítne schválit rozhodnutí o vydání příkazu, může ministr buď: i) rozhodnutí přijmout, a tudíž nevydat příkaz, nebo ii) postoupit věc komisaři pro kontrolu vyšetřovacích pravomocí k rozhodnutí (pokud původní rozhodnutí nepřijal komisař pro kontrolu vyšetřovacích pravomocí) ([379]).

ii) *Dodatečné záruky*

(226) Zákon o vyšetřovacích pravomocích z roku 2016 zavedl další omezení doby platnosti, prodloužení a úpravy hromadného příkazu. Doba platnosti příkazu nesmí přesáhnout šest měsíců a jakékoli rozhodnutí o prodloužení nebo úpravě příkazu (s výjimkou nepodstatných úprav) musí rovněž schválit soudní komisař ([380]). Kodex zásad pro odposlech a kodex zásad pro vzdálený síťový přístup k zařízení specifikovaly, že změna operativních účelů příkazu se považuje za podstatnou změnu příkazu ([381]).

([375]) Ustanovení čl. 138 odst. 1 písm. b) a c) a čl. 178 písm. b) a c) zákona o vyšetřovacích pravomocích z roku 2016.

([376]) Kodex zásad pro odposlech komunikace, bod 4.10, viz poznámka pod čarou 278.

([377]) Kodex zásad pro odposlech komunikace, bod 6.20, viz poznámka pod čarou 278, a kodex zásad pro vzdálený síťový přístup k zařízení, bod 6.13, viz poznámka pod čarou 348.

([378]) Ustanovení čl. 138 odst. 1 písm. g) a čl. 178 odst. 1 písm. f) zákona o vyšetřovacích pravomocích z roku 2016. Za důležitou záruku proti zneužití v rámci hromadného odposlechu Evropský soud pro lidská práva označil zejména povolení, které předem vydá nezávislý subjekt. Evropský soud pro lidská práva (velký senát), věc Big Brother Watch and others v United Kingdom (viz poznámka pod čarou 269 výše), body 351 a 352. Je důležité mít na paměti, že tento rozsudek se týkal předchozího právního rámce (zákona o úpravě vyšetřovacích pravomocí z roku 2000), který neobsahoval některé záruky (včetně předem vydaného povolení nezávislého soudního komisaře), jež zavedl zákon o vyšetřovacích pravomocích z roku 2016.

([379]) Ustanovení čl. 159 odst. 3 a 4 zákona o vyšetřovacích pravomocích z roku 2016.

([380]) Články 143–146 a 184–188 zákona o vyšetřovacích pravomocích z roku 2016. V případě naléhavé úpravy může ministr provést změnu bez souhlasu, musí však vyrozumět komisaře a komisař poté musí rozhodnout, zda úpravu schválí, nebo zamítne (článek 147 zákona o vyšetřovacích pravomocích z roku 2016). Příkazy musí být zrušeny, pokud již nejsou nezbytné nebo přiměřené, nebo pokud již není nezbytné šetřit zachycený obsah, metadata nebo jiná data získaná na základě příkazu pro žádný z operativních účelů uvedených v příkazu (články 148 a 189 zákona o vyšetřovacích pravomocích z roku 2016).

([381]) Kodex zásad pro odposlech komunikace, body 6.44–6.47, viz poznámka pod čarou 278, a kodex zásad pro vzdálený síťový přístup k zařízení, bod 6.48, viz poznámka pod čarou 348.

(227) Obdobně tomu, co je stanoveno pro cílené odposlechy, stanoví část 6 zákona o vyšetřovacích pravomocích z roku 2016, že ministr musí zajistit, aby byla v platnosti opatření zajišťující záruky uchovávání a zpřístupňování materiálu získaného na základě příkazu ([382]), jakož i pro zahraniční zpřístupnění ([383]). Ustanovení čl. 150 odst. 5 a čl. 191 odst. 5 zákona o vyšetřovacích pravomocích z roku 2016 vyžadují zejména , aby každá kopie kteréhokoli z těchto materiálů shromážděných na základě příkazu byla uložena bezpečně a byla zničena, jakmile již nebudou existovat žádné podstatné důvody pro její uchovávání, zatímco ustanovení čl. 150 odst. 2 a čl. 191 odst. 2 vyžadují, aby počet osob, kterým je materiál zpřístupněn, a rozsah, v jakém je jakýkoli materiál zveřejněn, zpřístupněn, zpřístupňován nebo kopírován, byl omezen na minimum, které je pro zákonné účely nezbytné ([384]).

(228) A konečně, pokud má být materiál, který byl zachycen prostřednictvím hromadného odposlechu nebo hromadného vzdáleného síťového přístupu k zařízení, předán třetí zemi („zahraniční zpřístupnění"), zákon o vyšetřovacích pravomocích z roku 2016 stanoví, že ministr se musí ujistit, že existuje zvláštní vhodný režim, který zaručí, že v této třetí zemi budou existovat obdobné záruky zabezpečení, uchovávání a zpřístupňování ([385]). Kromě toho článek 109 zákona o ochraně údajů z roku 2018 stanoví zvláštní požadavky na mezinárodní předávání osobních údajů zpravodajskými službami třetím zemím nebo mezinárodním organizacím a nepovoluje předávat osobní údaje do země nebo na území mimo Spojené království nebo mezinárodní organizaci, pokud není předání nezbytné a přiměřené pro účely zákonných funkcí správce nebo pro jiné účely stanovené v čl. 2 odst. 2 písm. a) zákona o Bezpečnostní službě z roku 1989 nebo v čl. 2 odst. 2 písm. a) a čl. 4 odst. 2 písm. a) zákona o zpravodajských službách z roku 1994 ([386]). Důležité je, že tyto požadavky se použijí i v případech, v nichž je uplatněna výjimka z důvodu národní bezpečnosti podle článku 110 zákona o ochraně údajů z roku 2018, neboť článek 110 zákona o ochraně údajů z roku 2018 neuvádí článek 109 zákona o ochraně údajů z roku 2018 jako jedno z ustanovení, které se nemusí použít, pokud je pro účely ochrany národní bezpečnosti nutná výjimka z určitých ustanovení.

(229) Jakmile je příkaz schválen a údaje hromadně získány, budou údaje před prozkoumáním podrobeny výběru. Fáze výběru a šetření podléhá dalšímu testu přiměřenosti provedenému analytikem, který na základě operativních účelů uvedených v příkazu (a potenciálně existujících režimů filtrování) vymezí kritéria výběru. Jak stanoví články 152 a 193 zákona o vyšetřovacích pravomocích, ministr se musí při vydání příkazu ujistit, že existuje zvláštní vhodný režim, který zaručí, že výběr materiálu bude proveden pouze pro stanovené operativní účely a že bude za všech okolností nezbytný a přiměřený. V tomto ohledu orgány Spojeného království objasnily, že hromadně zachycený materiál se vybírá především automatizovaným filtrováním, které má vyřadit údaje, u nichž není pravděpodobné, že by měly význam z hlediska národní bezpečnosti. Filtry se budou dle potřeby lišit (podle průběžných změn vzorců, druhů a protokolů internetového provozu) a budou záviset na technologii a operativních souvislostech. Po této fázi lze údaje vybrat k šetření, pouze pokud jsou důležité pro operativní účely uvedené v příkazu ([387]). Záruky stanovené zákonem o vyšetřovacích pravomocích z roku 2016 pro šetření shromážděného materiálu se použijí pro jakýkoli druh údajů (odposlechnutý obsah i sekundární údaje) ([388]). Články 152 a 193 zákona o vyšetřovacích pravomocích z roku 2016 rovněž stanoví obecný zákaz vybírat k šetření materiál, který se týká rozhovorů zaslaných jednotlivci nebo určených jednotlivcům, kteří se nacházejí na Britských ostrovech. Pokud orgány chtějí takový materiál prozkoumat, podají žádost o vydání příkazu k cílenému šetření podle části 2 a části 4 zákona o vyšetřovacích pravomocích z roku 2016, který vydá ministr a schválí soudní komisař ([389]). Pokud určitá osoba záměrně vybere zachycený obsah k šetření v rozporu s požadavky stanovenými v právních předpisech ([390]), dopustí se trestného činu ([391]).

([382]) Článek 156 zákona o vyšetřovacích pravomocích z roku 2016.

([383]) Články 150 a 191 zákona o vyšetřovacích pravomocích z roku 2016.

([384]) Velký senát Evropského soudu pro lidská práva ve věci Big Brother Watch and others v United Kingdom (viz poznámka pod čarou 268 výše) potvrdil systém dodatečných záruk pro uchovávání údajů, přístup k údajům a zveřejňování údajů, který byl stanoven v rámci zákona o úpravě vyšetřovacích pravomocí z roku 2000, viz body 392–394 a 402–405. Tentýž systém záruk poskytuje zákon o vyšetřovacích pravomocích z roku 2016.

([385]) Články 151 a 192 zákona o vyšetřovacích pravomocích z roku 2016.

([386]) Další informace o těchto účelech viz poznámka pod čarou 312.

([387]) Kodexy pro odposlech komunikace v tomto ohledu specifikují: „Tyto systémy zpracování zpracovávají data z komunikačních linek nebo signálů, které se odposlouchávající orgán rozhodl odposlouchávat. Poté se na provoz na těchto linkách a signálech použije určitý stupeň filtrování, který je navržen tak, aby vybíral druhy komunikace s potenciální zpravodajskou hodnotou a vyřazoval ty, u nichž je zpravodajská hodnota nejméně pravděpodobná. V důsledku tohoto filtrování, které se bude u různých systémů zpracování lišit, bude významná část komunikace na těchto linkách a signálech automaticky vyřazena. Poté může proběhnout další komplexní vyhledávání, aby byly vyčleněny další komunikace, které mají s největší pravděpodobností nejvyšší zpravodajskou hodnotu a dotýkají se zákonných funkcí služby. Tyto komunikace pak mohou být vybrány k šetření pro jeden nebo více operativních účelů uvedených v příkazu, pokud jsou splněny podmínky nezbytnosti a přiměřenosti. K šetření oprávněnými osobami mohou být potenciálně vybrány pouze položky, které nebyly vyřazeny při filtrování" (kodex zásad pro odposlech komunikace, bod 6.6, viz poznámka pod čarou 278).

([388]) Viz čl. 152 odst. 1 písm. a) a b) zákona o vyšetřovacích pravomocích z roku 2016, podle nichž musí být šetření obou typů údajů (odposlechnutý obsah a sekundární údaje) prováděno pouze za stanoveným účelem a musí být za všech okolností nezbytné a přiměřené.

([389]) Tento druh příkazu se nevyžaduje, pokud jsou údaje vztahující se k jednotlivcům, kteří se nacházejí na Britských ostrovech, „sekundárními údaji" (viz čl. 152 odst. 1 písm. c) zákona o vyšetřovacích pravomocích z roku 2016).

([390]) Články 152 a 193 zákona o vyšetřovacích pravomocích z roku 2016.

([391]) Články 155 a 196 zákona o vyšetřovacích pravomocích z roku 2016.

(230) Posouzení provedené analytikem při výběru materiálu podléhá následnému dohledu komisaře pro kontrolu vyšetřovacích pravomocí, který hodnotí dodržování konkrétních záruk stanovených v zákoně o vyšetřovacích pravomocích z roku 2016 pro fázi šetření ([392]) (viz také 229. bod odůvodnění). Komisař pro kontrolu vyšetřovacích pravomocí musí průběžně kontrolovat (mimo jiné prostřednictvím auditu, inspekce a vyšetřování), jak orgány veřejné moci vykonávají vyšetřovací pravomoci uvedené v zákoně o vyšetřovacích pravomocích z roku 2016 ([393]). V tomto ohledu kodex zásad pro odposlech a kodex zásad pro vzdálený síťový přístup k zařízení objasňují, že služba musí vést záznamy pro účely následných šetření a auditů a tyto záznamy musí uvádět, proč je přístup oprávněných osob k materiálu nezbytný a přiměřený, a příslušné operativní účely ([394]). Například ve své výroční zprávě za rok 2018 dospěl Úřad komisaře pro kontrolu vyšetřovacích pravomocí ([395]) k závěru, že odůvodnění zaznamenaná analytiky pro šetření určitého materiálu shromážděného hromadně splňují požadovanou normu přiměřenosti, neboť uvádějí dostatečné podrobnosti o důvodech jejich „šetření" ve vztahu k účelu, kterého má být dosaženo ([396]). Pokud jde o hromadné pravomoci, Úřad komisaře pro kontrolu vyšetřovacích pravomocí ve své zprávě za rok 2019 jasně deklaroval svůj záměr pokračovat v kontrolách hromadného odposlechu, včetně podrobného zkoumání selektorů a kritérií vyhledávání ([397]). Rovněž bude i nadále pečlivě a případ od případu zkoumat výběr opatření v oblasti sledování (cílené versus plošné), a to jak během posuzování návrhů na vydání příkazu v rámci postupu dvojitého zámku, tak při inspekcích ([398]). Toto další monitorování bude náležitě zohledněno v rámci sledování tohoto rozhodnutí Komisí podle 281.–284. bodu odůvodnění.

