II.

(Nezakonodavni akti)

ODLUKE

PROVEDBENA UREDBA KOMISIJE (EU) 2021/1772

od 28. lipnja 2021.

u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća o primjerenoj zaštiti osobnih podataka u Ujedinjenoj Kraljevini

(priopćeno pod brojem dokumenta C(2021) 4800)

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) ([1]), a posebno njezin članak 45. stavak 3.,

budući da:

1. UVOD

(1) Uredbom (EU) 2016/679 utvrđuju se pravila za prijenos osobnih podataka od voditelja obrade ili izvršitelja obrade u Europskoj uniji trećim zemljama i međunarodnim organizacijama, u mjeri u kojoj je takav prijenos obuhvaćen njezinim područjem primjene. Pravila o međunarodnim prijenosima podataka utvrđena su u poglavlju V. te uredbe, odnosno u člancima od 44. do 50. Iako je protok osobnih podataka u zemlje izvan Europske unije i iz njih bitan za proširenje međunarodne suradnje i prekogranične trgovine, razina zaštite osobnih podataka u Europskoj uniji ne smije se ugroziti prijenosima trećim zemljama ([2]).

(2) U skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 Komisija može putem provedbenog akta odlučiti da treća zemlja, područje, ili jedan ili više određenih sektora unutar treće zemlje, ili međunarodna organizacija osigurava primjerenu razinu zaštite. Pod tim uvjetom prijenosi osobnih podataka trećoj zemlji mogu se obavljati bez potrebe za bilo kakvim dodatnim odobrenjem, kako je utvrđeno u članku 45. stavku 1. i uvodnoj izjavi 103. te uredbe.

(3) Kako je navedeno u članku 45. stavku 2. Uredbe (EU) 2016/679, donošenje odluke o primjerenosti mora se temeljiti na sveobuhvatnoj analizi pravnog poretka treće zemlje, koja obuhvaća i pravila koja se primjenjuju na uvoznike podataka i ograničenja i zaštitne mjere u pogledu pristupa tijela javne vlasti osobnim podacima. Komisija u procjeni mora utvrditi jamči li predmetna treća zemlja razinu zaštite koja je „u načelu istovjetna" onoj koja je osigurana u Europskoj uniji (uvodna izjava 104. Uredbe (EU) 2016/679). Standard na temelju kojeg se procjenjuje je li zaštita „u načelu istovjetna" utvrđen je u zakonodavstvu Europske unije, ponajprije Uredbi (EU) 2016/679, te u sudskoj praksi Suda Europske unije ([3]). U tom je pogledu važan i Referentni dokument o primjerenosti koji je izdao Europski odbor za zaštitu podataka (EDPB) ([4]).

([1]) SL L 119, 4.5.2016., str. 1.
([2]) Vidjeti uvodnu izjavu 101. Uredbe (EU) 2016/679.
([3]) Vidjeti nedavni predmet C-311/18, *Facebook Ireland i Schrems* (dalje u tekstu „*Schrems II*"), ECLI:EU:C:2020:559.
([4]) Europski odbor za zaštitu podataka, Referentni dokument o primjerenosti, WP 254 rev.01. dostupan na: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Kako je pojasnio Sud Europske unije, to ne zahtijeva utvrđivanje potpuno istovjetne razine zaštite ([5]). Naime, pravna sredstva kojima se predmetna treća zemlja koristi za zaštitu osobnih podataka mogu se razlikovati od onih koja se primjenjuju u Europskoj uniji, pod uvjetom da se u praksi pokažu djelotvornima za osiguravanje primjerene razine zaštite ([6]). Prema tome, standard primjerenosti ne podrazumijeva doslovno ponavljanje pravila Unije. Umjesto toga ispituje se pruža li predmetni strani sustav kao cjelina potrebnu razinu zaštite podataka sadržajem prava na zaštitu osobnih podataka i njihovom djelotvornom provedbom, nadzorom i ostvarivanjem ([7]).

(5) Komisija je pomno analizirala pravo i praksu Ujedinjene Kraljevine. Na temelju nalaza navedenih u uvodnim izjavama od 8. do 270. Komisija zaključuje da Ujedinjena Kraljevina osigurava primjerenu razinu zaštite osobnih podataka koji se prenose iz Europske unije u Ujedinjenu Kraljevinu u okviru područja primjene Uredbe (EU) 2016/679.

(6) Taj se zaključak ne odnosi na osobne podatke koji se prenose za potrebe kontrole useljavanja koju provodi Ujedinjena Kraljevina ili koji su na drugi način obuhvaćeni izuzećem od određenih prava ispitanika radi provedbe učinkovite kontrole useljavanja („izuzeće o useljavanju”) u skladu s točkom 4. podtočkom 1. Priloga 2. Zakonu Ujedinjene Kraljevine o zaštiti podataka. Prema odluci Žalbenog suda Engleske i Walesa (*Court of Appeal*) od 26. svibnja 2021. valjanost i tumačenje izuzeća o useljavanju nisu riješeni u skladu s pravom Ujedinjene Kraljevine. Iako priznaje da se prava ispitanika u načelu mogu ograničiti za potrebe kontrole useljavanja kao „važan aspekt javnog interesa”, Žalbeni sud utvrdio je da je izuzeće o useljavanju u svojem postojećem obliku nespojivo s pravom Ujedinjene Kraljevine jer u zakonodavnoj mjeri nedostaju posebne odredbe kojima se utvrđuju zaštitne mjere iz članka 23. stavka 2. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine ([8]). U tim bi uvjetima prijenose osobnih podataka iz Unije u Ujedinjenu Kraljevinu na koje se može primijeniti izuzeće o useljavanju trebalo isključiti iz područja primjene ove Odluke ([9]). Nakon što se otkloni nespojivost s pravom Ujedinjene Kraljevine, trebalo bi ponovno ocijeniti izuzeće o useljavanju, kao i potrebu za zadržavanjem ograničenja područja primjene ove Odluke.

(7) Ova Odluka ne bi trebala utjecati na izravnu primjenu Uredbe (EU) 2016/679 na organizacije s poslovnim nastanom u Ujedinjenoj Kraljevini ako su ispunjeni uvjeti o teritorijalnom području primjene te uredbe utvrđeni u njezinu članku 3.

2. PRAVILA KOJA SE PRIMJENJUJU NA OBRADU OSOBNIH PODATAKA

2.1. Ustavni okvir

(8) Ujedinjena Kraljevina je parlamentarna demokracija s ustavnim monarhom kao šefom države. Ima suvereni parlament, koji je nadređen svim ostalim vladinim institucijama, izvršnu vlast koja proizlazi iz parlamenta i odgovorna je parlamentu te neovisno sudstvo. Ovlasti izvršne vlasti proizlaze iz njezine sposobnosti da osigura povjerenje izabranog Zastupničkog doma, a odgovorna je obama domovima Parlamenta, čija je zadaća preispitivanje rada Vlade te raspravljanje o zakonskim prijedlozima i donošenje zakona.

([5]) Predmet C-362/14, *Schrems* (dalje u tekstu „*Schrems I*”), ECLI:EU:C:2015:650, točka 73.

([6]) Predmet *Schrems I*, točka 74.

([7]) Vidjeti Komunikaciju Komisije Europskom parlamentu i Vijeću „Razmjena i zaštita osobnih podataka u globaliziranom svijetu”, COM(2017) 7 od 10.1.2017., odjeljak 3.1., str. 6.–7., dostupnu na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:52017DC0007&from=HR.

([8]) Žalbeni sud (Građanski odjel), predmet *Open Rights Group protiv Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport*, [2021] EWCA Civ 800, točke od 53. do 56. Žalbeni sud poništio je odluku Visokog suda (*High Court of Justice*) kojom je izuzeće prethodno ocijenjeno s obzirom na Uredbu (EU) 2016/679 (posebno njezin članak 23.) i Povelju Europske unije o temeljnim pravima te je utvrdio da je izuzeće zakonito *(Open Rights Group & Anor, R (On the Application Of) protiv Secretary of State for the Home Department i Anor* [2019] EWHC 2562).

([9]) Pod uvjetom da su ispunjeni primjenjivi uvjeti, prijenosi za potrebe kontrole useljavanja Ujedinjene Kraljevine mogu se izvršiti na temelju mehanizama prijenosa predviđenih člancima od 46. do 49. Uredbe (EU) 2016/679.

(9) Parlament Ujedinjene Kraljevine prenio je određene ovlasti Škotskom parlamentu (*Scottish Parliament*), Velškom parlamentu (*Senedd Cymru*) i Skupštini Sjeverne Irske (*Northern Ireland Assembly*) koje im omogućuju da u Škotskoj, Walesu i Sjevernoj Irskoj uređuju domaća pitanja koja Parlament Ujedinjene Kraljevine nije zadržao za sebe. Iako je za zaštitu podataka nadležan Parlament Ujedinjene Kraljevine, tj. isti se propisi primjenjuju u cijeloj zemlji, druga područja politike relevantna za ovu Odluku obuhvaćena su prenesenim nadležnostima. Na primjer, nadležnosti za sustave kaznenog pravosuđa, uključujući policijsku djelatnost, u Škotskoj su prenesene Škotskom parlamentu, a u Sjevernoj Irskoj Skupštini Sjeverne Irske. Ujedinjena Kraljevina nema kodificirani ustav u smislu zadanog konstitutivnog dokumenta. Ustavna načela proizašla su s vremenom, posebice iz sudske prakse i običaja. Sudovi su priznali ustavnopravni značaj određenih akata, kao što su Velika povelja sloboda (*Magna Carta*), Povelja o pravima iz 1689. (*Bill of Rights 1689*) i Zakon o ljudskim pravima iz 1998. (*Human Rights Act 1998*). Temeljna prava pojedinaca razvila su se, kao dio ustava, u okviru precedentnog prava (*common law*), navedenih akata i međunarodnih ugovora, osobito Europske konvencije o ljudskim pravima, koju je Ujedinjena Kraljevina ratificirala 1951. Ujedinjena Kraljevina ratificirala je 1987. i Konvenciju Vijeća Europe za zaštitu osoba glede automatizirane obrade osobnih podataka (Konvencija br. 108) ([10]).