3.3.1.1.4.2 Hromadné získávání komunikačních údajů

(231) Kapitola 2 části 6 zákona o ochraně údajů z roku 2016 upravuje příkazy k hromadnému získávání údajů, které adresáta opravňují požadovat, aby provozovatel telekomunikační služby sdělil nebo získal jakékoli komunikační údaje, které má v držení. Tyto příkazy rovněž opravňují dožadující orgán k výběru údajů pro další fázi šetření. Stejně jako cílené uchovávání a získávání komunikačních údajů (viz 199. bod odůvodnění) se ani hromadné získávání komunikačních údajů obvykle nedotýká osobních údajů subjektů údajů z EU předávaných podle tohoto rozhodnutí do Spojeného království. Povinnost zpřístupňovat komunikační údaje podle kapitoly 2 části 6 zákona o vyšetřovacích pravomocích z roku 2016 zahrnuje údaje, které shromažďují provozovatelé telekomunikačních služeb ve Spojeném království přímo od uživatelů telekomunikační služby ([399]). Tento druh zpracování „v přímém vztahu k zákazníkovi" obvykle nezahrnuje předání na základě tohoto rozhodnutí, tj. předání správcem/zpracovatelem v EU správci/zpracovateli ve Spojeném království.

(232) Pro úplnost jsou však níže popsány podmínky a záruky, kterými se získávání hromadných komunikačních údajů řídí.

([392]) Články 152 a 193 zákona o vyšetřovacích pravomocích z roku 2016.

([393]) Článek 229 zákona o vyšetřovacích pravomocích z roku 2016.

([394]) Kodex zásad pro odposlech komunikace, bod 6.74, viz poznámka pod čarou 278, a kodex zásad pro vzdálený síťový přístup k zařízení, bod 6.78, viz poznámka pod čarou 348.

([395]) Úřad komisaře pro kontrolu vyšetřovacích pravomocí je zřízen podle článku 238 zákona o vyšetřovacích pravomocích z roku 2016, aby poskytoval komisaři pro kontrolu vyšetřovacích pravomocí potřebný personál, prostory, vybavení a jiné zařízení a služby nutné pro výkon jeho funkcí (viz (251). bod odůvodnění).

([396]) Ve výroční zprávě Úřadu komisaře pro kontrolu vyšetřovacích pravomocí za rok 2018 je uvedeno, že odůvodnění zaevidovaná analytiky GCHQ „splňovala požadovaný standard a analytici dostatečně podrobně vykazovali přiměřenost svých šetření hromadných údajů". Výroční zpráva komisaře pro kontrolu vyšetřovacích pravomocí za rok 2018, bod 6.22, viz poznámka pod čarou 464.

([397]) Výroční zpráva komisaře pro kontrolu vyšetřovacích pravomocí za rok 2019, bod 7.6, viz poznámka pod čarou 463.

([398]) Výroční zpráva komisaře pro kontrolu vyšetřovacích pravomocí za rok 2019, bod 10.22, viz poznámka pod čarou 463.

([399]) To vyplývá z definice komunikačních údajů uvedené v čl. 261 odst. 5 zákona o vyšetřovacích pravomocích z roku 2016, podle nichž jsou komunikační údaje uchovávány nebo získávány poskytovatelem telekomunikačních služeb a buď se týkají uživatele telekomunikační služby a vztahují se k poskytování této služby, nebo jsou obsaženy v určité komunikaci, zahrnuty jako součást komunikace, připojeny ke komunikaci nebo s komunikací logicky spojeny (viz také kodex zásad pro hromadné získávání komunikačních údajů, k dispozici na této adrese: 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). Definice poskytovatele telekomunikačních služeb uvedená v čl. 261 odst. 10 zákona o vyšetřovacích pravomocích z roku 2016 navíc vyžaduje, aby poskytovatelem telekomunikačních služeb byla osoba, která nabízí nebo poskytuje telekomunikační službu osobám ve Spojeném království nebo která ovládá nebo poskytuje telekomunikační systém, který se (zcela nebo zčásti) nachází ve Spojeném království nebo je ze Spojeného království ovládán. Tyto definice objasňují, že povinnosti podle zákona o vyšetřovacích pravomocích z roku 2016 nelze uložit poskytovatelům telekomunikačních služeb, jejichž zařízení se nenachází ve Spojeném království nebo není ze Spojeného království ovládáno, a kteří nenabízejí ani neposkytují služby osobám ve Spojeném království (viz také kodex zásad pro hromadné získávání komunikačních údajů, bod 2.2). Pokud účastníci z EU (ať se nacházejí v EU, nebo ve Spojeném království) využívají služeb ve Spojeném království, veškerá komunikace související s poskytováním této služby by byla shromažďována přímo poskytovatelem služeb ve Spojeném království a nebyla by předávána z EU.

(233) Zákon o vyšetřovacích pravomocích z roku 2016 nahrazuje právní předpisy týkající se získávání hromadných komunikačních údajů, kterých se týkal rozsudek SDEU ve věci Privacy International. Právní předpisy projednávané v uvedeném případu byly zrušeny a nový režim stanoví konkrétní podmínky a záruky, za nichž lze takové opatření povolit.

(234) Na rozdíl od předchozího režimu, kdy měl ministr při schvalování opatření plnou možnost volného uvážení ([400]), zákon o vyšetřovacích pravomocích z roku 2016 požaduje, aby ministr vydal příkaz, pouze pokud je opatření nezbytné a přiměřené. V praxi to znamená, že by měla existovat souvislost mezi přístupem k údajům a sledovaným cílem ([401]). Přesněji řečeno, ministr bude muset posoudit existenci souvislosti mezi požadovaným opatřením a jedním nebo více „operativními účely" uvedenými v příkazu (viz 219. bod odůvodnění). Pokud jde o posouzení přiměřenosti, příslušný kodex zásad stanoví, že „ministr musí vzít v úvahu, zda by bylo možné cíle, kterého má být příkazem dosaženo, rozumně dosáhnout jinými, méně rušivými prostředky (čl. 2 odst. 2 písm. a) zákona). Například získat požadované údaje na základě méně rušivé pravomoci, například cíleným získáváním komunikačních údajů" ([402]).

(235) Při provádění tohoto posouzení se ministr bude opírat o informace, které jsou povinni vedoucí představitelé zpravodajských služeb ([403]) ve svém návrhu uvádět, například důvody, proč je opatření považováno za nezbytné z jednoho ze zákonných důvodů, a důvody, proč nebylo možné cíle, kterého má být příkazem dosaženo, rozumně dosáhnout jinými, méně rušivými prostředky ([404]). Kromě toho operativní účely omezují rozsah, pro který lze údaje získané na základě příkazu vybrat k šetření ([405]). Jak je uvedeno v příslušném kodexu zásad, operativní účely musí popisovat jasný požadavek a musí obsahovat podrobnosti dostatečné k tomu, aby byl ministr přesvědčen, že získané údaje lze vybrat k šetření pouze ze specifických důvodů ([406]). Ministr se bude muset před schválením příkazu ujistit, že existuje zvláštní vhodný režim, který zaručí, že bude k šetření vybrán pouze materiál, který je pro operativní a zákonem stanovené účely považován pro šetření za nezbytný a který by měl být za všech okolností přiměřený a nezbytný. Tento specifický požadavek, který se odráží v článcích 158 a 172 ([407]) zákona o vyšetřovacích pravomocích z roku 2016, pokud jde o předchozí posouzení nezbytnosti a přiměřenosti kritérií použitých pro účely výběru, představuje další důležitou novinku režimu zavedeného zákonem o vyšetřovacích pravomocích z roku 2016 ve srovnání s režimem, který existoval dříve.

(236) Zákon o vyšetřovacích pravomocích z roku 2016 rovněž zavedl povinnost ministra zajistit, aby před vydáním příkazu k hromadnému získávání komunikačních údajů byla zavedena zvláštní omezení týkající se zabezpečení, uchovávání a zpřístupňování shromážděných osobních údajů ([408]). V případě zahraničních zpřístupnění se pro hromadné odposlechy a hromadný vzdálený síťový přístup k zařízení v této souvislosti použijí také záruky popsané ve 227. bodě odůvodnění ([409]). Další omezení jsou stanovena v právních předpisech týkajících se doby platnosti ([410]), prodloužení ([411]) a úpravy hromadných příkazů ([412]).

(237) Důležité je, že stejně jako u ostatních hromadných pravomocí musí ministr před vydáním příkazu získat souhlas soudního komisaře ([413]). Jedná se o klíčový prvek režimu zavedeného zákonem o vyšetřovacích pravomocích z roku 2016.

([400]) Podle čl. 94 odst. 1 zákona o telekomunikacích z roku 1984 mohl ministr vydávat „příkazy obecné povahy, které ministr považuje za potřebné nebo účelné v zájmu národní bezpečnosti (…)" (viz poznámka pod čarou 451).

([401]) Viz rozsudek ve věci Privacy International, bod 78.

([402]) Viz kodex zásad pro hromadné získávání komunikačních údajů, bod 4.11 (viz poznámka pod čarou 399414).

([403]) O příkaz k hromadnému získání údajů mohou žádat pouze vedoucí představitelé zpravodajských služeb, kterými jsou: i) generální ředitel Bezpečnostní služby; ii) náčelník Tajné zpravodajské služby nebo iii) ředitel GCHQ (viz články 158 a 263 zákona o vyšetřovacích pravomocích z roku 2016).

([404]) Kodex zásad pro hromadné získávání komunikačních údajů, bod 4.5 (viz poznámka pod čarou 399).

([405]) Podle článku 161 zákona o vyšetřovacích pravomocích z roku 2016 musí být operativními účely uvedenými v příkazu účely, které jsou upřesněny v seznamu vedeném vedoucími představiteli zpravodajských služeb („seznam operativních účelů") jakožto účely, které považují za operativní účely, pro které mohou být zachycený obsah nebo sekundární údaje získané na základě příkazů k hromadnému odposlechu vybrány k šetření.

([406]) Kodex zásad pro hromadné získávání komunikačních údajů, bod 6.6 (viz poznámka pod čarou 399).

([407]) Článek 172 zákona o vyšetřovacích pravomocích z roku 2016 vyžaduje, aby byly zavedeny zvláštní záruky pro fázi filtrování a výběru hromadně získaných komunikačních údajů pro šetření. Úmyslné šetření porušující tyto záruky je také trestným činem (viz článek 173 zákona o vyšetřovacích pravomocích z roku 2016).

([408]) Článek 171 zákona o vyšetřovacích pravomocích z roku 2016.

([409]) Ustanovení čl. 171 odst. 9 zákona o vyšetřovacích pravomocích z roku 2016.

([410]) Článek 162 zákona o vyšetřovacích pravomocích z roku 2016.

([411]) Článek 163 zákona o vyšetřovacích pravomocích z roku 2016.

([412]) Ustanovení článků 164–166 zákona o vyšetřovacích pravomocích z roku 2016.

([413]) Článek 159 zákona o vyšetřovacích pravomocích z roku 2016.

(238) Komisař pro kontrolu vyšetřovacích pravomocí provádí následný dohled nad postupem šetření hromadně získaného materiálu (komunikačních údajů) (viz 254. bod odůvodnění níže). V tomto ohledu zákon o vyšetřovacích pravomocích z roku 2016 zavedl požadavek, aby zpravodajský analytik provádějící šetření před výběrem údajů k šetření zaznamenal důvod, proč je navrhované šetření nezbytné a přiměřené pro konkrétní operativní účel ([414]). Ve výroční zprávě Úřadu komisaře pro kontrolu vyšetřovacích pravomocí za rok 2019 bylo s ohledem na praxi GCHQ a MI5 zjištěno, že „kritická úloha hromadných komunikačních údajů ve vztahu k celé řadě činností prováděných GCHQ byla v kontrolovaných případech formulována řádně. Posuzovali jsme povahu požadovaných údajů a stanovené zpravodajské požadavky a dokumentace k naší spokojenosti prokázala, že přístup útvaru byl nezbytný a přiměřený.“ ([415]). „Odůvodnění zaznamenaná službou MI5 byla na dobré úrovni a splňovala zásady nezbytnosti a přiměřenosti“ ([416]).

3.3.1.1.4.3 Uchovávání a šetření hromadných souborů osobních údajů

(239) Příkazy týkající se hromadných souborů osobních údajů ([417]) povolují zpravodajským službám uchovávat a šetřit soubory údajů, které obsahují osobní údaje týkající se více jednotlivců. Podle vysvětlení, které poskytly orgány Spojeného království, může být analýza těchto datových souborů „jediným způsobem, jak může agentura UKIC pokročit ve vyšetřování a identifikovat teroristy na základě velmi omezených zpravodajských poznatků nebo v případě, že jejich komunikace byla záměrně utajena“ ([418]). Existují dva typy příkazů: „skupinové příkazy pro hromadné soubory osobních údajů“ ([419]), které se týkají určité kategorie souborů údajů, tj. souborů údajů, které jsou si svým obsahem a navrhovaným použitím podobné a vzbuzují podobné úvahy například ohledně míry rušivosti a citlivosti a ohledně přiměřenosti použití údajů, a tudíž ministrovi umožňují posoudit nezbytnost a přiměřenost získání všech údajů v příslušné skupině najednou. Skupinový příkaz pro hromadný soubor osobních údajů může zahrnovat například soubory cestovních údajů, které se vztahují k podobným trasám ([420]). „Specifické příkazy pro hromadné soubory osobních údajů“ ([421]) se naopak týkají jednoho konkrétního souboru údajů, například souboru údajů nového nebo neobvyklého druhu, které nespadají do stávajícího skupinového příkazu pro soubor osobních údajů, nebo souboru údajů, který se týká zvláštních druhů osobních údajů ([422]), a proto vyžaduje dodatečné záruky ([423]). Ustanovení zákona o vyšetřovacích pravomocích z roku 2016 týkající se hromadných souborů osobních údajů umožňují šetření a uchovávání těchto souborů údajů, pouze pokud je nezbytné a přiměřené ([424]) a v souladu s obecnými povinnostmi týkajícími se ochrany soukromí ([425]).

(240) Pravomoc vydat příkaz pro hromadný soubor osobních údajů podléhá postupu „dvojitého zámku“: posouzení nezbytnosti a přiměřenosti opatření provádí nejprve ministr a poté soudní komisař ([426]). Ministr je povinen posoudit povahu a rozsah požadovaného druhu příkazu, kategorii dotčených údajů a počet jednotlivých hromadných souborů osobních údajů, které pravděpodobně konkrétní druh příkazu zahrnuje ([427]). Jak uvádí kodex zásad týkajících se šetření a uchovávání hromadných souborů osobních údajů ve zpravodajských službách, musí být vedeny podrobné záznamy, které podléhají auditu ze strany komisaře pro kontrolu vyšetřovacích pravomocí ([428]). Uchovávání a šetření hromadných souborů osobních údajů mimo meze stanovené zákonem o vyšetřovacích pravomocích z roku 2016 je trestným činem ([429]).

([414]) Výroční zpráva Úřadu komisaře pro kontrolu vyšetřovacích pravomocí za rok 2019, bod 8.6, viz poznámka pod čarou 463.
([415]) Výroční zpráva Úřadu komisaře pro kontrolu vyšetřovacích pravomocí za rok 2019, bod 10.4, viz poznámka pod čarou 463.
([416]) Výroční zpráva Úřadu komisaře pro kontrolu vyšetřovacích pravomocí za rok 2019, bod 8.37, viz poznámka pod čarou 463.
([417]) Článek 200 zákona o vyšetřovacích pravomocích z roku 2016.
([418]) Britský vysvětlující rámec pro diskuse o odpovídající ochraně, oddíl H: Národní bezpečnost, s. 34, viz poznámka pod čarou 29.
([419]) Článek 204 zákona o vyšetřovacích pravomocích z roku 2016.
([420]) Kodex zásad týkajících se šetření a uchovávání hromadných souborů osobních údajů ve zpravodajských službách, bod 4.7, k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf
([421]) Článek 205 zákona o vyšetřovacích pravomocích z roku 2016.
([422]) Například citlivé osobní údaje, viz článek 202 zákona o vyšetřovacích pravomocích z roku 2016 a kodex zásad týkajících se šetření a uchovávání hromadných souborů osobních údajů ve zpravodajských službách, body 4.21 a 4.12, viz poznámka pod čarou 469.
([423]) Ministr musí návrh na vydání specifického příkazu pro hromadný soubor osobních údajů posoudit individuálně, tj. s ohledem na jeden konkrétní soubor údajů. Podle článku 205 zákona o vyšetřovacích pravomocích je zpravodajská služba povinna zahrnout do svého návrhu na vydání specifického příkazu pro hromadný soubor osobních údajů podrobné vysvětlení povahy a rozsahu dotyčného materiálu a seznam „operativních účelů“, pro které příslušná zpravodajská služba hodlá šetřit daný hromadný soubor osobních údajů (pokud zpravodajská služba žádá o příkaz k uchování a šetření, nikoli jen k uchování). Při vydání skupinového příkazu pro hromadný soubor osobních údajů naopak ministr posuzuje celou kategorii souborů údajů najednou.
([424]) Články 204 a 205 zákona o vyšetřovacích pravomocích z roku 2016.
([425]) Článek 2 zákona o vyšetřovacích pravomocích z roku 2016.
([426]) Články 204 a 205 zákona o vyšetřovacích pravomocích z roku 2016.
([427]) Kodex zásad týkajících se šetření a uchovávání hromadných souborů osobních údajů ve zpravodajských službách, bod 5.2, viz poznámka pod čarou 420.
([428]) Kodex zásad týkajících se šetření a uchovávání hromadných souborů osobních údajů ve zpravodajských službách, body 8.1–8.15, viz poznámka pod čarou 420.
([429]) Britský vysvětlující rámec pro diskuse o odpovídající ochraně, oddíl H: Národní bezpečnost, s. 34, viz poznámka pod čarou 29.

3.3.2 *Další použití shromážděných informací*

(241) Osobní údaje zpracovávané podle části 4 zákona o ochraně údajů z roku 2018 nesmí být zpracovávány způsobem, který je neslučitelný s účelem, pro který byly údaje shromážděny ([430]). Zákon o ochraně údajů z roku 2018 stanoví, že správce může zpracovávat údaje k jinému účelu, než je ten, pro který byly údaje shromážděny, pokud je slučitelný s původním účelem, pokud je správce ze zákona oprávněn zpracovávat údaje a pokud je zpracování nezbytné a přiměřené ([431]). Kromě toho zákon o Bezpečnostní službě z roku 1989 a zákon o zpravodajských službách z roku 1994 upřesňují, že vedoucí představitelé zpravodajských služeb jsou povinni zajistit, aby nebyly získávány ani zveřejňovány žádné informace, pokud to není nezbytné pro řádné plnění funkcí služby nebo pro ostatní omezené a konkrétní účely uvedené v příslušných ustanoveních ([432]).

(242) Článek 109 zákona o ochraně údajů z roku 2018 také stanoví zvláštní požadavky na mezinárodní předávání osobních údajů zpravodajskými službami třetím zemím nebo mezinárodním organizacím. Podle tohoto ustanovení není povoleno předávat osobní údaje do země nebo na území mimo Spojené království nebo mezinárodní organizaci, pokud není předání nezbytné a přiměřené pro účely zákonných funkcí správce nebo pro jiné účely stanovené v čl. 2 odst. 2 písm. a) zákona o Bezpečnostní službě z roku 1989 nebo v čl. 2 odst. 2 písm. a) a čl. 4 odst. 2 písm. a) zákona o zpravodajských službách z roku 1994 ([433]). Důležité je, že tyto požadavky se použijí i v případech, v nichž je uplatněna výjimka z důvodu národní bezpečnosti podle článku 110 zákona o ochraně údajů z roku 2018, neboť článek 110 zákona o ochraně údajů z roku 2018 neuvádí článek 109 zákona o ochraně údajů z roku 2018 jako jedno z ustanovení, které se nemusí použít, pokud je pro účely ochrany národní bezpečnosti nutná výjimka z určitých ustanovení.

(243) Kromě toho, jak zdůraznil Úřad komisaře pro informace ve svých pokynech ke zpracování osobních údajů zpravodajskými službami, kromě záruk stanovených v části 4 zákona o ochraně údajů z roku 2018 podléhá zpravodajská služba při sdílení údajů se zpravodajským subjektem třetí země také zárukám, jež stanoví jiná legislativní opatření vztahující se na danou službu, aby bylo zajištěno zákonné a zodpovědné získávání, sdílení a nakládání s osobními údaji ([434]). Například zákon o vyšetřovacích pravomocích z roku 2016 stanoví další záruky v souvislosti s předáváním materiálu shromážděného prostřednictvím cíleného odposlechu ([435]), cíleného vzdáleného síťového přístupu k zařízení ([436]), hromadného odposlechu ([437]), hromadného získávání komunikačních údajů ([438]) a hromadného vzdáleného síťového přístupu k zařízení ([439]) (tzv. zahraniční zpřístupnění) do třetí země. Orgán vydávající příkaz musí zejména zajistit, aby byl zaveden režim, který zaručí, že třetí země přijímající údaje omezí počet osob, které budou do materiálu nahlížet, a rozsah zpřístupnění a počet kopií jakéhokoli materiálu na minimum nezbytné pro povolené účely stanovené v zákoně o vyšetřovacích pravomocích z roku 2016 ([440]).

3.3.3 *Dohled*

(244) Dohled nad přístupem vládních institucí pro účely národní bezpečnosti vykonává řada různých subjektů. Komisař pro informace dohlíží na zpracování osobních údajů podle zákona o ochraně údajů z roku 2018 (další informace o nezávislosti, úloze při jmenování a pravomocích komisaře viz 85. až 98. bod odůvodnění), zatímco nezávislý a soudní dohled nad používáním vyšetřovacích pravomocí podle zákona o vyšetřovacích pravomocích z roku 2016 zajišťuje komisař pro kontrolu vyšetřovacích pravomocí. Komisař pro kontrolu vyšetřovacích pravomocí dohlíží na

([430]) Ustanovení čl. 87 odst. 1 zákona o ochraně údajů z roku 2018.

([431]) Ustanovení čl. 87 odst. 3 zákona o ochraně údajů z roku 2018. Ačkoli podle článku 110 zákona o ochraně údajů z roku 2018 mohou být správci z této zásady vyňati v rozsahu, v jakém je taková výjimka požadována k zajištění národní bezpečnosti, musí být tato výjimka posouzena individuálně a lze se jí dovolávat, pouze pokud by použití konkrétního ustanovení mělo negativní důsledky pro národní bezpečnost (viz (132). bod odůvodnění). Osvědčení o omezení z důvodu národní bezpečnosti pro britské zpravodajské služby (k dispozici na této adrese: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) nezahrnují čl. 87 odst. 3 zákona o ochraně údajů z roku 2018. Kromě toho jakékoli zpracování za jiným účelem musí být povoleno zákonem a zpravodajské služby tedy musí mít pro další zpracování jasný právní základ.

([432]) Další informace o těchto účelech viz poznámka pod čarou 312.

([433]) Viz poznámka pod čarou 312.

([434]) Pokyny Úřadu komisaře pro informace ke zpracování osobních údajů zpravodajskými službami (viz poznámka pod čarou 161).

([435]) Článek 54 zákona o vyšetřovacích pravomocích z roku 2016.

([436]) Článek 130 zákona o vyšetřovacích pravomocích z roku 2016.

([437]) Článek 151 zákona o vyšetřovacích pravomocích z roku 2016.

([438]) Ustanovení čl. 171 odst. 9 zákona o vyšetřovacích pravomocích z roku 2016.

([439]) Článek 192 zákona o vyšetřovacích pravomocích z roku 2016.

([440]) Režim musí zahrnovat opatření, která zajistí, že každá pořízená kopie kteréhokoli materiálu bude po dobu, po kterou bude uchovávána, bezpečně uložena. Materiál získaný na základě příkazu a každá kopie tohoto materiálu musí být zničeny, jakmile pominou veškeré podstatné důvody pro jejich uchovávání (viz čl. 150 odst. 2, čl. 150 odst. 5, čl. 151 odst. 2 a čl. 151 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016). Stojí za zmínku, že podobné záruky poskytované předchozím právním rámcem (zákonem o úpravě vyšetřovacích pravomocí z roku 2000) byly shledány v souladu s požadavky, které stanovil Evropský soud pro lidská práva, pokud jde o sdílení materiálu získaného hromadným odposlechem s cizími státy nebo mezinárodními organizacemi (Evropský soud pro lidská práva (velký senát), věc Big Brother Watch and others v United Kingdom (viz poznámka pod čarou 279 výše), body 362 a 399).

použití vyšetřovacích pravomocí podle zákona o vyšetřovacích pravomocích z roku 2016 ze strany donucovacích i vnitrostátních bezpečnostních orgánů. Politický dohled zaručuje Výbor parlamentu Spojeného království pro zpravodajské služby.