(10) Zakonom o ljudskim pravima iz 1998. prava iz Europske konvencije o ljudskim pravima ugrađuju se u pravo Ujedinjene Kraljevine. Zakonom o ljudskim pravima svim se pojedincima daju temeljna prava i slobode predviđene člancima od 2. do 12. i člankom 14. Europske konvencije o ljudskim pravima, člancima 1., 2. i 3. Prvog protokola uz tu konvenciju te člankom 1. Trinaestog protokola uz tu konvenciju, u vezi s člancima 16., 17. i 18. te konvencije. To uključuje pravo na poštovanje osobnog i obiteljskog života (i pravo na zaštitu podataka koje je dio tog prava) te pravo na pošteno suđenje ([11]). Naime, u skladu s člankom 8. te konvencije tijelo javne vlasti smije zadirati u pravo na privatnost samo u skladu sa zakonom i ako je to u demokratskom društvu nužno radi interesa nacionalne sigurnosti, javnog reda i mira ili gospodarske dobrobiti zemlje te radi sprečavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih.

(11) U skladu sa Zakonom o ljudskim pravima iz 1998. svi postupci tijelâ javne vlasti moraju biti u skladu s pravima iz Konvencije ([12]). Osim toga, primarno i sekundarno zakonodavstvo moraju se tumačiti i provoditi u skladu s pravima iz Konvencije ([13]).

2.2. **Okvir za zaštitu podataka u Ujedinjenoj Kraljevini**

(12) Ujedinjena Kraljevina povukla se iz Europske unije 31. siječnja 2020. Na temelju Sporazuma o povlačenju Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske iz Europske unije i Europske zajednice za atomsku energiju ([14]) pravo Unije nastavilo se primjenjivati u Ujedinjenoj Kraljevini u prijelaznom razdoblju do 31. prosinca 2020. Prije povlačenja i u prijelaznom razdoblju zakonodavni okvir za zaštitu osobnih podataka u Ujedinjenoj Kraljevini sastojao se od relevantnih propisa EU-a (posebno Uredbe (EU) 2016/679 i Direktive (EU) 2016/680 Europskog parlamenta i Vijeća ([15])) i nacionalnih propisa, osobito Zakona o zaštiti podataka iz 2018. (DPA iz 2018.) ([16]) u kojem su propisana nacionalna pravila, kad je to dopušteno Uredbom (EU) 2016/679, kojima se određuje i ograničava primjena pravila iz Uredbe (EU) 2016/679 i prenesene Direktive (EU) 2016/680.

([10]) Načela iz Konvencije br. 108 izvorno su provedena u pravu Ujedinjene Kraljevine Zakonom o zaštiti podataka iz 1984., koji je zamijenjen Zakonom o zaštiti podataka iz 1998., a zatim Zakonom o zaštiti podataka iz 2018. (tumačenim zajedno s Općom uredbom o zaštiti podataka Ujedinjene Kraljevine). Ujedinjena Kraljevina potpisala je 2018. i Protokol o izmjeni Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka (poznat kao Konvencija br. 108+), a trenutačno radi na ratifikaciji te konvencije.

([11]) Članci 6. i 8. EKLJP-a (vidjeti i Prilog 1. Zakonu o ljudskim pravima iz 1998.).

([12]) Članak 6. Zakona o ljudskim pravima iz 1998.

([13]) Članak 3. Zakona o ljudskim pravima iz 1998.

([14]) Sporazum o povlačenju Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske iz Europske unije i Europske zajednice za atomsku energiju, 2019/C 384 I/01, XT/21054/2019/INIT, (SL C 384I, 12.11.2019., str. 1.), dostupan na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=HR.

([15]) Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL L 119, 4.5.2016., str. 89.), dostupna na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016L0680&from=HR.

([16]) Zakon o zaštiti podataka iz 2018., dostupan na: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

(13) Kako bi se pripremila za povlačenje iz Europske unije, Vlada Ujedinjene Kraljevine donijela je Zakon o povlačenju iz Europske unije iz 2018. ([17]), kojim se izravno primjenjivo zakonodavstvo Unije uključuje u pravo Ujedinjene Kraljevine ([18]). To takozvano „zadržano pravo Unije" uključuje cijelu Uredbu (EU) 2016/679 (uključujući uvodne izjave) ([19]). Prema tom zakonu sudovi u Ujedinjenoj Kraljevini neizmijenjeno zadržano pravo Unije moraju tumačiti u skladu s relevantnom sudskom praksom Suda Europske unije i općim načelima prava Unije, u skladu s učinkom koji ta praksa i načela imaju neposredno prije kraja prijelaznog razdoblja (takozvana „zadržana sudska praksa EU-a" odnosno „zadržana opća načela prava Unije") ([20]).

(14) Na temelju Zakona o povlačenju iz Europske unije iz 2018. ministri Ujedinjene Kraljevine imaju ovlast putem zakonskih instrumenata donositi sekundarno zakonodavstvo kako bi uveli potrebne promjene zadržanog prava Unije koje su posljedica povlačenja Ujedinjene Kraljevine iz Europske unije. Ministri su iskoristili tu ovlast tako što su donijeli Uredbu o zaštiti podataka, privatnosti i elektroničkim komunikacijama (izmjene itd.) (izlazak iz Unije) iz 2019. (Uredba DPPEC) ([21]). Uredbom DPPEC izmijenjena je Uredba (EU) 2016/679, kako je uvedena u pravo Ujedinjene Kraljevine Zakonom o povlačenju iz Europske unije iz 2018., Zakonom o zaštiti podataka iz 2018. i drugim zakonodavstvom o zaštiti podataka, da bi odgovarala nacionalnom kontekstu ([22]).

(15) Stoga se pravni okvir za zaštitu osobnih podataka u Ujedinjenoj Kraljevini nakon završetka prijelaznog razdoblja sastoji od:

— Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, kako je uključena u pravo Ujedinjene Kraljevine na temelju Zakona o povlačenju iz Europske unije iz 2018. i izmijenjena Uredbom DPPEC ([23]), i

— DPA-a iz 2018. ([24]), kako je izmijenjen Uredbom DPPEC.

(16) Budući da se Opća uredba o zaštiti podataka Ujedinjene Kraljevine temelji na zakonodavstvu EU-a, pravila o zaštiti podataka u Ujedinjenoj Kraljevini u mnogim aspektima uvelike odražavaju odgovarajuća pravila primjenjiva unutar Europske unije.

(17) Uz ovlasti koje su Zakonom o povlačenju iz Europske unije iz 2018. dane ministru, nekoliko odredbi DPA-a iz 2018. daje ovlasti ministru da donosi sekundarno zakonodavstvo kako bi se izmijenile određene odredbe Zakona ili navela dopunska i dodatna pravila ([25]). Ministar je dosad izvršio ovlast iz članka 137. DPA-a iz 2018. samo kako bi

([17]) Zakon o povlačenju iz Europske unije iz 2018., dostupan na: https://www.legislation.gov.uk/ukpga/2018/16/contents.

([18]) Namjera je i učinak Zakona o povlačenju iz Europske unije iz 2018. da se svi izravni propisi Unije koji su bili uključeni u pravo Ujedinjene Kraljevine na kraju prijelaznog razdoblja uključe u pravo Ujedinjene Kraljevine s učinkom kakav imaju u pravu Unije neposredno prije kraja prijelaznog razdoblja; vidjeti članak 3. Zakona o povlačenju iz Europske unije iz 2018.

([19]) U Pojašnjenjima Zakona o povlačenju iz Europske unije iz 2018. navedeno je: „Ako se propis prenosi na temelju ovog članka, sam tekst propisa činit će dio nacionalnog propisa. To će uključivati cjeloviti tekst bilo kojeg instrumenta EU-a (uključujući njegove uvodne izjave)." (Pojašnjenja Zakona o povlačenju iz Europske unije iz 2018., točka 83., dostupno na: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Prema informacijama koje su dostavila tijela Ujedinjene Kraljevine, s obzirom na to da uvodne izjave nemaju status obvezujućih pravnih pravila, nije ih bilo potrebno izmijeniti na isti način kao što su članci Uredbe (EU) 2016/679 izmijenjeni Uredbom DPPEC.

([20]) Članak 6. Zakona o povlačenju iz Europske unije iz 2018.

([21]) Uredba o zaštiti podataka, privatnosti i elektroničkim komunikacijama (izmjene itd.) (izlazak iz EU-a) iz 2019., dostupna na: https://www.legislation.gov.uk/uksi/2019/419/contents/made, kako je izmijenjena Uredbom DPPEC iz 2020., koja je dostupna na: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([22]) Te izmjene Opće uredbe o zaštiti podataka Ujedinjene Kraljevine i DPA-a iz 2018. uglavnom su tehničke, na primjer brisanje upućivanja na „države članice" ili prilagodba terminologije, npr. zamjena upućivanja na Uredbu (EU) 2016/679 upućivanjima na Opću uredbu o zaštiti podataka Ujedinjene Kraljevine. U nekim su slučajevima izmjene bile potrebne kako bi se odrazio isključivo domaći kontekst odredbi, na primjer s obzirom na to „tko" donosi „uredbe o primjerenosti" za potrebe zakonodavnog okvira Ujedinjene Kraljevine za zaštitu podataka (vidjeti članak 17.A DPA-a iz 2018.), tj. ministar umjesto Europske komisije.