3.3.3.1 Dohled podle části 4 zákona o ochraně údajů

(245) Na zpracování osobních údajů prováděné zpravodajskými službami podle části 4 zákona o ochraně údajů z roku 2018 dohlíží komisař pro informace ([441]).

(246) Obecné funkce komisaře pro informace v souvislosti se zpracováním osobních údajů zpravodajskými službami podle části 4 zákona o ochraně údajů z roku 2018 jsou stanoveny v příloze 13 zákona o ochraně údajů z roku 2018. K těmto úkolům mimo jiné patří monitorování a prosazování části 4 zákona o ochraně údajů z roku 2018, zvyšování povědomí veřejnosti, poskytování doporučení parlamentu Spojeného království, vládě a dalším institucím ohledně legislativních a správních opatření, zvyšování povědomí správců a zpracovatelů o jejich povinnostech, poskytování informací subjektu údajů ohledně výkonu práv subjektu údajů, vedení vyšetřování atd.

(247) Komisař má podle části 3 zákona o ochraně údajů z roku 2018 pravomoc upozorňovat správce na údajné porušení předpisů a vydávat napomenutí, že zpracování pravděpodobně porušuje pravidla, a uděluje výtky, pokud je porušení předpisů potvrzeno. Může také vydávat oznámení o vymáhání a sankci za porušení určitých ustanovení zákona ([442]). Na rozdíl od postupu podle jiných částí zákona o ochraně údajů z roku 2018 však komisař nemůže vydat oznámení o posouzení vůči vnitrostátnímu bezpečnostnímu orgánu ([443]).

(248) Kromě toho článek 110 zákona o ochraně údajů z roku 2018 stanoví výjimku z použití určitých pravomocí komisaře, pokud je to nutné pro účely zajištění národní bezpečnosti. To zahrnuje pravomoc komisaře vydávat (jakýkoli druh) oznámení podle zákona o ochraně údajů (výzvu k podání informací, oznámení o posouzení, vymáhání a o sankci), pravomoc provádět inspekce v souladu s mezinárodními závazky, pravomoci vstupu a inspekce a pravidla pro trestné činy ([444]). Jak je vysvětleno ve 126. bodě odůvodnění, tyto výjimky se použijí, pouze pokud je to v konkrétním jednotlivém případě nutné a přiměřené.

(249) Úřad komisaře pro informace a britské zpravodajské služby podepsaly memorandum o porozumění ([445]), které stanoví rámec spolupráce v řadě otázek, včetně oznámení o porušení zabezpečení údajů a vyřizování stížností subjektů údajů. Memorandum zejména stanoví, že po obdržení stížnosti Úřad komisaře pro informace posoudí, zda byla jakákoli výjimka z důvodu národní bezpečnosti použita řádně. Odpovědi na dotazy Úřadu komisaře pro informace v souvislosti s šetřením jednotlivých stížností musí dotčená zpravodajská služba poskytnout do 20 pracovních dnů, a to pomocí vhodných zabezpečených kanálů, pokud se jedná o utajované informace. Od dubna 2018 do dnešního dne obdržel Úřad komisaře pro informace 21 stížností od jednotlivců týkajících se zpravodajských služeb. Každá stížnost byla posouzena a výstup byl sdělen subjektu údajů ([446]).

([441]) Článek 116 zákona o ochraně údajů z roku 2018.

([442]) Podle článku 2 přílohy 13 zákona o ochraně údajů z roku 2018 mohou být vůči správci nebo zpracovateli vydána oznámení o vymáhání nebo sankcích v souvislosti s porušením kapitoly 2 části 4 zákona o ochraně údajů z roku 2018 (zásady zpracování), ustanovení části 4 zákona o ochraně údajů z roku 2018, která přiznávají práva subjektu údajů, požadavku na oznámení případu porušení zabezpečení osobních údajů komisaři podle článku 108 zákona o ochraně údajů z roku 2018 a zásad pro předávání osobních údajů do třetích zemí, zemí, které nejsou členy úmluvy, a mezinárodním organizacím podle článku 109 zákona o ochraně údajů z roku 2018 (další podrobnosti o oznámení o vymáhání nebo sankci viz (92). bod odůvodnění).

([443]) Podle čl. 147 odst. 6 zákona o ochraně údajů z roku 2018 nemůže komisař pro informace vydat oznámení o posouzení subjektu uvedenému v čl. 23 odst. 3 zákona o svobodě informací z roku 2000. To zahrnuje Bezpečnostní službu (MI5), Tajnou zpravodajskou službu (MI6) a Vládní ředitelství pro komunikaci (GCHQ)).

([444]) Ustanovení, která mohou být předmětem výjimky: článek 108 (oznámení o porušení zabezpečení osobních údajů komisaři), článek 119 (inspekce v souladu s mezinárodními závazky); články 142 až 154 a příloha 15 (oznámení komisaře a pravomoci vstupu a inspekce) a články 170 až 173 (trestné činy týkající se osobních údajů). Rovněž ustanovení týkající se zpracování zpravodajskými službami podle čl. 1 písm. a) a g) a článku 2 přílohy 13 (další obecné funkce komisaře).

([445]) Memorandum o porozumění mezi Úřadem komisaře pro informace a zpravodajskými službami Spojeného království, viz poznámka pod čarou 165.

([446]) V sedmi z těchto případů Úřad komisaře pro informace doporučil stěžovateli podat stížnost u správce údajů (jedná se o případ, kdy jednotlivec podal stížnost Úřadu komisaře pro informace, ale měl ji nejprve podat u správce údajů), v jednom z těchto případů poskytl Úřad komisaře pro informace správci údajů obecné doporučení (používá se, pokud jednání správce zřejmě neporušilo právní předpisy, ale zlepšením postupů se mohlo předejít stížnosti podané u Úřadu komisaře pro informace) a v ostatních třinácti případech nebylo od správce údajů požadováno žádné opatření (používá se, když stížnosti podané jednotlivci spadají pod zákon o ochraně údajů z roku 2018, protože se týkají zpracování osobních údajů, ale podle poskytnutých informací správce zřejmě zákon neporušil).

3.3.3.2 Dohled nad využíváním vyšetřovacích pravomocí podle zákona o vyšetřovacích pravomocích z roku 2016

(250) Podle části 8 zákona o vyšetřovacích pravomocích z roku 2016 vykonává dohled nad využíváním vyšetřovacích pravomocí komisař pro kontrolu vyšetřovacích pravomocí. Komisaři pro kontrolu vyšetřovacích pravomocí jsou nápomocni další soudní komisaři, kteří se souhrnně označují jako soudní komisaři ([447]). Zákon o vyšetřovacích pravomocích z roku 2016 stanoví záruky, které chrání nezávislost soudních komisařů. Od soudních komisařů se vyžaduje, aby v současnosti nebo minulosti zastávali vysokou soudní funkci (tj. musí v současnosti nebo v minulosti být členy soudů nejvyššího stupně) ([448]), a jako každý člen soudnictví mají na vládě nezávislé postavení ([449]). Podle článku 227 zákona o vyšetřovacích pravomocích z roku 2016 jmenuje komisaře pro kontrolu vyšetřovacích pravomocí předseda vlády, který jmenuje tolik soudních komisařů, kolik považuje za nezbytné. Všichni komisaři, ať už jsou současnými nebo bývalými členy soudnictví, mohou být jmenováni pouze na základě společného doporučení tří nejvyšších soudců pro Anglii a Wales, Skotsko a Severní Irsko a lorda kancléře ([450]). Ministr musí komisaři pro kontrolu vyšetřovacích pravomocí zajistit personál, prostory, vybavení a další zařízení a služby ([451]). Funkční období komisařů je tříleté a komisaře lze jmenovat opakovaně ([452]). První zárukou jejich nezávislosti je skutečnost, že soudní komisaře lze z funkce odvolat pouze za přísných podmínek s vysokou prahovou hranicí: odvolat je může buď předseda vlády za specifických okolností taxativně vyjmenovaných v čl. 228 odst. 5 zákona o vyšetřovacích pravomocích z roku 2016 (např. úpadek nebo trest odnětí svobody), nebo mohou být odvoláni, pokud obě komory Parlamentu Spojeného království přijaly usnesení schvalující toto odvolání ([453]).

(251) Komisaři pro kontrolu vyšetřovacích pravomocí a soudním komisařům je při výkonu jejich funkcí nápomocen Úřad komisaře pro kontrolu vyšetřovacích pravomocí. Zaměstnanci Úřadu komisaře pro kontrolu vyšetřovacích pravomocí zahrnují tým inspektorů, interní právní a technické odborníky a technologickou poradní komisi, která poskytuje odborné poradenství. Stejně jako nezávislost jednotlivých soudních komisařů je chráněna i nezávislost Úřadu komisaře pro kontrolu vyšetřovacích pravomocí. Úřad komisaře pro kontrolu vyšetřovacích pravomocí je „nezávislým subjektem" Ministerstva vnitra, tj. získává finanční prostředky od Ministerstva vnitra, ale své funkce vykonává nezávisle ([454]).

(252) Hlavní funkce soudních komisařů jsou stanoveny v článku 229 zákona o vyšetřovacích pravomocích z roku 2016 ([455]). Soudní komisaři mají zejména rozsáhlou pravomoc předchozího souhlasu, která je součástí záruk zavedených v právním rámci Spojeného království zákonem o vyšetřovacích pravomocích z roku 2016. Příkazy týkající se cíleného odposlechu, vzdáleného síťového přístupu k zařízení, hromadných souborů osobních údajů, hromadného získávání komunikačních údajů i výzvy k uchovávání komunikačních údajů musí být schváleny soudními komisaři ([456]). Komisař pro kontrolu vyšetřovacích pravomocí musí také vždy předem schválit získání komunikačních údajů pro účely vymáhání práva ([457]). Pokud komisař odmítne příkaz schválit, může ministr podat opravný prostředek ke komisaři pro kontrolu vyšetřovacích pravomocí, jehož rozhodnutí je konečné.

([447]) V souladu s čl. 227 odst. 7 a 8 zákona o vyšetřovacích pravomocích z roku 2016 je komisař pro kontrolu vyšetřovacích pravomocí soudním komisařem a komisař pro kontrolu vyšetřovacích pravomocí a ostatní soudní komisaři se společně označují jako soudní komisaři. V současné době působí patnáct soudních komisařů.

([448]) Podle čl. 60 odst. 2 části 3 zákona o ústavní reformě z roku 2005, se „vysokou soudní funkcí" rozumí funkce soudce kteréhokoli z těchto soudů: i) Nejvyšší soud; ii) Odvolací soud v Anglii a Walesu; iii) Vrchní soud v Anglii a Walesu; iv) Court of Session; v) Odvolací soud v Severním Irsku; vi) Vrchní soud v Severním Irsku nebo člen Nejvyššího odvolacího soudu.

([449]) Nezávislost soudnictví vychází ze zvyklostí a je obecně uznávána od zákona o nástupnictví z roku 1701.

([450]) Ustanovení čl. 227 odst. 3 zákona o vyšetřovacích pravomocích z roku 2016. Soudní komisaře musí doporučit i komisař pro kontrolu vyšetřovacích pravomocí, čl. 227 odst. 4 písm. e) zákona o vyšetřovacích pravomocích z roku 2016.

([451]) Článek 238 zákona o vyšetřovacích pravomocích z roku 2016.

([452]) Ustanovení čl. 227 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016.

([453]) Postup odvolání je totožný s postupem odvolání jiných soudců ve Spojeném království (viz např. čl. 11 odst. 3 zákona o soudech vyšší instance z roku 1981 a článek 33 zákona o ústavní reformě z roku 2005, které také vyžadují usnesení v návaznosti na souhlas obou komor Parlamentu Spojeného království). Dosud nebyl ze své funkce odvolán žádný soudní komisař.

([454]) Nezávislý subjekt je organizace nebo agentura, která získává finanční prostředky od vládních institucí, může však jednat nezávisle (definice a další informace o nezávislém subjektu viz Příručka Úřadu vlády o klasifikaci subjektů veřejného sektoru, k dispozici na této adrese: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf a první zpráva zvláštního výboru Dolní sněmovny Spojeného království pro veřejnou správu za období 2014–2015, k dispozici na této adrese: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf).

([455]) Podle článku 229 zákona o vyšetřovacích pravomocích z roku 2016 má soudní komisař rozsáhlé pravomoci, které zahrnují i dohled nad uchováváním a zpřístupňováním údajů shromážděných zpravodajskými službami.

([456]) Rozhodnutí o schválení rozhodnutí ministra vydat příkaz jsou věci soudních komisařů samotných. Pokud komisař odmítne příkaz schválit, může ministr podat opravný prostředek ke komisaři pro kontrolu vyšetřovacích pravomocí, jehož rozhodnutí je konečné.

([457]) Schválení komisařem pro kontrolu vyšetřovacích pravomocí je vyžadováno vždy, když jsou komunikační údaje získávány pro účely vymáhání práva (článek 60A zákona o vyšetřovacích pravomocích z roku 2016). Jsou-li komunikační údaje získávány pro účely národní bezpečnosti, může schválení udělit komisař pro kontrolu vyšetřovacích pravomocí nebo alternativně určený vyšší úředník příslušného orgánu veřejné moci (viz články 61 a 61A zákona o vyšetřovacích pravomocích z roku 2016 a (203). bod odůvodnění).

(253) Zvláštní zpravodaj OSN pro právo na soukromí důrazně uvítal zřízení funkce soudních komisařů v rámci zákona o vyšetřovacích pravomocích z roku 2016, neboť „všechny citlivější nebo rušivější žádosti o sledování musí schválit jak ministr vlády, tak Úřad komisaře pro kontrolu vyšetřovacích pravomocí". Zvláště zdůraznil, že „tento prvek soudního přezkumu [prostřednictvím úlohy komisaře pro kontrolu vyšetřovacích pravomocí], kterému je nápomocen tým zkušených inspektorů a technických odborníků s lepšími zdroji, je jednou z nejvýznamnějších nových záruk zavedených zákonem o vyšetřovacích pravomocích", který nahradil dříve roztříštěný systém orgánů dohledu a doplňuje úlohu výboru Parlamentu Spojeného království pro zpravodajství a bezpečnost Parlamentu a tribunálu pro kontrolu vyšetřovacích pravomocí" ([458]).

(254) Komisař pro kontrolu vyšetřovacích pravomocí je navíc oprávněn provádět následný dohled (mimo jiné prostřednictvím auditu, inspekce a vyšetřování) nad využíváním vyšetřovacích pravomocí podle zákona o vyšetřovacích pravomocích z roku 2016 ([459]) a nad některými dalšími pravomocemi a funkcemi stanovenými v příslušných právních předpisech ([460]). Výsledky tohoto následného dohledu jsou zahrnuty ve zprávě, kterou musí komisař pro kontrolu vyšetřovacích pravomocí každoročně vypracovat a předložit předsedovi vlády ([461]) a která musí být zveřejněna a předložena Parlamentu Spojeného království ([462]). Zpráva obsahuje příslušné statistiky a informace o využívání vyšetřovacích pravomocí zpravodajskými službami a donucovacími orgány, jakož i o využití záruk ve vztahu k otázkám, na které se vztahuje povinnost mlčenlivosti, důvěrným novinářským materiálům a zdrojům novinářských informací a informace o přijatých režimech a operativních účelech použitých v souvislosti s hromadnými příkazy. A konečně je ve výroční zprávě Úřadu komisaře pro kontrolu vyšetřovacích pravomocí také upřesněno, ve které oblasti byla vydána doporučení orgánům veřejné moci a jaká byla reakce na tato doporučení ([463]).

(255) Pokud se komisař pro kontrolu vyšetřovacích pravomocí dozví o jakékoli významné chybě, které se dopustily orgány veřejné moci při použití svých vyšetřovacích pravomocí, musí v souladu s článkem 231 zákona o vyšetřovacích pravomocích z roku 2016 informovat dotyčnou osobu, jestliže má za to, že je chyba závažná a je ve veřejném zájmu, aby tato osoba byla informována ([464]). Článek 231 zákona o vyšetřovacích pravomocích z roku 2016 zejména stanoví, že při informování osoby o chybě musí komisař pro kontrolu vyšetřovacích pravomocí poskytnout informace o jakémkoli právu dané osoby, které lze uplatnit u tribunálu pro kontrolu vyšetřovacích pravomocí, a uvést podrobnosti, které komisař považuje za nezbytné pro výkon těchto práv a jejichž zpřístupnění je ve veřejném zájmu ([465]).

([458]) Prohlášení po skončení mise zvláštního zpravodaje pro právo na soukromí týkající se ukončení jeho mise do Spojeného království Velké Británie a Severního Irska (viz poznámka pod čarou 281).

([459]) Článek 229 zákona o vyšetřovacích pravomocích z roku 2016. Pravomoci soudního komisaře v oblasti vyšetřování a informací jsou stanoveny v článku 235 zákona o vyšetřovacích pravomocích z roku 2016.

([460]) Zahrnuje opatření v oblasti sledování podle zákona o úpravě vyšetřovacích pravomocí z roku 2000, výkon funkcí podle části 3 zákona o policii z roku 1997 (oprávnění přijmout opatření ve vztahu k majetku) a výkon funkcí ministra podle článků 5 až 7 zákona o zpravodajských službách z roku 1994 (příkazy k zásahu do radiotelegrafické komunikace, vstupu do nemovitosti a zásahu do vlastnických práv (článek 229 zákona o vyšetřovacích pravomocích z roku 2016).

([461]) Článek 230 zákona o vyšetřovacích pravomocích z roku 2016. Komisař pro kontrolu vyšetřovacích pravomocí může také předsedovi vlády z vlastního podnětu podávat zprávy o jakékoli záležitosti týkající se jeho funkcí. Komisař pro kontrolu vyšetřovacích pravomocí musí také podat zprávu předsedovi vlády na jeho žádost a předseda vlády může komisaři pro kontrolu vyšetřovacích pravomocí nařídit, aby přezkoumal jakékoli funkce zpravodajských služeb.

([462]) Některé části mohou být vyloučeny, pokud by jejich zveřejnění bylo v rozporu s národní bezpečností.

([463]) Například ve výroční zprávě Úřadu komisaře pro kontrolu vyšetřovacích pravomocí za rok 2019 (bod 6.38) se uvádí, že službě MI5 bylo doporučeno upravit politiku uchovávání hromadných souborů osobních údajů, neboť měla uplatnit přístup zohledňující přiměřenost uchovávání pro všechny oblasti držených hromadných souborů osobních údajů a pro každý držený hromadný soubor osobních údajů. Na konci roku 2018 nebyl Úřad komisaře pro kontrolu vyšetřovacích pravomocí přesvědčen, že toto doporučení bylo dodrženo, a zpráva z roku 2019 vysvětlila, že služba MI5 nyní zavádí nový postup pro splnění tohoto požadavku. Výroční zpráva za rok 2019 (bod 8.22) rovněž zmiňuje, že GHCQ obdrželo řadu doporučení týkajících se vedení evidence ohledně přiměřenosti šetření hromadných údajů prováděných útvarem. Zpráva potvrzuje, že ke konci roku 2018 došlo v této oblasti ke zlepšení. Výroční zpráva Úřadu komisaře pro kontrolu vyšetřovacích pravomocí za rok 2019, k dispozici na této adrese: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Kromě toho je každá inspekce Úřadu komisaře pro kontrolu vyšetřovacích pravomocí provedená u orgánu veřejné moci zakončena zprávou, která je orgánu předána a obsahuje veškerá doporučení, která z této inspekce vyplývají. Úřad komisaře pro kontrolu vyšetřovacích pravomocí. poté každou následující inspekci zahájí přezkoumáním případných předchozích doporučení z poslední návštěvy a v nové inspekční zprávě bude zohledněno, zda byla předchozí doporučení řešena nebo se přenášejí dále.

([464]) Chyba je považována za „závažnou", pokud má komisař za to, že dotčené osobě způsobila významnou újmu nebo škodu (čl. 231 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016). V roce 2018 bylo oznámeno 22 chyb, z nichž osm bylo považováno za závažné a vedlo k informování dotčené osoby. Viz Výroční zpráva Úřadu komisaře pro kontrolu vyšetřovacích pravomocí za rok 2018, příloha C (viz https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). V roce 2019 bylo za závažné považováno čtrnáct chyb. Viz Výroční zpráva Úřadu komisaře pro kontrolu vyšetřovacích pravomocí za rok 2019, příloha C, viz poznámka pod čarou 463.

([465]) Článek 231 zákona o vyšetřovacích pravomocích z roku 2016 uvádí, že při informování osoby o chybě musí komisař pro kontrolu vyšetřovacích pravomocí uvést takové podrobnosti, jaké považuje za nezbytné pro výkon těchto práv, a to zejména s ohledem na míru, v níž by zpřístupnění těchto podrobností bylo v rozporu s veřejným zájmem nebo by bylo na újmu prevence nebo odhalování závažné trestné činnosti, hospodářského blahobytu Spojeného království nebo pokračujícího výkonu jakýchkoli funkcí kterékoli ze zpravodajských služeb.

3.3.3.3 Parlamentní dohled nad zpravodajskými službami

(256) Parlamentní dohled, který vykonává výbor pro bezpečnost a zpravodajskou činnost, odvozuje svůj zákonný základ ze zákona o spravedlnosti a bezpečnosti z roku 2013 ([466]). Zákon zřizuje výbor pro bezpečnost a zpravodajskou činnost jako výbor Parlamentu Spojeného království. Od roku 2013 má výbor pro bezpečnost a zpravodajskou činnost větší pravomoci, včetně dohledu nad operativními činnostmi bezpečnostních služeb. Podle článku 2 zákona o spravedlnosti a bezpečnosti z roku 2013 je úkolem výboru pro bezpečnost a zpravodajskou činnost dohlížet na výdaje, správu, politiku a operace národních bezpečnostních služeb. Zákon o spravedlnosti a bezpečnosti z roku 2013 stanoví, že výbor pro bezpečnost a zpravodajskou činnost může vést vyšetřování operativních záležitostí, pokud se netýkají probíhajících operací ([467]). Memorandum o porozumění dohodnuté mezi předsedou vlády a výborem pro bezpečnost a zpravodajskou činnost ([468]) podrobně stanoví prvky, které je třeba vzít v úvahu při posuzování toho, zda daná činnost není součástí probíhající operace ([469]). Výbor pro bezpečnost a zpravodajskou činnost může být o prošetření probíhajících operací také požádán předsedou vlády a může přezkoumávat informace, které služby poskytnou dobrovolně.

(257) Podle přílohy 1 zákona o spravedlnosti a bezpečnosti z roku 2013 může výbor pro bezpečnost a zpravodajskou činnost požádat ředitele kterékoli ze tří zpravodajských služeb o sdělení jakýchkoli informací. Služba musí tyto informace zpřístupnit, pokud ministr neuplatní právo veta ([470]). Podle vysvětlení poskytnutých orgány Spojeného království je výboru pro bezpečnost a zpravodajskou činnost v praxi odepřeno jen velmi málo informací ([471]).

(258) Výbor pro bezpečnost a zpravodajskou činnost se skládá z členů náležejících do kterékoli komory Parlamentu Spojeného království, které jmenuje předseda vlády po konzultaci s vedoucím představitelem opozice ([472]). Výbor pro bezpečnost a zpravodajskou činnost je povinen předkládat parlamentu Spojeného království výroční zprávu o výkonu svých funkcí a další zprávy, které považuje za vhodné ([473]). Kromě toho je výbor pro bezpečnost a zpravodajskou činnost oprávněn obdržet každé tři měsíce seznam operativních účelů, které se používají pro šetření hromadně získaného materiálu ([474]). Předseda vlády sdílí s výborem pro bezpečnost a zpravodajskou činnost kopie vyšetřování, inspekcí nebo auditů komisaře pro kontrolu vyšetřovacích pravomocí, pokud je předmět zpráv významný z hlediska zákonných kompetencí výboru ([475]). Výbor může také požádat komisaře pro kontrolu vyšetřovacích pravomocí o provedení vyšetřování a komisař musí výbor pro bezpečnost a zpravodajskou činnost informovat o rozhodnutí, zda takové vyšetřování provede ([476]).