([23]) Opća uredba o zaštiti podataka, Keelingov prilog, dostupno na: 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]) Zakon o zaštiti podataka iz 2018., Keelingov prilog, dostupno na: 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]) Takve se ovlasti primjerice nalaze u članku 16. (ovlast donošenja, u specifičnim, usko ograničenim situacijama, daljnjih izuzeća od određenih odredbi Opće uredbe o zaštiti podataka Ujedinjene Kraljevine), članku 17.A (ovlast donošenja uredbi o primjerenosti), člancima 212. i 213. (ovlasti za početak primjene zakonodavnih akata i donošenja prijelaznih odredbi) i članku 211. (ovlast donošenja manjih i bitnih izmjena) DPA-a iz 2018.

donio Uredbu o zaštiti podataka (naknade i informacije) (izmjena) iz 2019., u kojoj su utvrđene okolnosti u kojima voditelji obrade podataka moraju platiti godišnju naknadu neovisnom tijelu za zaštitu podataka u Ujedinjenoj Kraljevini – povjereniku za informiranje.

(18) Naposljetku, daljnje smjernice o zakonodavstvu Ujedinjene Kraljevine u području zaštite podataka dostupne su u kodeksima dobre prakse i drugim smjernicama koje donosi povjerenik za informiranje. Iako službeno nisu pravno obvezujuće, te smjernice važne su za tumačenje i pokazuju kako se zakonodavstvo u području zaštite podataka primjenjuje i kako ga povjerenik izvršava u praksi. Ponajprije, u člancima od 121. do 125. DPA-a iz 2018. zahtijeva se da povjerenik izradi kodekse dobre prakse o razmjeni podataka, izravnom marketingu, dizajnu i zaštiti podataka primjerenima za dob te novinarstvu.

(19) Stoga su struktura i glavne sastavnice pravnog okvira Ujedinjene Kraljevine koji se primjenjuje na podatke koji se prenose na temelju ove Odluke vrlo slične okviru koji se primjenjuje u Europskoj uniji. To uključuje činjenicu da se taj okvir ne oslanja samo na obveze utvrđene u nacionalnom pravu, koje su oblikovane pravom Unije, već i na obveze iz međunarodnog prava, osobito obveze Ujedinjene Kraljevine da poštuje EKLJP i Konvenciju br. 108 i priznavanje nadležnosti Europskog suda za ljudska prava. Stoga su te obveze koje proizlaze iz pravno obvezujućih međunarodnih instrumenata, a koje se posebno odnose na zaštitu osobnih podataka, važan element pravnog okvira koji se procjenjuje u ovoj Odluci.

2.3. **Materijalno i teritorijalno područje primjene**

(20) Slično Uredbi (EU) 2016/679, Opća uredba o zaštiti podataka Ujedinjene Kraljevine primjenjuje se na obradu osobnih podataka koja se u cijelosti ili djelomično obavlja automatizirano ili na neautomatiziranu obradu ako su osobni podaci dio sustava pohrane ([26]). Definicije „osobnih podataka”, „ispitanika” i „obrade” u Općoj uredbi o zaštiti podataka Ujedinjene Kraljevine iste su kao i definicije iz Uredbe (EU) 2016/679 ([27]). Osim toga, Opća uredba o zaštiti podataka Ujedinjene Kraljevine primjenjuje se na ručnu obradu nestrukturiranih osobnih podataka ([28]) koje drže određena tijela javne vlasti u Ujedinjenoj Kraljevini ([29]), iako su načela i prava iz Opće uredbe o zaštiti podataka Ujedinjene Kraljevine koja nisu relevantna za takve osobne podatke ukinuta člancima 24. i 25. DPA-a iz 2018. Slično odredbama iz Uredbe (EU) 2016/679, Opća uredba o zaštiti podataka Ujedinjene Kraljevine ne primjenjuje se na obradu osobnih podataka koju provodi pojedinac u okviru isključivo osobne ili kućne aktivnosti ([30]).

(21) Područje primjene Opće uredbe o zaštiti podataka Ujedinjene Kraljevine prošireno je i na obradu tijekom aktivnosti koje neposredno prije kraja prijelaznog razdoblja nisu bile obuhvaćene područjem primjene prava Unije (npr. nacionalna sigurnost) ([31]) ili su bile obuhvaćene područjem primjene glave V. poglavlja 2. Ugovora o Europskoj uniji (aktivnosti zajedničke vanjske i sigurnosne politike) ([32]). Kao i u sustavu Europske unije, Opća uredba o zaštiti podataka Ujedinjene Kraljevine ne primjenjuje se na obradu osobnih podataka koju obavlja nadležno tijelo u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od

([26]) Članak 2. stavci 1. i 5. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine.

([27]) Članak 4. stavak 1. i članak 2. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine.

([28]) Ručna nestrukturirana obrada osobnih podataka definirana je u članku 2. stavku 5. točki (b) kao obrada osobnih podataka koja nije automatizirana ili strukturirana obrada osobnih podataka.

([29]) U članku 2. stavku 1.A Opće uredbe o zaštiti podataka Ujedinjene Kraljevine navedeno je da se Uredba primjenjuje i na ručnu nestrukturiranu obradu osobnih podataka koje drži tijelo javne vlasti za slobodu informiranja. Upućivanje na tijela javne vlasti za slobodu informiranja znači svako tijelo javne vlasti kako je definirano u Zakonu o slobodi informiranja iz 2000. ili svako škotsko tijelo javne vlasti kako je definirano u Zakonu o slobodi informiranja (Škotska) iz 2002. (Akt Škotskog parlamenta br. 13). Članak 21. stavak 5. DPA-a iz 2018.

([30]) Članak 2. stavak 2. točka (a) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine.

([31]) Aktivnosti nacionalne sigurnosti obuhvaćene su područjem primjene Opće uredbe o zaštiti podataka Ujedinjene Kraljevine samo ako ih nadležno tijelo ne obavlja u svrhe kaznenog progona (kad se primjenjuje dio 3. DPA-a iz 2018.) ili ako takvu obradu provodi obavještajna služba ili drugi subjekt koji obrađuje podatke u njezino ime (njezine su aktivnosti izuzete iz područja primjene Opće uredbe o zaštiti podataka Ujedinjene Kraljevine i podliježu dijelu 4. DPA-a iz 2018. u skladu s člankom 2. stavkom 2. točkom (c) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine). Na primjer, policija može provesti sigurnosne provjere zaposlenika kako bi osigurala da mu se može povjeriti pristup materijalu koji se tiče nacionalne sigurnosti. Iako je policija nadležno tijelo za potrebe kaznenog progona, predmetna obrada ne provodi se u svrhu kaznenog progona pa bi se primjenjivala Opća uredba o zaštiti podataka Ujedinjene Kraljevine. Vidjeti Okvir za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, odjeljak H: Okvir za zaštitu podataka i istražne ovlasti s obzirom na nacionalnu sigurnost, str. 8., dostupno na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf

([32]) Članak 2. stavak 1. točke (a) i (b) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine.

prijetnji javnoj sigurnosti i njihova sprečavanja (takozvane „svrhe kaznenog progona") (umjesto toga, takva je obrada uređena dijelom 3. DPA-a iz 2018., kao što je uređena i Direktivom (EU) 2016/680 na temelju prava Unije) ni na obradu osobnih podataka koju obavljaju obavještajne službe (Sigurnosna služba, Tajna obavještajna služba i Vladin komunikacijski stožer), koja je uređena dijelom 4. DPA-a iz 2018. ([33])

(22) Teritorijalno područje primjene Opće uredbe o zaštiti podataka Ujedinjene Kraljevine opisano je u članku 3. te uredbe ([34]) i uključuje obradu osobnih podataka (neovisno o tome gdje se ona obavlja) u okviru aktivnosti poslovnog nastana voditelja obrade ili izvršitelja obrade u Ujedinjenoj Kraljevini te obradu osobnih podataka ispitanika koji se nalaze u Ujedinjenoj Kraljevini ako su aktivnosti obrade povezane s ponudom robe ili usluga takvim ispitanicima ili praćenjem njihova ponašanja ([35]). To odražava pristup iz članka 3. Uredbe (EU) 2016/679.

2.4. **Definicije osobnih podataka i koncepata voditelja obrade i izvršitelja obrade**

(23) Definicije osobnih podataka, obrade, voditelja obrade, izvršitelja obrade te definicija pseudonimizacije, utvrđene u Uredbi (EU) 2016/679, zadržane su u Općoj uredbi o zaštiti podataka Ujedinjene Kraljevine bez bitnih izmjena ([36]). Nadalje, posebne kategorije podataka definirane su u članku 9. stavku 1. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine na isti način kao i na temelju Uredbe (EU) 2016/679 („koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka ili biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca"). U članku 205. DPA-a iz 2018. navodi se definicija „biometrijskih podataka" ([37]), „podataka koji se odnose na zdravlje" ([38]) i „genetskih podataka" ([39]).

2.5. **Zaštitne mjere, prava i obveze**

2.5.1. *Zakonitost i poštenost obrade*

(24) Osobni podaci trebali bi se obrađivati zakonito i pošteno.

(25) Načela zakonitosti, poštenosti i transparentnosti te osnove za zakonitu obradu zajamčeni su pravom Ujedinjene Kraljevine u članku 5. stavku 1. točki (a) i članku 6. stavku 1. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, koji su isti kao odgovarajuće odredbe u Uredbi (EU) 2016/679 ([40]). Članak 8. DPA-a iz 2018. dopunjuje članak 6. stavak 1. točku (e) tako što se u njemu određuje da obrada osobnih podataka na temelju članka 6. stavka 1. točke (e) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine (nužna za izvršavanje zadaće od javnog interesa ili pri

([33]) Članak 2. stavak 2. točke (b) i (c) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine.