(259) Výbor pro bezpečnost a zpravodajskou činnost rovněž přispěl k návrhu zákona o vyšetřovacích pravomocích z roku 2016, což vyústilo v řadu pozměňovacích návrhů, které nyní zákon o vyšetřovacích pravomocích z roku 2016 zohledňuje ([477]). Výbor pro bezpečnost a zpravodajskou činnost doporučil zejména posílit ochranu soukromí

([466]) Jak vysvětlily orgány Spojeného království, zákon o spravedlnosti a bezpečnosti rozšířil oblast působnosti výboru pro bezpečnost a zpravodajskou činnost o úlohu dohledu nad zpravodajskou komunitou nad rámec tří služeb a povolil zpětný dohled nad operativními činnostmi služeb v záležitostech významného vnitrostátního zájmu.

([467]) Článek 2 zákona o spravedlnosti a bezpečnosti z roku 2013.

([468]) Memorandum o porozumění mezi předsedou vlády a výborem pro bezpečnost a zpravodajskou činnost, k dispozici na této adrese: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf

([469]) Memorandum o porozumění mezi předsedou vlády a výborem pro bezpečnost a zpravodajskou činnost, bod 14, viz poznámka pod čarou 468.

([470]) Ministr může zpřístupnění informací vetovat pouze ze dvou důvodů: informace jsou citlivé a neměly by být výboru pro bezpečnost a zpravodajskou činnost sděleny v zájmu národní bezpečnosti nebo jde o informace takové povahy, že pokud by byl ministr požádán, aby je předložil zvláštnímu výboru Dolní sněmovny, považoval by (z důvodů, které se neomezují na národní bezpečnost), za vhodné tak neučinit (čl. 4 odst. 2 přílohy 1 zákona o spravedlnosti a bezpečnosti z roku 2013).

([471]) Britský vysvětlující rámec pro diskuse o odpovídající ochraně, oddíl H: Národní bezpečnost, s. 43, viz poznámka pod čarou 31.

([472]) Článek 1 zákona o spravedlnosti a bezpečnosti z roku 2013. Ministři se nemohou stát členy výboru. Členové zastávají svou funkci ve výboru pro bezpečnost a zpravodajskou činnost po dobu parlamentního funkčního období, během kterého byli jmenováni. Mohou být odvoláni usnesením sněmovny, která je jmenovala, nebo jsou odvoláni, pokud přestanou být poslanci nebo se stanou ministrem. Člen výboru může také odstoupit.

([473]) Zprávy a prohlášení výboru jsou k dispozici on-line na této adrese: https://isc.independent.gov.uk/publications/. V roce 2015 zveřejnil výbor pro bezpečnost a zpravodajskou činnost zprávu „Privacy and Security: A modern and transparent legal framework" (Ochrana soukromí a bezpečnost: Moderní a transparentní právní rámec") (viz: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), v níž posoudil právní rámec pro techniky sledování používané zpravodajskými službami a vydal řadu doporučení, která byla následně zvážena a začleněna do návrhu zákona o vyšetřovacích pravomocích, který byl přijat jako právní předpis, zákon o vyšetřovacích pravomocích z roku 2016. Odpověď vládních institucí na zprávu o ochraně soukromí a bezpečnosti je k dispozici na této adrese: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf

([474]) Článek 142, 161 a 183 zákona o vyšetřovacích pravomocích z roku 2016.

([475]) Článek 234 zákona o vyšetřovacích pravomocích z roku 2016.

([476]) Článek 236 zákona o vyšetřovacích pravomocích z roku 2016.

([477]) Výbor pro bezpečnost a zpravodajskou činnost Parlamentu Spojeného království, zpráva o návrhu zákona o vyšetřovacích pravomocích, k dispozici na této adrese: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

zavedením souboru opatření k ochraně soukromí, která platí v celém rozsahu vyšetřovacích pravomocí ([478]). Rovněž předložil změny navrhovaných pravomocí týkajících vzdáleného síťového přístupu k zařízení, hromadných souborů osobních údajů a komunikačních údajů a vyžádal si další konkrétní změny s cílem posílit omezení a záruky pro použití vyšetřovacích pravomocí ([479]).

3.3.4 *Soudní ochrana*

(260) V oblasti přístupu vlády pro účely národní bezpečnosti musí mít subjekty údajů možnost podat žalobu k nezávislému a nestrannému soudu pro získání přístupu ke svým osobním údajům nebo pro dosažení opravy nebo výmazu takovýchto údajů ([480]). Tento soudní orgán musí mít zejména pravomoc přijímat závazná rozhodnutí týkající se zpravodajské služby ([481]). Ve Spojeném království, jak je vysvětleno ve 261–271. bodě odůvodnění, poskytuje řada soudních opravných prostředků subjektům údajů možnost o takové právní prostředky usilovat a získat je.

3.3.4.1 Ochranné mechanismy dostupné podle části 4 zákona o ochraně údajů

(261) Podle článku 165 zákona o ochraně údajů z roku 2018 má subjekt údajů právo podat stížnost u komisaře pro informace, pokud má za to, že v souvislosti s jeho osobními údaji došlo k porušení části 4 zákona o ochraně údajů z roku 2018. Komisař pro informace má pravomoc posoudit, jak správce a zpracovatel dodržují zákon o ochraně údajů z roku 2018 a vyžadovat od nich nezbytné kroky. Kromě toho jsou podle části 4 zákona o ochraně údajů z roku 2018 jednotlivci oprávněni podat u Vrchního soudu (nebo soudu Court of Session ve Skotsku) návrh na vydání příkazu, který bude vyžadovat, aby správce dodržoval práva na přístup k údajům ([482]), podání námitky vůči zpracování ([483]) a na opravu nebo výmaz ([484]).

(262) Jednotlivci jsou rovněž oprávněni požadovat od správce nebo zpracovatele náhradu škody způsobené porušením požadavku části 4 zákona o ochraně údajů z roku 2018 ([485]). Škoda zahrnuje jak finanční ztrátu, tak nefinanční újmu, například utrpení ([486]).

3.3.4.2 Ochranné mechanismy podle zákona o vyšetřovacích pravomocích z roku 2016

(263) Jednotlivci mohou dosáhnout nápravy v případě porušení zákona o vyšetřovacích pravomocích z roku 2016 u tribunálu pro kontrolu vyšetřovacích pravomocí.

(264) Tribunál pro kontrolu vyšetřovacích pravomocí je zřízen zákonem o úpravě vyšetřovacích pravomocí z roku 2000 a je nezávislý na výkonné moci ([487]). V souladu s článkem 65 zákona o úpravě vyšetřovacích pravomocí z roku 2000 jsou členové tohoto tribunálu jmenováni Jejím Veličenstvem na dobu pěti let. Člena tohoto tribunálu může z funkce odvolat Její Veličenstvo na návrh („address“) ([488]) obou komor Parlamentu Spojeného království ([489]).

([478]) Tyto obecné povinnosti týkající se ochrany soukromí jsou nyní stanoveny v čl. 2 odst. 2 zákona o vyšetřovacích pravomocích z roku 2016, který stanoví, že orgán veřejné moci jednající podle zákona o vyšetřovacích pravomocích z roku 2016 musí brát v úvahu, zda by bylo možné cíle, kterého se má dosáhnout příkazem, povolením nebo oznámením, rozumně dosáhnout jinými, méně rušivými prostředky, zda je úroveň ochrany, která se má uplatnit v souvislosti s jakýmkoli získáváním informací na základě příkazu, povolení nebo oznámení, vyšší kvůli zvláštní citlivosti daných informací, veřejnému zájmu na integritě a bezpečnosti telekomunikačních systémů a poštovních služeb a jakékoli další aspekty veřejného zájmu na ochraně soukromí.

([479]) Například na základě žádosti výboru pro zpravodajství a bezpečnost lze počet dní, během nichž může platit „naléhavý“ příkaz, nežli jej bude muset schválit soudní komisař, snížit z pěti na tři pracovní dny, a výbor získal pravomoc postoupit věci komisaři pro kontrolu vyšetřovacích pravomocí k šetření.

([480]) Rozsudek ve věci Schrems II, bod 194.

([481]) Rozsudek ve věci Schrems II, bod 197.

([482]) Ustanovení čl. 94 odst. 11 zákona o ochraně údajů z roku 2018.

([483]) Ustanovení čl. 99 odst. 4 zákona o ochraně údajů z roku 2018.

([484]) Ustanovení čl. 100 odst. 1 zákona o ochraně údajů z roku 2018.

([485]) Článek 169 zákona o ochraně údajů z roku 2018 připouští nároky podané „osobou, která utrpí škodu z důvodu porušení požadavku právních předpisů o ochraně údajů“. Podle informací poskytnutých orgány Spojeného království je v praxi pravděpodobné, že budou nárok nebo stížnost na zpravodajské služby podány u tribunálu pro kontrolu vyšetřovacích pravomocí, který má širokou jurisdikci a je schopen přiznat odškodnění / náhradu škody a u něhož vznesení nároku není spojeno s žádnými náklady.

([486]) Ustanovení čl. 169 odst. 5 zákona o ochraně údajů z roku 2018.

([487]) Podle přílohy 3 zákona o úpravě vyšetřovacích pravomocí z roku 2000 musí mít členové tribunálu konkrétní soudní praxi a mohou být jmenováni opětovně.

([488]) Tzv. „address“ je návrh předložený v Parlamentu Spojeného království, který má panovníka informovat o stanoviscích parlamentu v konkrétní věci.

([489]) Ustanovení čl. 1 odst. 5 přílohy 3 zákona o úpravě vyšetřovacích pravomocí z roku 2000.

(265) Podle článku 65 zákona o úpravě vyšetřovacích pravomocí z roku 2000 je tribunál příslušným soudním orgánem pro jakoukoli stížnost osoby poškozené jednáním podle zákona o vyšetřovacích pravomocích z roku 2016, zákona o úpravě vyšetřovacích pravomocí z roku 2000 nebo jakýmkoli jednáním zpravodajských služeb ([490]).

(266) K podání návrhu u tribunálu pro kontrolu vyšetřovacích pravomocí („vstupní požadavek“) musí být podle článku 65 zákona o úpravě vyšetřovacích pravomocí z roku 2000 jednotlivec přesvědčen ([491]), že došlo k jednání zpravodajské služby ve vztahu k němu, k jeho majetku, ke komunikaci zasílané jím nebo jemu nebo určené pro něj nebo k jeho využití jakékoli poštovní služby, telekomunikačních služeb nebo telekomunikačního systému“ ([492]). Kromě toho musí být stěžovatel přesvědčen, že k jednání došlo za „napadnutelných okolností“ ([493]) nebo „že bylo uskutečněno zpravodajskými službami nebo jejich jménem“ ([494]). Vzhledem k tomu, že zejména tento standard „přesvědčení“ je vykládán poměrně široce ([495]), je podání návrhu u tribunálu podmíněno nenáročnými vstupními požadavky.

(267) Pokud tribunál pro kontrolu vyšetřovacích pravomocí projednává stížnost, která k němu byla podána, je jeho povinností vyšetřit, zda osoby, proti nimž je ve stížnosti vzneseno jakékoli obvinění, jednaly ve vztahu ke stěžovateli, a rovněž vyšetřit orgán, který se údajně podílel na porušování právních předpisů, a to, zda k tvrzenému jednání došlo ([496]). Pokud tribunál vede jakékoli řízení, musí při svém rozhodování v těchto řízeních uplatňovat stejné zásady, jaké by použil soud při návrhu na soudní přezkum ([497]). Kromě toho jsou adresáti příkazů nebo výzev podle zákona o vyšetřovacích pravomocích z roku 2016 a každá další osoba, která zastává funkci podléhající Koruně nebo je zaměstnancem policie, nebo policejní komisař pro vyšetřování a přezkum, povinni zpřístupnit nebo poskytnout tomuto tribunálu všechny dokumenty a informace, které může tribunál požadovat k tomu, aby mohl vykonávat svou soudní pravomoc ([498]).

(268) Tribunál pro kontrolu vyšetřovacích pravomocí musí stěžovateli oznámit, zda bylo vydáno rozhodnutí v jeho prospěch, či nikoli ([499]). Podle čl. 67 odst. 6 a 7 zákona o úpravě vyšetřovacích pravomocí z roku 2000 má tribunál pravomoc vydávat předběžné příkazy a přiznávat jakékoli odškodnění nebo vydávat jiné příkazy, které uzná za vhodné. To může zahrnovat příkaz, kterým se anuluje nebo zruší jakýkoli příkaz nebo povolení, a příkaz vyžadující

([490]) Ustanovení čl. 65 odst. 5 zákona o úpravě vyšetřovacích pravomocí z roku 2000.