([34]) Isto teritorijalno područje primjene primjenjuje se na obradu osobnih podataka na temelju dijela 2. DPA-a iz 2018. koji dopunjuje Opću uredbu o zaštiti podataka Ujedinjene Kraljevine (članak 207. stavak 1.A).

([35]) To posebno znači da se DPA iz 2018. i samim time ova Odluka ne primjenjuju na krunske posjede Ujedinjene Kraljevine (Jersey, Guernsey i Otok Man) i prekomorske teritorije Ujedinjene Kraljevine, kao što su, na primjer, Falklandski otoci i teritorij Gibraltara.

([36]) Članak 4. stavci 1., 2., 5., 7. i 8. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine.

([37]) „Biometrijski podaci" znači osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci.

([38]) „Podaci koji se odnose na zdravlje" znači osobni podaci povezani s fizičkim ili mentalnim zdravljem pojedinca, uključujući pružanje zdravstvenih usluga, kojima se daju informacije o njegovu zdravstvenom statusu.

([39]) „Genetski podaci" znači osobni podaci koji se odnose na naslijeđena ili stečena genetska obilježja pojedinca koja daju jedinstvenu informaciju o fiziologiji ili zdravlju tog pojedinca, i koji su dobiveni osobito analizom biološkog uzorka dotičnog pojedinca.

([40]) Prema članku 6. stavku 1. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine obrada je zakonita samo ako i u onoj mjeri u kojoj je ispunjeno sljedeće: (a) ispitanik je dao privolu za obradu svojih osobnih podataka u jednu ili više posebnih svrha; (b) obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora; (c) obrada je nužna radi poštovanja pravnih obveza voditelja obrade; (d) obrada je nužna kako bi se zaštitili životno važni interesi ispitanika ili druge fizičke osobe; (e) obrada je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade; ili (f) obrada je nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

izvršavanju službene ovlasti voditelja obrade) uključuje obradu osobnih podataka koja je nužna za pravosuđe, izvršavanje funkcije bilo kojeg doma Parlamenta, izvršavanje funkcije dodijeljene osobi zakonom, propisima ili načelima vladavine prava, izvršavanje funkcije Krune, ministra Krune ili ministarstva ili aktivnost koja podupire ili promiče demokratski angažman.

(26) Kad je riječ o privoli (jedna od osnova za zakonitu obradu), u Općoj uredbi o zaštiti podataka Ujedinjene Kraljevine neizmijenjenima su zadržani i uvjeti predviđeni u članku 7. Uredbe (EU) 2016/679, što znači da voditelj obrade mora moći dokazati da je ispitanik dao privolu, pisani zahtjev za privolu mora se predočiti na jasnom i jednostavnom jeziku, ispitanik mora imati pravo da u bilo kojem trenutku povuče privolu, a kad se procjenjuje je li privola bila dobrovoljna, treba uzeti u obzir je li izvršenje ugovora uvjetovano privolom za obradu osobnih podataka koja nije nužna za izvršenje tog ugovora. Nadalje, prema članku 8. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, ako informacijsko društvo pruža usluge djetetu, djetetova privola je zakonita samo ako dijete ima najmanje 13 godina. To je u skladu s dobnom skupinom utvrđenom u članku 8. Uredbe (EU) 2016/679.

2.5.2. *Obrada posebnih kategorija osobnih podataka*

(27) Trebale bi postojati posebne zaštitne mjere ako se obrađuju „posebne kategorije” podataka.

(28) Opća uredba o zaštiti podataka Ujedinjene Kraljevine i DPA iz 2018. sadržavaju posebna pravila za obradu posebnih kategorija osobnih podataka, koja su definirana u članku 9. stavku 1. te uredbe na isti način kao i na temelju Uredbe (EU) 2016/679 (vidjeti uvodnu izjavu 23.). Prema članku 9. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine obrada posebnih kategorija podataka načelno je zabranjena, osim ako se primjenjuje posebna iznimka.

(29) Te iznimke (navedene u članku 9. stavcima 2. i 3. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine) ne uvode nikakve sadržajne izmjene odredbi iz članka 9. stavaka 2. i 3. Uredbe (EU) 2016/679. Osim ako je ispitanik dao izričitu privolu za obradu tih osobnih podataka, obrada posebnih kategorija osobnih podataka dopuštena je samo u specifičnim i ograničenim okolnostima. U većini slučajeva obrada osjetljivih podataka mora biti nužna za posebnu svrhu definiranu u odgovarajućoj odredbi (vidjeti članak 9. stavak 2. točke (b), (c), (f), (g), (h), (i) i (j)).

(30) Nadalje, ako se za iznimku iz članka 9. stavka 2. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine zahtijeva da bude odobrena u okviru prava ili se upućuje na javni interes, u članku 10. DPA-a iz 2018. zajedno s Prilogom 1. DPA-u iz 2018. dodatno se određuju uvjeti koji se moraju ispuniti da bi se mogle primijeniti iznimke. Na primjer, ako se osjetljivi podaci obrađuju radi zaštite „javnog zdravlja” (članak 9. stavak 2. točka (i) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine), u dijelu 1. točki 3. podtočki (b) Priloga 1., uz provjeru nužnosti, zahtijeva se da takvu obradu provodi „zdravstveni radnik ili da je takva obrada pod odgovornošću zdravstvenog radnika” ili „druga osoba na koju se primjenjuje obveza povjerljivosti na temelju zakona, propisa ili načela vladavine prava”, među ostalim na temelju ustaljene obveze povjerljivosti iz precedentnog prava.

(31) Ako se osjetljivi podaci obrađuju za potrebe značajnog javnog interesa (članak 9. stavak 2. točka (g) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine), u dijelu 2. Priloga 1. DPA-u iz 2018. naveden je iscrpan popis svrha za koje se može smatrati da su od značajnog javnog interesa i za svaku od tih svrha utvrđeni su specifični dodatni uvjeti. Na primjer, promicanje rasne i etničke raznolikosti na visokim razinama rukovodstva organizacije priznaje se kao značajan javni interes. Obrada osjetljivih podataka u tu posebnu svrhu podliježe detaljnim zahtjevima, među ostalim da se provodi u okviru procesa utvrđivanja primjerenih pojedinaca koji mogu biti na visokim položajima, da je nužna za promicanje rasne i etničke raznolikosti te da vjerojatno neće uzrokovati veliku štetu ili duševnu bol ispitanika.

(32) U članku 11. stavku 1. DPA-a iz 2018. utvrđeni su uvjeti za obradu osobnih podataka u okolnostima opisanima u članku 9. stavku 3. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, koji se odnosi na obvezu čuvanja tajne. To uključuje okolnosti u kojima obradu provodi zdravstveni radnik ili socijalni radnik ili je obrada pod njegovom odgovornošću ili ako je provodi druga osoba koja je u tim okolnostima vezana obvezom povjerljivosti na temelju zakona, propisa ili načela vladavine prava.

(33) Osim toga, za primjenu mnogih iznimki navedenih u članku 9. stavku 2. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine potrebne su primjerene i posebne zaštitne mjere. Ovisno o prirodi obrade i stupnju rizika za prava i slobode ispitanika, uvjetima za obradu predviđenima u Prilogu 1. DPA-u iz 2018. utvrđene su različite zaštitne mjere. U Prilogu 1. utvrđeni su uvjeti za svaki slučaj obrade.

(34) U nekim slučajevima DPA iz 2018. uređuje i ograničava vrstu osjetljivih podataka koji se mogu obrađivati kako bi se ispunila određena pravna osnova. Na primjer, u točki 8. Priloga 1. dopušta se obrada osjetljivih podataka u svrhu promicanja jednakih mogućnosti ili jednakog postupanja. Taj uvjet za obradu može se primijeniti samo ako podaci otkrivaju rasno ili etničko podrijetlo, vjerska ili filozofska uvjerenja, spolnu orijentaciju ili ako je riječ o zdravstvenim podacima.

(35) U nekim slučajevima DPA iz 2018. ograničava vrstu voditelja obrade koji može primijeniti uvjet za obradu. Na primjer, u točki 23. Priloga 1. predviđa se obrada osjetljivih podataka s obzirom na odgovore izabranih predstavnika javnosti. Taj uvjet za obradu može se primijeniti samo ako je voditelj obrade izabrani predstavnik ili ako djeluje pod njegovim vodstvom.

(36) U nekim drugim slučajevima DPA iz 2018. ograničava kategorije ispitanika za primjenu uvjeta za obradu. Na primjer, u točki 21. Priloga 1. uređuje se obrada osjetljivih podataka za strukovne mirovinske programe. Taj se uvjet može primijeniti samo ako je predmetni ispitanik brat ili sestra, roditelj, djed ili baka ili pradjed ili prabaka člana programa.

(37) Osim toga, ako se poziva na iznimke iz članka 9. stavka 2. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine koje su dodatno određene u članku 10. DPA-a iz 2018. zajedno s Prilogom 1. DPA-u iz 2018., voditelj obrade u većini je slučajeva obvezan sastaviti „dokument o odgovarajućoj politici”. U tom se dokumentu moraju opisati postupci kojima voditelj obrade osigurava usklađenost s načelima iz članka 5. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine. Moraju se utvrditi i politike za zadržavanje i brisanje te navesti vjerojatno razdoblje pohrane. Voditelji obrade prema potrebi moraju preispitivati i ažurirati taj dokument. Voditelj obrade mora zadržati dokument o politici šest mjeseci nakon završetka obrade i na zahtjev ga mora staviti na raspolaganje povjereniku za informiranje ([41]).