([491]) Standard testu „přesvědčení“ viz rozsudek ve věci Human Rights Watch v Secretary of State [2016] UKIPTrib15_165-CH, bod 41. V této věci tribunál pro kontrolu vyšetřovacích pravomocí s odkazem na judikaturu Evropského soudu pro lidská práva rozhodl, že vhodným testem je, zda pro tvrzené přesvědčení, že jakékoli jednání spadající do oblasti působnosti čl. 68 odst. 5 zákona o úpravě vyšetřovacích pravomocí z roku 2000 bylo uskutečněno zpravodajskými službami nebo jejich jménem, existuje jakýkoli základ, tedy že jednotlivec může tvrdit, že je obětí porušení právních předpisů způsobeného pouhou existencí tajných opatření nebo právních předpisů povolujících tajná opatření, pouze pokud je tento jednotlivec schopen prokázat, že vzhledem ke své osobní situaci je potenciálně vystaven riziku, že bude těmto opatřením podroben.

([492]) Ustanovení čl. 65 odst. 4 písm. a) zákona o úpravě vyšetřovacích pravomocí z roku 2000.

([493]) Takové okolnosti se týkají jednání orgánů veřejné moci, ke kterému dochází na základě oprávnění (např. příkazu, povolení / výzvy k získávání komunikace atd.), nebo pokud jsou okolnosti takové, že (ať už takové oprávnění existuje, či nikoli) by nebylo vhodné, aby k jednání došlo bez oprávnění, nebo alespoň bez řádného zvážení, zda je třeba o takové oprávnění žádat. Jednání schválené soudním komisařem se považuje za jednání, ke kterému došlo za napadnutelných okolností (čl. 65 odst. 7ZA zákona o úpravě vyšetřovacích pravomocí z roku 2000), zatímco jiná jednání, k nimž dojde se svolením osoby zastávající soudní funkci, se považuje za jednání, které se neuskutečnilo za napadnutelných okolností (čl. 65 odst. 7 a 8 zákona o úpravě vyšetřovacích pravomocí z roku 2000).

([494]) Podle informací, které poskytly orgány Spojeného království, nízká prahová hranice pro podání stížnosti určuje, že není neobvyklé, aby vyšetřování tribunálu došlo k závěru, že stěžovatel ve skutečnosti nikdy nebyl vyšetřován orgánem veřejné moci. Poslední statistická zpráva tribunálu pro kontrolu vyšetřovacích pravomocí uvádí, že v roce 2016 obdržel tribunál 209 stížností, z nichž 52 % z nich bylo považováno za bezdůvodné nebo šikanózní a 25 % bylo uzavřeno „bez rozhodnutí“. Orgány Spojeného království vysvětlily, že to buď znamená, že ve vztahu k stěžovateli nebyly použity žádné skryté činnosti/pravomoci, nebo že byly použity skryté techniky a tribunál rozhodl, že tato činnost byla zákonná. Kromě toho bylo 11 % stížností zamítnuto z důvodu soudní příslušnosti, staženo nebo bylo neplatných, 5 % bylo zamítnuto pro nedodržení lhůty a 7 % bylo rozhodnuto ve prospěch stěžovatele. Statistická zpráva tribunálu pro kontrolu vyšetřovacích pravomocí za rok 2016, k dispozici na této adrese: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([495]) Viz věc Human Rights Watch v Secretary of State [2016] UKIPTrib15_165-CH. V této věci tribunál pro kontrolu vyšetřovacích pravomocí s odkazem na judikaturu Evropského soudu pro lidská práva rozhodl, že vhodným testem pro dané přesvědčení, že jakékoli jednání spadající do oblasti působnosti čl. 68 odst. 5 zákona o úpravě vyšetřovacích pravomocí z roku 2000 bylo uskutečněno zpravodajskými službami nebo jejich jménem, je to, zda existuje jakýkoli základ pro takové přesvědčení, včetně toho, že jednotlivec může tvrdit, že je obětí porušení právních předpisů způsobeného pouhou existencí tajných opatření nebo právních předpisů povolujících tajná opatření, pokud je tento jednotlivec schopen prokázat, že vzhledem ke své osobní situaci je potenciálně vystaven riziku, že bude těmto opatřením podroben (viz rozsudek ve věci Human Rights Watch v Secretary of State, bod 41).

([496]) Ustanovení čl. 67 odst. 3 zákona o úpravě vyšetřovacích pravomocí z roku 2000.

([497]) Ustanovení čl. 67 odst. 2 zákona o úpravě vyšetřovacích pravomocí z roku 2000.

([498]) Ustanovení čl. 68 odst. 6 a 7 zákona o úpravě vyšetřovacích pravomocí z roku 2000.

([499]) Ustanovení čl. 68 odst. 4 zákona o úpravě vyšetřovacích pravomocí z roku 2000.

zničení jakýchkoli záznamů informací získaných při výkonu jakékoli pravomoci udělené příkazem, povolením nebo oznámením nebo jinak držené jakýmkoli orgánem veřejné moci ve vztahu k jakékoli osobě ([500]). Podle článku 67A zákona o úpravě vyšetřovacích pravomocí z roku 2000 lze proti rozhodnutí tribunálu podat opravný prostředek s výhradou povolení uděleného tribunálem nebo příslušným odvolacím soudem.

(269) A konečně je třeba zmínit, že úloha tribunálu pro kontrolu vyšetřovacích pravomocí byla při několika příležitostech projednávána v rámci stížností podaných k Evropskému soudu pro lidská práva, jmenovitě v rámci věci Kennedy proti Spojenému království ([501]) a nověji ve věci Big Brother Watch and others v. United Kingdom ([502]), kde soud prohlásil, že „tribunál pro kontrolu vyšetřovacích pravomocí nabízel robustní opravné prostředky komukoli, kdo měl podezření, že jeho komunikace byla odposlouchávána zpravodajskými službami“ ([503]).

3.3.4.3 Další dostupné ochranné mechanismy

(270) Jak je vysvětleno ve 109. až 111. bodě odůvodnění, prostředky nápravy podle zákona o lidských právech z roku 1998 a Evropského soudu pro lidská práva ([504]) jsou k dispozici také v oblasti národní bezpečnosti. Ustanovení čl. 65 odst. 2 zákona o úpravě vyšetřovacích pravomocí z roku 2000 poskytuje tribunálu pro kontrolu vyšetřovacích pravomocí výlučnou soudní pravomoc pro všechny nároky podle zákona o lidských právech ve vztahu ke zpravodajským službám ([505]). To znamená, jak uvedl Vrchní soud, „to, zda došlo k porušení zákona o lidských právech podle skutkových okolností konkrétního případu, v zásadě může projednat a rozhodnout nezávislý tribunál, který má přístup ke všem relevantním materiálům, včetně tajného materiálu. […] V této souvislosti máme také na paměti, že samotný tribunál nyní může podat opravný prostředek k příslušnému odvolacímu soudu (v Anglii a Walesu by jím byl odvolací soud) a že Nejvyšší soud nedávno rozhodl, že tribunál v zásadě podléhá soudnímu přezkumu: viz rozsudek ve věci R (Privacy International) v Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219” ([506]).

(271) Z výše uvedeného vyplývá, že pokud donucovací orgány nebo národní bezpečnostní orgány Spojeného království přistupují k osobním údajům spadajícím do oblasti působnosti tohoto rozhodnutí, řídí se takový přístup zákony, které stanoví podmínky, za nichž může přístup probíhat, a je zajištěno, aby byly přístup a další využívání údajů omezeny na to, co je nezbytné a přiměřené sledovaným cílům v oblasti vymáhání práva nebo národní bezpečnosti. Kromě toho takový přístup ve většině případů podléhá předchozímu schválení soudním orgánem, prostřednictvím schválení příkazu nebo výzvy k předání a v každém případě i nezávislému dohledu. Jakmile orgány veřejné moci získají přístup k údajům, podléhá zpracování údajů včetně dalšího sdílení a dalšího předávání zvláštním zárukám ochrany údajů podle části 3 zákona o ochraně údajů z roku 2018, které odrážejí záruky stanovené směrnicí (EU) 2016/680, pokud jde o zpracování donucovacími orgány, a části 4 zákona o ochraně údajů z roku 2018, pokud jde o zpracování zpravodajskými službami. A konečně také subjekty údajů požívají v této oblasti práv účinné správní a soudní ochrany, včetně práva dosáhnout přístupu k údajům nebo opravy nebo výmazu těchto údajů.

(272) Vzhledem k důležitosti těchto podmínek, omezení a záruk pro účely tohoto rozhodnutí bude Komise pečlivě sledovat uplatňování a výklad pravidel Spojeného království, která upravují přístup vlády k údajům. Tato činnost bude zahrnovat příslušný vývoj v oblasti právních předpisů, regulace a judikatury, jakož i aktivity Úřadu komisaře pro informace a dalších orgánů dohledu v této oblasti. Zvláštní pozornost bude rovněž věnována výkonu

([500]) Příkladem použití těchto pravomocí je rozsudek ve věci Liberty & Others vs. the Security Service, SIS, GCHQ, [2015] UKIP Trib 13_77-H_2. Tribunál rozhodl ve prospěch dvou stěžovatelů, neboť jejich komunikace byla v jednom případě uchovávána nad stanovené meze a ve druhém případě nebyl dodržen postup šetření stanovený vnitřními pravidly GCHQ. V prvním případě soud zpravodajským službám nařídil zničit komunikaci, která byla uchovávána po dobu delší, než činí příslušná lhůta. Ve druhém případě nebyl vydán příkaz ke zničení, protože komunikace nebyla uchována.

([501]) Rozsudek ve věci Kennedy, viz poznámka pod čarou 129.

([502]) Evropský soud pro lidská práva, věc Big Brother Watch and others v. United Kingdom (viz poznámka pod čarou 268 výše), body 413–415.

([503]) Evropský soud pro lidská práva, rozsudek ve věci Big Brother Watch, bod 425.

([504]) Jak dokládá například nedávný rozsudek velkého senátu Evropského soudu pro lidská práva ve věci Big Brother Watch and others v. United Kingdom (viz poznámka pod čarou 279 výše), umožňuje to účinnou soudní kontrolu (obdobnou kontrole, které podléhají členské státy EU) mezinárodním soudem, pokud jde o dodržování základních práv při přístupu k osobním údajům ze strany orgánů veřejné moci. Výkon rozsudků Evropského soudu pro lidská práva navíc podléhá zvláštnímu dohledu Rady Evropy.

([505]) V rozsudku ve věci Belhaj & others [2017] UKSC 3 bylo určení nezákonnosti odposlouchávání materiálu podléhajícího povinnosti mlčenlivosti založeno přímo na článku 8 EÚLP (viz rozhodnutí 11).

([506]) Vrchní soud, rozsudek ve věci Liberty, [2019] EWHC 2057 (Admin), bod 170.

příslušných rozsudků Evropského soudu pro lidská práva ze strany Spojeného království, včetně opatření uvedených v „akčních plánech“ a „akčních zprávách“ předložených Výboru ministrů v rámci dohledu nad dodržováním rozhodnutí Soudního dvora.

4. ZÁVĚR

(273) Komise má za to, že britské nařízení GDPR a zákon o ochraně údajů z roku 2018 zajišťují úroveň ochrany osobních údajů předávaných z Evropské unie, která je v zásadě rovnocenná úrovni ochrany zaručené nařízením (EU) 2016/679.

(274) Kromě toho má Komise za to, že jako celek mechanismy dohledu a způsoby ochrany v právních předpisech Spojeného království umožňují, aby porušení právních předpisů byla identifikována a v praxi potrestána, a subjektu údajů nabízejí právní prostředky pro získání přístupu k osobním údajům, které se ho týkají, a případně pro dosažení opravy nebo výmazu takovýchto údajů.

(275) V neposlední řadě má Komise na základě dostupných informací o právním řádu Spojeného království za to, že jakýkoli zásah do základních práv fyzických osob, jejichž osobní údaje se předávají z Evropské unie do Spojeného království, ze strany orgánů veřejné moci Spojeného království pro účely veřejného zájmu, zejména pro účely vymáhání práva a národní bezpečnosti, bude omezen na rozsah nezbytný pro dosažení daného oprávněného cíle a že existuje účinná právní ochrana před takovým zásahem.

(276) S ohledem na zjištění tohoto rozhodnutí by proto mělo být rozhodnuto, že Spojené království zajišťuje odpovídající úroveň ochrany ve smyslu článku 45 nařízení (EU) 2016/679 vykládaného ve světle Listiny základních práv Evropské unie.