(38) Prema točki 41. Priloga 1. DPA-u iz 2018., dokumentu o politici uvijek se mora priložiti proširena evidencija obrade. U toj se evidenciji moraju pratiti obveze iz dokumenta o politici, tj. brišu li se ili zadržavaju podaci u skladu s politikama. Ako se ne poštuju politike, u evidenciji se moraju navesti razlozi. U evidenciji se mora opisati i kako obrada ispunjava članak 6. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine (zakonitost obrade) i specifični uvjet iz Priloga 1. DPA-u iz 2018. na koji se poziva.

(39) Naposljetku, kao i u Uredbi (EU) 2016/679, u Općoj uredbi o zaštiti podataka Ujedinjene Kraljevine predviđaju se i opće zaštitne mjere za određene postupke obrade posebnih kategorija podataka. U članku 35. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine zahtijeva se procjena učinka na zaštitu podataka u slučaju opsežne obrade posebnih kategorija podataka. Prema članku 37. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, voditelj obrade ili izvršitelj obrade mora imenovati službenika za zaštitu podataka ako se njegove osnovne djelatnosti sastoje od opsežne obrade posebnih kategorija podataka.

(40) Kad je riječ o osobnim podacima koji se odnose na kaznene osude i kažnjiva djela, članak 10. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine isti je kao i članak 10. Uredbe (EU) 2016/679. Dopušta obradu osobnih podataka koji se odnose na kaznene osude i kažnjiva djela samo pod nadzorom službenog tijela ili kad je obrada odobrena nacionalnim pravom kojim se propisuju odgovarajuće zaštitne mjere za prava i slobode ispitanikâ.

(41) Ako se obrada podataka koji se odnose na kaznene osude i kažnjiva djela ne obavlja pod nadzorom službenog tijela, u članku 10. stavku 5. DPA-a iz 2018. predviđeno je da se takva obrada može obavljati samo u posebne svrhe/u posebnim situacijama utvrđenima u dijelovima 1., 2. i 3. Priloga 1. DPA-u iz 2018. i da ta obrada podliježe posebnim zahtjevima koji su utvrđeni za svaku od tih svrha/situacija. Na primjer, podatke o kaznenim osudama može obrađivati neprofitno tijelo ako se obrada provodi (a) u sklopu njegovih legitimnih aktivnosti s odgovarajućim zaštitnim mjerama zaklade, udruženja ili drugog neprofitnog tijela s političkim, filozofskim, vjerskim ili sindikalnim ciljem te (b) pod uvjetom i. da se obrada odnosi samo na članove ili bivše članove tijela ili na osobe koje imaju redovan kontakt s njim u vezi s njegovim svrhama i ii. da osobni podaci nisu priopćeni nikome izvan tog tijela bez privole ispitanikâ.

([41]) Točke od 38. do 40. Priloga 1. DPA-u iz 2018.

(42) Nadalje, u dijelu 3. Priloga 1. DPA-u iz 2018. utvrđuju se daljnje okolnosti u kojima se podaci o kaznenim osudama mogu koristiti, a koje odgovaraju pravnim osnovama za obradu osjetljivih podataka iz članka 9. stavka 2. Uredbe (EU) 2016/679 i Opće uredbe o zaštiti podataka Ujedinjene Kraljevine (npr. privola ispitanika, životno važni interesi pojedinca ako ispitanik pravno ili fizički nije u mogućnosti dati privolu, ako je očito da je podatke već objavio ispitanik, ako je obrada nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva itd.).

2.5.3. *Ograničavanje svrhe, točnost, smanjenje količine podataka, ograničenje pohrane i sigurnost podataka*

(43) Osobni podaci trebali bi se obrađivati u određenu svrhu i zatim se upotrebljavati samo ako to nije nespojivo sa svrhom obrade.

(44) To je načelo predviđeno člankom 5. stavkom 1. točkom (b) Uredbe (EU) 2016/679 i zadržano je bez izmjena u članku 5. stavku 1. točki (b) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine. I uvjeti za daljnju usklađenu obradu na temelju članka 6. stavka 4. Uredbe (EU) 2016/679 zadržani su bez bitnih izmjena u članku 6. stavku 4. točkama od (a) do (e) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine.

(45) Nadalje, podaci bi trebali biti točni i, prema potrebi, ažurirani. Trebali bi biti i primjereni i relevantni i ne bi trebali biti pretjerani u odnosu na svrhe u koje se obrađuju te bi se načelno trebali čuvati samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju.

(46) Ta načela smanjenja količine podataka, točnosti i ograničenja pohrane utvrđena su u članku 5. stavku 1. točkama od (c) do (e) Uredbe (EU) 2016/679 i zadržana su bez izmjena u članku 5. stavku 1. točkama od (c) do (e) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine.

(47) Osobni podaci trebali bi se obrađivati i tako da se jamči njihova sigurnost, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja. U tu bi svrhu poslovni subjekti trebali poduzeti odgovarajuće tehničke ili organizacijske mjere za zaštitu osobnih podataka od mogućih prijetnji. Te bi mjere trebalo procijeniti tako da se uzmu u obzir najnovija dostignuća i povezani troškovi.

(48) Sigurnost podataka sadržana je u pravu Ujedinjene Kraljevine primjenom načela cjelovitosti i povjerljivosti u članku 5. stavku 1. točki (f) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine i članku 32. te uredbe o sigurnosti obrade. Te su odredbe iste kao i odgovarajuće odredbe Uredbe (EU) 2016/679. Nadalje, pod istim uvjetima kao što su oni utvrđeni u člancima 33. i 34. Uredbe (EU) 2016/679, u Općoj uredbi o zaštiti podataka Ujedinjene Kraljevine zahtijeva se izvješćivanje nadzornog tijela o povredi osobnih podataka (članak 33. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine) i obavješćivanje ispitanika o povredi osobnih podataka (članak 34. te uredbe).

2.5.4. *Transparentnost*

(49) Ispitanike bi trebalo obavijestiti o glavnim obilježjima obrade njihovih osobnih podataka.

(50) To se osigurava člancima 13. i 14. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, u kojima su uz opće načelo transparentnosti navedena i pravila o informacijama koje treba dostaviti ispitaniku ([42]). Općom uredbom o zaštiti podataka Ujedinjene Kraljevine nisu uvedene nikakve bitne izmjene tih pravila u usporedbi s odgovarajućim člancima Uredbe (EU) 2016/679. Međutim, kao i na temelju Uredbe (EU) 2016/679, zahtjevi za transparentnost iz tih članaka podložni su određenim iznimkama određenima u DPA-u iz 2018. (vidjeti uvodne izjave od 55. do 72.).

([42]) U članku 13. stavku 1. točki (f) i članku 14. stavku 1. točki (f) upućivanja na odluke o primjerenosti koje donosi Komisija zamijenjena su upućivanjima na jednakovrijedne instrumente Ujedinjene Kraljevine, tj. uredbe o primjerenosti na temelju DPA-a iz 2018. Osim toga, u članku 14. stavku 5. točkama (c) i (d) upućivanja na pravo Unije ili pravo države članice zamijenjena su upućivanjem na nacionalno pravo (kao primjere takvog nacionalnog prava koje može pripadati području primjene članka 14. stavka 5. točke (c) Ujedinjena Kraljevina navela je članak 7. Zakona o trgovcima metalnim otpadom iz 2013., u kojem se nalaze pravila o registru dozvola za metalni otpad, ili dio 35. Zakona o trgovačkim društvima iz 2006., u kojem se nalaze pravila o registru trgovačkih društava. Slično tome, primjer nacionalnog zakona koji bi mogao pripadati području primjene članka 14. stavka 5. točke (d) mogao bi uključivati propise kojima se utvrđuju pravila o čuvanju poslovne tajne ili obveze iz ugovora o radu ili obvezu povjerljivosti iz precedentnog prava (kao što su osobni podaci koje obrađuju zdravstveni radnici, službe za ljudske resurse, socijalni radnici itd.).

2.5.5. *Prava pojedinaca*

(51) Ispitanici bi trebali imati određena prava koja mogu ostvariti u odnosu na voditelja obrade ili izvršitelja obrade, osobito pravo na pristup podacima, pravo na prigovor na obradu i pravo na ispravak ili brisanje podataka. Takva prava istodobno mogu biti ograničena ako su ta ograničenja nužna i proporcionalna za zaštitu javne sigurnosti ili drugih važnih ciljeva od općeg javnog interesa.

2.5.5.1. Materijalna prava

(52) U Općoj uredbi o zaštiti podataka Ujedinjene Kraljevine pojedincima se daju ista provediva prava kao i u Uredbi (EU) 2016/679. Odredbe kojima se osiguravaju prava pojedinaca zadržane su u Općoj uredbi o zaštiti podataka Ujedinjene Kraljevine bez bitnih izmjena.

(53) Ta prava uključuju pravo ispitanika na pristup (članak 15. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine), pravo na ispravak (članak 16. te uredbe), pravo na brisanje (članak 17. te uredbe), pravo na ograničenje obrade (članak 18. te uredbe), obvezu izvješćivanja u vezi s ispravkom ili brisanjem osobnih podataka ili ograničenjem obrade (članak 19. te uredbe), pravo na prenosivost podataka (članak 20. te uredbe) i pravo na prigovor (članak 21. te uredbe) ([43]). Potonje uključuje i pravo ispitanika da uloži prigovor na obradu osobnih podataka za potrebe izravnog marketinga predviđene člankom 21. stavcima 2. i 3. Uredbe (EU) 2016/679. Nadalje, na temelju članka 122. DPA-a iz 2018. povjerenik za informiranje mora izraditi kodeks dobre prakse o provođenju izravnog marketinga u skladu sa zahtjevima iz zakonodavstva o zaštiti podataka (i Uredbe o privatnosti i elektroničkim komunikacijama (Direktiva EK-a) iz 2003.) i druge takve smjernice za promicanje dobre prakse u izravnom marketingu koje povjerenik smatra primjerenima. Ured povjerenice za informiranje trenutačno radi na kodeksu za izravni marketing ([44]).

(54) U Općoj uredbi o zaštiti podataka Ujedinjene Kraljevine bez bitnih izmjena zadržano je i pravo ispitanika da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi koja proizvodi pravne učinke koji se na njega odnose ili na sličan način značajno na njega utječu, kako je navedeno u članku 22. Opće uredbe o zaštiti podataka. Međutim, dodan je novi stavak 3.A kako bi se uputilo na to da su u članku 14. DPA-a iz 2018. utvrđene zaštitne mjere za prava, slobode i legitimne interese ispitanika kad se obrada obavlja na temelju članka 22. stavka 2. točke (b) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine. To se primjenjuje samo ako je osnova za takvu odluku odobrenje ili zahtjev na temelju prava Ujedinjene Kraljevine i ne primjenjuje se ako je odluka nužna na temelju ugovora ili ako se donosi uz izričitu privolu ispitanika. Ako se primjenjuje članak 14. DPA-a iz 2018., voditelj obrade mora, čim je to razumno izvedivo, u pisanom obliku obavijestiti ispitanika da je odluka donesena isključivo na temelju automatizirane obrade. Ispitanik ima pravo tražiti da voditelj obrade, u roku od jednog mjeseca od primitka obavijesti, preispita odluku ili da donese novu odluku koja se ne temelji isključivo na automatiziranoj obradi. Ministar ima ovlast donositi daljnje zaštitne mjere u vezi s automatiziranim donošenjem odluka. Ta ovlast još nije iskorištena.

2.5.5.2. Ograničenja prava pojedinaca i druge odredbe

(55) U DPA-u iz 2018. utvrđeno je nekoliko ograničenja prava pojedinaca, koja odgovaraju okviru članka 23. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine. U tom se okviru ne uvode nikakva ograničenja prava na prigovor na izravni marketing, kako je predviđeno u članku 21. stavcima 2. i 3. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, ili prava ispitanika da se na njega ne odnosi automatizirano donošenje odluka, kako je predviđeno u članku 22. te uredbe.

(56) Ograničenja su detaljno opisana u prilozima od 2. do 4. DPA-u iz 2018. Tijela Ujedinjene Kraljevine objasnila su da se vode dvama načelima: načelom specifičnosti (primjena detaljnog pristupa, podjela širokih ograničenja na više specifičnijih odredbi) i načelom uvjetovanosti (svaka je odredba dopunjena zaštitnim mjerama u obliku ograničenja ili uvjeta za sprečavanje zloupotrebe) ([45]).

([43]) U članku 17. stavku 1. točki (e) i članku 17. stavku 3. točki (b) upućivanja na pravo Unije ili pravo države članice zamijenjena su upućivanjem na nacionalno pravo (kao primjere takvog nacionalnog prava na temelju članka 17. stavka 1. točke (e) Ujedinjena Kraljevina navela je Uredbu o obrazovanju (informacije o učenicima) (Engleska) iz 2006., u kojoj se zahtijeva da se imena učenika izbrišu iz školskih registara nakon što učenici napuste školu, ili članak 34.F Zakona o zdravstvenoj djelatnosti iz 1983., u kojem su utvrđena pravila o uklanjanju imena iz Registra liječnika primarne zdravstvene zaštite i Registra specijalista.

([44]) Nacrt kodeksa dobre prakse dostupan je na: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf

([45]) Okvir za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, odjeljak E: Ograničenja, str. 1., dostupno na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf

(57) Ograničenja opisana u članku 23. stavku 1. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine osmišljena su tako da se osigura da se primjenjuju samo u utvrđenim okolnostima kad je to nužno u demokratskom društvu i proporcionalno legitimnim ciljevima koji se ograničenjima nastoje ostvariti. Nadalje, u skladu s ustaljenom sudskom praksom o tumačenju ograničenja, izuzeće od sustava zaštite podataka može se u nekom određenom slučaju primijeniti samo ako je to nužno i proporcionalno ([46]). Zahtijeva se da ocjena nužnosti bude „stroga, tako da svako zadiranje u prava ispitanika mora biti proporcionalno ozbiljnosti prijetnje javnom interesu. Stoga je za njegovu primjenu potrebna klasična analiza proporcionalnosti" ([47]).

(58) Ciljevi koje se nastoji ostvariti tim ograničenjima odgovaraju ciljevima navedenima u članku 23. Uredbe (EU) 2016/679, osim ograničenja za nacionalnu sigurnost i obranu koja su umjesto toga uređena člankom 26. DPA-a iz 2018., ali se na njih primjenjuju isti zahtjevi nužnosti i proporcionalnosti (vidjeti uvodne izjave od 63. do 66.).

(59) Neka ograničenja, na primjer ona povezana sa sprečavanjem i otkrivanjem kaznenih djela, uhićenjem ili kaznenim progonom počinitelja i utvrđivanjem ili naplatom poreza ili pristojbi ([48]), dopuštaju ograničenja svih prava pojedinaca i obveza u pogledu transparentnosti (uz iznimku prava iz članka 21. stavka 2. i članka 22.). Područje primjene drugih ograničenja ograničeno je na obveze u pogledu transparentnosti i prava pristupa, kao što su ograničenja povezana s odvjetničkom tajnom ([49]), pravom oslobođenja od zahtjeva za davanje informacija koje bi dovele do samooptuživanja ([50]) i korporativnim financijama, osobito sprečavanjem trgovanja na temelju povlaštenih informacija ([51]). Mali broj ograničenja dopušta ograničenje obveze voditelja obrade da obavijesti ispitanika o povredi podataka te načela ograničavanja svrhe i zakonitosti, poštenosti i transparentnosti obrade ([52]).

(60) Neka se ograničenja automatski „u potpunosti" primjenjuju na određenu vrstu obrade osobnih podataka (na primjer, primjena obveza u pogledu transparentnosti i prava pojedinaca isključena je ako se osobni podaci obrađuju u svrhu procjene primjerenosti osobe za pravosudnu dužnost ili ako osobne podatke obrađuje sud ili pojedinac u okviru svoje sudske nadležnosti).

(61) Međutim, u većini slučajeva relevantna točka iz Priloga 2. DPA-u iz 2018. određuje da se ograničenje primjenjuje samo kad (i u mjeri u kojoj) bi primjena odredbi „vjerojatno dovela u pitanje" legitimni cilj koji se nastoji ostvariti tim ograničenjem: na primjer, navedene odredbe Opće uredbe o zaštiti podataka Ujedinjene Kraljevine ne primjenjuju se na osobne podatke koji se obrađuju u svrhu sprečavanja ili otkrivanja kaznenog djela, uhićenja ili kaznenog progona počinitelja ili utvrđivanja ili naplate poreza ili pristojbi „u mjeri u kojoj bi primjena tih odredbi vjerojatno dovela u pitanje" bilo koju od tih aktivnosti ([53]).

(62) Sudovi Ujedinjene Kraljevine dosljedno tumače standard „vjerojatno dovela u pitanje" kao „vrlo veliku i važnu vjerojatnost ugrožavanja utvrđenih javnih interesa" ([54]). Stoga se na ograničenje na koje se primjenjuje test ugrožavanja može pozvati samo ako i u mjeri u kojoj postoji vrlo velika i važna vjerojatnost da bi se dodjelom određenog prava ugrozio predmetni javni interes. Voditelj obrade odgovoran je da u svakom pojedinom slučaju ocijeni jesu li ti uvjeti ispunjeni ([55]).

(63) Uz ograničenja iz Priloga 2. DPA-u iz 2018., u članku 26. DPA-a iz 2018. predviđeno je izuzeće koje se može primijeniti na određene odredbe Opće uredbe o zaštiti podataka Ujedinjene Kraljevine i DPA-a iz 2018. ako je nužno za potrebe zaštite nacionalne sigurnosti ili u svrhe obrane. To se izuzeće primjenjuje na načela zaštite podataka (osim načela zakonitosti), obveze u pogledu transparentnosti, prava ispitanika, obvezu obavješćivanja o povredi podataka, pravila o međunarodnim prijenosima, neke od dužnosti i ovlasti povjerenika za informiranje te

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

([47]) *Guriev protiv Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), točka 43. U vezi s tim vidjeti i predmet *Lin protiv Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), točka 80.

([48]) Točka 2. Priloga 2. DPA-u iz 2018.

([49]) Točka 19. Priloga 2. DPA-u iz 2018.

([50]) Točka 20. Priloga 2. DPA-u iz 2018.

([51]) Točka 21. Priloga 2. DPA-u iz 2018.

([52]) Na primjer, ograničenja prava na obavješćivanje o povredi osobnih podataka dopuštena su samo u vezi s kaznenim djelima i oporezivanjem (točka 2. Priloga 2. DPA-u iz 2018.), parlamentarnim imunitetom (točka 13. Priloga 2. DPA-u iz 2018.) i obradom u novinarske, akademske, umjetničke i književne svrhe (točka 26. Priloga 2. DPA-u iz 2018.).

([53]) Točka 2. Priloga 2. DPA-u iz 2018.

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

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

pravila o pravnim sredstvima, odgovornostima i sankcijama, osim na odredbu o općim uvjetima za izricanje upravnih novčanih kazni utvrđenima u članku 83. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine i na odredbu o sankcijama iz članka 84. te uredbe. Nadalje, člankom 28. DPA-a iz 2018. izmijenjena je primjena članka 9. stavka 1. kako bi se omogućila obrada posebnih kategorija podataka iz članka 9. stavka 1. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine u mjeri u kojoj se ta obrada provodi za potrebe zaštite nacionalne sigurnosti ili u svrhe obrane te uz odgovarajuće zaštitne mjere za prava i slobode ispitanika ([56]).