(277) Tento závěr se opírá o příslušný vnitrostátní režim i mezinárodní závazky Spojeného království, zejména o dodržování Evropské úmluvy o lidských právech a podrobení se soudní pravomoci Evropského soudu pro lidská práva. Pokračující dodržování těchto mezinárodních závazků je proto obzvláště důležitým prvkem posouzení, na němž se zakládá toto rozhodnutí.

5. ÚČINKY TOHOTO ROZHODNUTÍ A ČINNOST ORGÁNŮ PRO OCHRANU ÚDAJŮ

(278) Členské státy a jejich orgány musí přijmout opatření nezbytná k dosažení souladu s akty orgánů Unie, neboť jim v zásadě svědčí presumpce legality, a tudíž zakládají právní účinky tak dlouho, dokud nejsou vzaty zpět, zrušeny v rámci žaloby na neplatnost nebo prohlášeny za neplatné v návaznosti na žádost o rozhodnutí o předběžné otázce nebo na námitku protiprávnosti.

(279) V důsledku toho je rozhodnutí Komise o odpovídající ochraně podle čl. 45 odst. 3 nařízení (EU) 2016/679 závazné pro všechny orgány členských států, kterým je určeno, a to i pro nezávislé dozorové úřady. Během období použitelnosti tohoto rozhodnutí může zejména docházet k předáním od správce nebo zpracovatele v Evropské unii správcům nebo zpracovatelům ve Spojeném království, aniž by bylo nutné získat další povolení.

(280) Je třeba připomenout, že podle čl. 58 odst. 5 nařízení (EU) 2016/679 a podle vysvětlení Soudního dvora v rozsudku ve věci Schrems ([507]), jestliže vnitrostátní orgán pro ochranu údajů zpochybňuje, a to i na základě stížnosti, slučitelnost rozhodnutí Komise o odpovídající ochraně se základními právy fyzické osoby na soukromí a ochranu údajů, musí mu vnitrostátní právo poskytnout procesní prostředek, který mu umožní uplatnit tyto výtky před vnitrostátním soudem, který může být povinen předložit Soudnímu dvoru žádost o rozhodnutí o předběžné otázce ([508]).

([507]) Rozsudek ve věci Schrems, bod 65.

([508]) Rozsudek ve věci Schrems, bod 65: „V tomto ohledu přísluší vnitrostátnímu normotvůrci, aby stanovil procesní prostředky, které by dotyčnému vnitrostátnímu orgánu dozoru umožnily uplatnit výtky, jež považuje za opodstatněné, před vnitrostátními soudy, aby tyto soudy v případě, že sdílejí pochybnosti vyjádřené tímto orgánem ohledně platnosti rozhodnutí Komise, předložily žádost o rozhodnutí o předběžné otázce za účelem přezkumu platnosti tohoto rozhodnutí.“

6. SLEDOVÁNÍ, POZASTAVENÍ PLATNOSTI, ZRUŠENÍ NEBO ZMĚNA TOHOTO ROZHODNUTÍ

(281) Podle čl. 45 odst. 4 nařízení (EU) 2016/679 musí Komise po přijetí tohoto rozhodnutí průběžně sledovat příslušný vývoj ve Spojeném království, aby mohla posoudit, zda stále zajišťuje v zásadě rovnocennou úroveň ochrany. Takové sledování je v tomto případě obzvláště důležité, neboť Spojené království bude spravovat, uplatňovat a vymáhat nový režim ochrany údajů, který již nebude podléhat právu Evropské unie a který se může vyvíjet. V tomto ohledu bude zvláštní pozornost věnována uplatňování pravidel Spojeného království pro předávání osobních údajů do třetích zemí v praxi a možnému dopadu tohoto uplatňování na úroveň ochrany poskytovanou údajům předávaným podle tohoto rozhodnutí; účinnosti výkonu individuálních práv včetně případného příslušného vývoje v oblasti práva a praxe, pokud jde o výjimky z těchto práv nebo omezení těchto práv (zejména výjimky týkající se zachování účinné kontroly imigrace); jakož i dodržování omezení a záruk týkajících se přístupu vlády. V rámci sledování ze strany Komise bude kromě jiných prvků zohledňován vývoj judikatury a dohledu ze strany Úřadu komisaře pro informace a ostatních nezávislých subjektů.

(282) Aby toto sledování usnadnily, měly by orgány Spojeného království neprodleně informovat Komisi o jakékoli podstatné změně právního řádu Spojeného království, která má dopad na právní rámec, který je předmětem tohoto rozhodnutí, jakož i o vývoji postupů souvisejících se zpracováním osobních údajů, které jsou posuzovány v tomto rozhodnutí, a to jak z hlediska zpracování osobních údajů správci a zpracovateli podle britského nařízení GDPR, tak z hlediska omezení a záruk použitelných na přístup orgánů veřejné moci k osobním údajům. Tyto informace by měly zahrnovat vývoj týkající se prvků uvedených ve 281. bodě odůvodnění.

(283) Aby Komise navíc mohla účinně plnit svou kontrolní funkci, měly by ji členské státy informovat o veškerých příslušných krocích vnitrostátních úřadů pro ochranu údajů, zejména v souvislosti s dotazy nebo stížnostmi subjektů údajů z EU týkajícími se předávání osobních údajů z Unie správcům nebo zpracovatelům ve Spojeném království. Komise by rovněž měla být informována o jakýchkoli známkách toho, že kroky orgánů veřejné moci Spojeného království odpovědných za prevenci, vyšetřování, odhalování nebo stíhání trestných činů nebo za národní bezpečnost, včetně jakýchkoli dozorových úřadů, nezajišťují požadovanou úroveň ochrany.

(284) Pokud z dostupných informací, zejména z informací vyplývajících ze sledování tohoto rozhodnutí nebo poskytnutých orgány Spojeného království nebo členských států, vyplyne, že úroveň ochrany poskytované Spojeným královstvím již nemusí být odpovídající, měla by Komise neprodleně informovat příslušné orgány Spojeného království a požadovat, aby byla ve stanovené lhůtě, která nesmí přesáhnout dobu tří měsíců, přijata vhodná opatření. V případě potřeby lze tuto lhůtu prodloužit o určitou dobu s přihlédnutím k povaze dané záležitosti a/nebo daných opatření, která mají být přijata. Takovýto postup by byl zahájen například v případech, kdy by se další předávání, včetně předávání na základě nových předpisů o přiměřené ochraně přijatých ministrem nebo mezinárodních dohod uzavřených Spojeným královstvím, již neuskutečňovalo v rámci záruk zajišťujících kontinuitu ochrany ve smyslu článku 44 nařízení (EU) 2016/679.

(285) Pokud po uplynutí stanovené lhůty příslušné orgány Spojeného království tato opatření nepřijmou nebo jiným způsobem uspokojivě neprokážou, že toto rozhodnutí je nadále založeno na odpovídající úrovni ochrany, zahájí Komise postup podle čl. 93 odst. 2 nařízení (EU) 2016/679 s cílem částečně nebo úplně zrušit toho rozhodnutí nebo pozastavit jeho platnost.

(286) Alternativně Komise tento postup zahájí s cílem změnit toto rozhodnutí, zejména tím, že se na předávání údajů budou vztahovat další podmínky, nebo že se omezí oblasti působnosti zjištění o odpovídající úrovni ochrany jen na předávání údajů, u nichž je odpovídající úroveň ochrany nadále zaručena.

(287) V závažných, naléhavých a řádně odůvodněných případech Komise využije možnost postupem podle čl. 93 odst. 3 nařízení (EU) 2016/679 přijmout okamžitě použitelné prováděcí akty, kterými se rozhodnutí zruší, změní nebo se dočasně pozastaví jeho platnost.

7. DOBA PLATNOSTI A PRODLOUŽENÍ PLATNOSTI TOHOTO ROZHODNUTÍ

(288) Komise musí vzít v úvahu, že až skončí přechodné období stanovené v dohodě o vystoupení a jakmile přestane platit prozatímní ustanovení podle článku 782 dohody o obchodu a spolupráci mezi EU a Spojeným královstvím, bude Spojené království spravovat, uplatňovat a vymáhat nový režim ochrany údajů oproti režimu existujícímu v době, kdy bylo vázáno právem EU. To může zejména znamenat úpravy nebo změny rámce ochrany údajů posuzovaného v tomto rozhodnutí, jakož i další relevantní vývoj.

(289) Je proto vhodné stanovit, že toto rozhodnutí bude použitelné po dobu čtyř let ode dne svého vstupu v platnost.

(290) Pokud zejména z informací získaných při sledování tohoto rozhodnutí vyplyne, že zjištění týkající se odpovídající úrovně ochrany zajištěné ve Spojeném království jsou stále věcně a právně odůvodněná, měla by Komise nejpozději šest měsíců před koncem platnosti tohoto rozhodnutí zahájit postup pro změnu tohoto rozhodnutí prodloužením jeho časové působnosti v zásadě o další čtyřleté období. Jakýkoli takový prováděcí akt, kterým se mění toto rozhodnutí, se přijímá postupem podle čl. 93 odst. 2 nařízení (EU) 2016/679.

8. **ZÁVĚREČNÉ ÚVAHY**

(291) Evropský sbor pro ochranu osobních údajů zveřejnil své stanovisko ([509]), které bylo při přípravě tohoto rozhodnutí zohledněno.

(292) Opatření stanovená tímto rozhodnutím jsou v souladu se stanoviskem výboru zřízeného podle článku 93 nařízení (EU) 2016/679,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

1. Pro účely článku 45 nařízení (EU) 2016/679 Spojené království zajišťuje odpovídající úroveň ochrany osobních údajů předávaných v oblasti působnosti nařízení (EU) 2016/679 z Evropské unie do Spojeného království.

2. Toto rozhodnutí se netýká osobních údajů předávaných pro účely kontroly imigrace ve Spojeném království nebo osobních údajů, které jinak spadají do oblasti působnosti výjimky z určitých práv subjektu údajů za účelem zachování účinné kontroly imigrace podle bodu 4 odst. 1 přílohy 2 zákona o ochraně údajů z roku 2018.

Článek 2

Pokud příslušné dozorové úřady v členských státech za účelem ochrany fyzických osob s ohledem na zpracování jejich osobních údajů uplatní pravomoc podle článku 58 nařízení (EU) 2016/679, pokud jde o předání údajů spadající do oblasti působnosti stanovené v článku 1, oznámí dotyčný členský stát tuto skutečnost bezodkladně Komisi.

Článek 3

1. Komise neustále sleduje uplatňování právního rámce, na němž je založeno toto rozhodnutí, včetně podmínek, za kterých dochází k dalšímu předávání, výkonu individuálních práv a přístupu orgánů Spojeného království k údajům předaným na základě tohoto rozhodnutí, s cílem posoudit, zda Spojené království i nadále zajišťuje odpovídající úroveň ochrany ve smyslu článku 1.

2. Členské státy a Komise se vzájemně informují o případech, kdy komisař pro informace nebo jakýkoli jiný příslušný orgán Spojeného království nezajišťuje soulad s právním rámcem, na němž je toto rozhodnutí založeno.

3. Členské státy a Komise se vzájemně informují o jakýchkoli známkách toho, že zásahy britských orgánů veřejné moci do práva fyzických osob na ochranu jejich osobních údajů přesahují rámec toho, co je nezbytně nutné, nebo že proti takovým zásahům není účinné právní ochrany.

4. Pokud má Komise informace o tom, že odpovídající úroveň ochrany již není zajištěna, informuje příslušné orgány Spojeného království a může rozhodnout o dočasném pozastavení platnosti, zrušení nebo změně tohoto rozhodnutí.

([509]) Stanovisko č. 14/2021 k návrhu prováděcího rozhodnutí podle nařízení Evropského parlamentu a Rady (EU) 2016/679 o odpovídající ochraně osobních údajů poskytované Spojeným královstvím, který předložila Evropská komise, k dispozici na této adrese: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

5. Komise může rozhodnout o dočasném pozastavení platnosti, zrušení nebo změně tohoto rozhodnutí v případě, že nedostatečná spolupráce vlády Spojeného království brání Komisi v určení, zda je dotčeno zjištění podle čl. 1 odst. 1.

Článek 4

Použitelnost tohoto rozhodnutí skončí dnem 27. června 2025, pokud nebude prodloužena v souladu s postupem uvedeným v čl. 93 odst. 2 nařízení (EU) 2016/679.

Článek 5

Toto rozhodnutí je určeno členským státům.

V Bruselu dne 28. června 2021.

Za Komisi
Didier REYNDERS
člen Komise