(64) Izuzeće se može primijeniti samo u mjeri u kojoj je nužno za zaštitu nacionalne sigurnosti ili obranu. Kao što vrijedi i za ostala izuzeća predviđena DPA-om iz 2018., voditelj obrade mora ga uzeti u obzir i pozivati se na njega na pojedinačnoj osnovi. Nadalje, sve primjene izuzeća moraju biti u skladu sa standardima ljudskih prava (koji se temelje na Zakonu o ljudskim pravima iz 1998.), prema kojima bi u demokratskom društvu svako zadiranje u prava na privatnost trebalo biti nužno i proporcionalno ([57]).

(65) To tumačenje izuzeća potvrđuje ICO, koji je izdao detaljne smjernice o primjeni izuzeća radi nacionalne sigurnosti i obrane, jasno navodeći da ga voditelj obrade mora razmotriti i primjenjivati za svaki slučaj pojedinačno ([58]). Konkretno, u smjernicama se naglašava da „[to] nije opće izuzeće" i da, kako bi se na njega pozivalo, „nije dovoljno da se podaci obrađuju radi nacionalne sigurnosti". S druge strane, voditelj obrade koji se koristi tim izuzećem mora „dokazati da postoji stvarna mogućnost negativnog utjecaja na nacionalnu sigurnost" i od njega se, prema potrebi, očekuje da „[ICO-u] dostavi dokaze o tome zašto je primijenio to izuzeće". Smjernice sadržavaju kontrolni popis i niz primjera kako bi se dodatno pojasnili uvjeti pod kojima se može pozvati na to izuzeće.

(66) Činjenica da se podaci obrađuju u svrhe nacionalne sigurnosti i obrane stoga sama po sebi nije dovoljna za primjenu izuzeća. Voditelj obrade mora uzeti u obzir stvarne posljedice za nacionalnu sigurnost ako bi morao ispuniti određenu odredbu o zaštiti podataka. Izuzeće se može primijeniti samo na specifične odredbe za koje je utvrđeno da predstavljaju rizik i mora se primijeniti što restriktivnije ([59]).

(67) Taj je pristup potvrdio Sud za informacije (*Information Tribunal*) ([60]). U predmetu *Baker protiv Secretary of State for the Home Department* („*Baker protiv Secretary of State*") utvrdio je da je bilo nezakonito primijeniti izuzeće radi nacionalne sigurnosti kao opće izuzeće za pristup zahtjevima koje su primile obavještajne službe. Umjesto toga izuzeće se moralo primjenjivati na pojedinačnoj osnovi, razmatranjem utemeljenosti svakog zahtjeva i s obzirom na pravo pojedinaca na poštovanje njihovih privatnih života ([61]).

([56]) Prema informacijama koje su dostavila tijela Ujedinjene Kraljevine, ako se obrada obavlja u kontekstu nacionalne sigurnosti, voditelji obrade obično će na obradu primjenjivati napredne zaštitne i sigurnosne mjere, koje odražavaju osjetljivu prirodu te obrade. Primjerene zaštitne mjere ovisit će o rizicima koja predmetna obrada predstavlja. To bi moglo uključivati ograničenja pristupa podacima tako da im mogu pristupiti samo ovlaštene osobe s odgovarajućim uvjerenjem o sigurnosnoj provjeri, stroga ograničenja razmjene podataka i visoki sigurnosni standard koji se primjenjuje na pohranu i postupke upravljanja.

([57]) Vidjeti i predmet *Guriev protiv Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), točka 45.; *Lin protiv Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), točka 80.

([58]) Vidjeti smjernice ICO-a o izuzeću radi nacionalne sigurnosti i obrane, dostupne na sljedećoj poveznici: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/

([59]) Prema primjeru koji su navela tijela Ujedinjene Kraljevine, ako bi osoba osumnjičena za terorizam koju MI5 aktivno istražuje uputila zahtjev Ministarstvu unutarnjih poslova (na primjer, zato što je u sporu s Ministarstvom unutarnjih poslova oko pitanja useljenja), od priopćavanja ispitaniku trebalo bi zaštititi sve podatke koje je MI5 možda podijelio s Ministarstvom unutarnjih poslova o istragama koje su u tijeku i koji bi mogli dovesti u pitanje osjetljive izvore, metode ili tehnike i/ili dovesti do povećanja prijetnje koju pojedinac predstavlja. U takvim bi okolnostima vjerojatno bio ispunjen prag za primjenu izuzeća iz članka 26. i izuzeće od otkrivanja informacija bilo bi potrebno za zaštitu nacionalne sigurnosti. Međutim, ako Ministarstvo unutarnjih poslova ima i osobne podatke o pojedincu koji se ne odnose na istragu koju provodi MI5 i te bi se informacije mogle dati bez rizika od ugrožavanja nacionalne sigurnosti, izuzeće radi nacionalne sigurnosti ne bi bilo primjenjivo kad se razmatra otkrivanje informacija pojedincu. Ured povjerenice za informiranje trenutačno radi na smjernicama o načinu na koji bi voditelji obrade trebali pristupati upotrebi izuzeća iz članka 26. Očekuje se da će te smjernice biti objavljene do kraja ožujka 2021.

([60]) Sud za informacije uspostavljen je za saslušanje žalbi u vezi sa zaštitom podataka na temelju Zakona o zaštiti podataka iz 1984. Sud za informacije postao je 2010. dijelom Općeg regulatornog vijeća (*General Regulatory Chamber*) Prvostupanjskog suda (*First Tier Tribunal*) kao dio reforme strukture sustava sudova Ujedinjene Kraljevine.

([61]) Vidjeti predmet *Baker protiv Secretary of State for the Home Department* [2001] UKIT NSA2 („*Baker protiv Secretary of State*").

2.5.6. *Ograničenja za osobne podatke koji se obrađuju u novinarske, umjetničke, akademske i književne svrhe te u svrhe arhiviranja i istraživanja*

(68) Članak 85. stavak 2. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine omogućuje da se predvidi izuzeće osobnih podataka koji se obrađuju u novinarske, umjetničke, akademske i književne svrhe od nekoliko odredbi Opće uredbe o zaštiti podataka Ujedinjene Kraljevine. U dijelu 5. Priloga 2. DPA-u iz 2018. utvrđena su izuzeća za obradu u te svrhe. Predviđaju se izuzeća od načela zaštite podataka (osim načela cjelovitosti i povjerljivosti), pravne osnove za obradu (uključujući posebne kategorije podataka i podatke o kaznenim osudama itd.), uvjeta za privolu, obveza u pogledu transparentnosti, prava ispitanika, obveza obavješćivanja o povredi podataka, zahtjeva za savjetovanje s povjerenikom za informiranje prije visokorizične obrade te pravila o međunarodnim prijenosima ([62]). U tom smislu Opća uredba o zaštiti podataka Ujedinjene Kraljevine ne odstupa bitno od Uredbe (EU) 2016/679, u čijem se članku 85. isto predviđa mogućnost izuzeća obrade koja se obavlja u novinarske svrhe ili svrhe akademskog, umjetničkog ili književnog izražavanja od nekoliko zahtjeva Uredbe (EU) 2016/679. Odredbe DPA-a iz 2018., osobito dio 5. Priloga 2., u skladu su s Općom uredbom o zaštiti podataka Ujedinjene Kraljevine.

(69) Osnovno uravnoteživanje koje je potrebno na temelju članka 85. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine odnosi se na to jesu li izuzeća od pravilâ o zaštiti podataka navedena u uvodnoj izjavi 68. „potrebna kako bi se uskladilo pravo na zaštitu osobnih podataka sa slobodom izražavanja i informiranja” ([63]). Prema točki 26. podtočkama 2. i 3. Priloga 2. DPA-u iz 2018. Ujedinjena Kraljevina primjenjuje test „opravdanog uvjerenja” kako bi uspostavila tu ravnotežu. Da bi izuzeće bilo opravdano, voditelj obrade mora opravdano vjerovati i. da je objava od javnog interesa; i ii. da primjena relevantne odredbe Opće uredbe o zaštiti podataka ne bi bila u skladu s novinarskim, akademskim, umjetničkim ili književnim svrhama. Kako je potvrđeno sudskom praksom ([64]), test „opravdanog uvjerenja” ima i subjektivnu i objektivnu sastavnicu: nije dovoljno da voditelj obrade dokaže da je sâm smatrao da poštovanje pravila nije usklađeno. Njegovo uvjerenje mora biti opravdano, tj. razumna osoba može vjerovati u njega ako poznaje relevantne činjenice. Voditelj obrade stoga mora postupati s dužnom pažnjom pri oblikovanju svojeg uvjerenja kako bi mogao dokazati opravdanost. Prema pojašnjenjima koja su dostavila tijela Ujedinjene Kraljevine test „opravdanog uvjerenja” mora se provoditi za svako pojedinačno izuzeće ([65]). Ako su uvjeti ispunjeni, izuzeće se smatra nužnim i proporcionalnim na temelju prava Ujedinjene Kraljevine.

(70) Prema članku 124. DPA-a iz 2018. Ured povjerenika za informiranje treba izraditi Kodeks dobre prakse o zaštiti podataka i novinarstvu. U tijeku je izrada tog kodeksa. Objavljene su smjernice o tom pitanju na temelju Zakona o zaštiti podataka iz 1998., u kojima se osobito naglašava da, kako bi se moglo pozvati na to izuzeće, nije dovoljno samo navesti da bi usklađenost stvarala poteškoće za novinarske aktivnosti, već mora

([62]) Vidjeti članak 85. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine i dio 5. točku 26. podtočku 9. Priloga 2. DPA-u iz 2018.

([63]) U skladu s dijelom 5. točkom 26. podtočkom 2. Priloga 2. DPA-u iz 2018. izuzeće se primjenjuje na obradu osobnih podataka koja se provodi u posebne svrhe (novinarske, akademske, umjetničke i književne svrhe) ako se obrada provodi kako bi osoba objavila novinarski, akademski, umjetnički ili književni materijal te voditelj obrade opravdano vjeruje da bi objava tog materijala bila od javnog interesa. Kad određuje je li objava od javnog interesa, voditelj obrade mora uzeti u obzir posebnu važnost javnog interesa u slobodi izražavanja i informiranja. Osim toga, voditelj obrade mora uzeti u obzir kodekse dobre prakse ili smjernice relevantne za predmetnu objavu (Uredničke smjernice BBC-a, Kodeks Ofcoma za emitiranje i Urednički kodeks dobre prakse). Nadalje, kako bi se primijenilo izuzeće, voditelj obrade mora opravdano vjerovati da poštovanje relevantne odredbe ne bi bilo u skladu s posebnim svrhama (točka 26. podtočka 3. Priloga 2. DPA-u iz 2018.).

([64]) U točki 102. presude u predmetu *NT1* protiv *Google* [2018] EWHC 799 (QB) govori se o raspravi o tome je li voditelj obrade podataka bio opravdano uvjeren da je objava u javnom interesu i da poštovanje relevantnih odredbi nije u skladu s posebnim svrhama. Sud je naveo da članak 32. stavak 1. točke (b) i (c) Zakona o zaštiti podataka iz 1998. imaju subjektivan i objektivan element: voditelj obrade podataka mora utvrditi da je vjerovao da bi objava bila u javnom interesu i da je to uvjerenje bilo objektivno opravdano; mora utvrditi subjektivno uvjerenje o tome da poštovanje odredbe od koje traži izuzeće ne bi bilo u skladu s predmetnom posebnom svrhom.

([65]) Primjer načina primjene testa „opravdanog uvjerenja” nalazi se u odluci Ureda povjerenika za informiranje da kazni društvo *True Visions Productions*, koja je donesena na temelju Zakona o zaštiti podataka iz 1998. Ured povjerenika za informiranje prihvatio je da je medijski voditelj obrade subjektivno vjerovao da poštovanje prvog načela zaštite podataka (poštenost i zakonitost) nije bilo u skladu s novinarskim svrhama. Međutim, Ured nije prihvatio da je to uvjerenje bilo objektivno opravdano. Odluka Ureda povjerenika za informiranje dostupna je na: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf.

postojati jasan argument da je predmetna odredba prepreka odgovornom novinarstvu ([66]). Smjernice o primjeni testa javnog interesa i uravnoteženju javnog interesa i interesa pojedinca za privatnost objavili su regulator Ujedinjene Kraljevine za telekomunikacije OFCOM i BBC u svojim uredničkim smjernicama ([67]). U smjernicama se osobito navode primjeri informacija za koje se može smatrati da su od javnog interesa i objašnjava se da je potrebno moći dokazati da javni interes u određenim okolnostima slučaja nadilazi prava na privatnost.

(71) Slično odredbama predviđenima u članku 89. Opće uredbe o zaštiti podataka, i osobni podaci koji se obrađuju u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe mogu se izuzeti od nekoliko navedenih odredbi Opće uredbe o zaštiti podataka Ujedinjene Kraljevine ([68]). Kad je riječ o istraživanjima i statističkim podacima, moguća su izuzeća od odredbi Opće uredbe o zaštiti podataka Ujedinjene Kraljevine koje se odnose na potvrdu obrade te pristup podacima i zaštitne mjere za prijenose trećim zemljama, pravo na ispravak, ograničavanje obrade i prigovor na obradu. Kad je riječ o arhiviranju u javnom interesu, moguća su i izuzeća od obveze obavješćivanja u vezi s ispravkom ili brisanjem osobnih podataka ili ograničavanjem obrade te od prava na prenosivost podataka.

(72) Prema točki 27. podtočki 1. i točki 28. podtočki 1. Priloga 2. DPA-u iz 2018. izuzeća od navedenih odredbi Opće uredbe o zaštiti podataka Ujedinjene Kraljevine moguća su ako bi njihova primjena „spriječila ili ozbiljno ugrozila postizanje" predmetnih svrha ([69]).

(73) S obzirom na njihovu važnost za učinkovito ostvarivanje prava pojedinaca, u kontekstu kontinuiranog praćenja ove Odluke propisno će se uzeti u obzir sve relevantne promjene u pogledu tumačenja i praktične primjene prethodno navedenih izuzeća (uz izuzeće koje se odnosi na provedbu učinkovite kontrole useljavanja, kako je objašnjeno u uvodnoj izjavi 6.), uključujući sve daljnje promjene sudske prakse te smjernica ICO-a i mjera izvršenja ([70]).

2.5.7. *Ograničenja daljnjih prijenosa*

(74) Razina zaštite osobnih podataka koji se prenose iz Europske unije voditeljima obrade ili izvršiteljima obrade u Ujedinjenoj Kraljevini ne smije se ugroziti daljnjim prijenosom takvih podataka primateljima u trećoj zemlji. Takvi „daljnji prijenosi", koji su iz perspektive voditelja obrade ili izvršitelja obrade iz Ujedinjene Kraljevine međunarodni prijenosi iz Ujedinjene Kraljevine, trebali bi biti dopušteni samo ako daljnji primatelj izvan Ujedinjene Kraljevine i sam podliježe pravilima koja osiguravaju razinu zaštite sličnu onoj koja se jamči pravnim poretkom Ujedinjene Kraljevine. Zbog toga je primjena pravila iz Opće uredbe o zaštiti podataka Ujedinjene Kraljevine i DPA-a iz 2018. na međunarodne prijenose osobnih podataka važan čimbenik za osiguravanje kontinuiteta zaštite u slučaju osobnih podataka koji se prenose iz Europske unije u Ujedinjenu Kraljevinu na temelju ove Odluke.

([66]) Prema tim smjernicama organizacije moraju moći objasniti zašto poštovanje relevantne odredbe Zakona o zaštiti podataka iz 1998. nije u skladu sa svrhama novinarstva. Voditelji obrade osobito moraju uspostaviti ravnotežu između štetnog učinka koji bi usklađenost imala na novinarstvo sa štetnim učinkom koji bi neusklađenost imala na prava ispitanika. Ako novinar opravdano može ostvariti svoje uredničke ciljeve na način koji je usklađen sa standardnim odredbama DPA-a, dužan je to učiniti. Organizacije moraju moći opravdati upotrebu ograničenja za svaku odredbu koju nisu poštovale. *Data protection and journalism: a guide for the media* (Zaštita osobnih podataka i novinarstvo: vodič za medije), dostupno na: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf.

([67]) Primjeri javnog interesa uključuju otkrivanje ili istraživanje kaznenih djela, zaštitu javnog zdravlja ili sigurnosti, razotkrivanje zavaravajućih tvrdnji pojedinaca ili organizacija ili otkrivanje nesposobnosti koja utječe na javnost. Vidjeti smjernice OFCOM-a dostupne na: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf i uredničke smjernice BBC-a dostupne na: https://www.bbc.com/editorialguidelines/guidelines/privacy.

([68]) Vidjeti članak 89. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine i dio 6. točku 27. podtočku 2. i točku 28. podtočku 2. Priloga 2. DPA-u iz 2018.

([69]) Na to se primjenjuje zahtjev da se osobni podaci obrađuju u skladu s člankom 89. stavkom 1. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine kako je dopunjen člankom 19. DPA-a iz 2018.

([70]) Vidjeti uvodne izjave od 281. do 287.

(75) Sustav međunarodnih prijenosa osobnih podataka iz Ujedinjene Kraljevine utvrđen je u člancima od 44. do 49. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine i dopunjen je DPA-om iz 2018., a u bitnom je identičan pravilima iz poglavlja V. Uredbe (EU) 2016/679 ([71]). Prijenosi osobnih podataka trećoj zemlji ili međunarodnoj organizaciji mogući su samo na temelju uredbe o primjerenosti (britanski ekvivalent odluke o primjerenosti iz Uredbe (EU) 2016/679) ili, ako uredba o primjerenost i ne postoji, ako voditelj obrade ili izvršitelj obrade osigura odgovarajuće zaštitne mjere u skladu s člankom 46. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine. Ako ne postoji uredba o primjerenosti ili odgovarajuće zaštitne mjere, prijenos je moguć samo na temelju odstupanja utvrđenih u članku 49. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine.

(76) U uredbama o primjerenosti koje donosi ministar može se odrediti da treća zemlja (ili područje ili sektor unutar treće zemlje), međunarodna organizacija ili opis ([72]) takve zemlje, područja, sektora ili organizacije osigurava primjerenu razinu zaštite osobnih podataka. Kad ocjenjuje primjerenost razine zaštite, ministar mora uzeti u obzir potpuno iste elemente koje Komisija mora procijeniti na temelju članka 45. stavka 2. točaka od (a) do (c) Uredbe (EU) 2016/679, koje se tumače zajedno s uvodnom izjavom 104. te uredbe i zadržanom sudskom praksom EU-a. To znači da će pri procjeni primjerene razine zaštite treće zemlje relevantni standard biti osigurava li predmetna treća zemlja razinu zaštite koja je „u načelu istovjetna" onoj koja se jamči u Ujedinjenoj Kraljevini.

(77) Na uredbe o primjerenosti primjenjuju se „opći" postupovni zahtjevi predviđeni u članku 182. DPA-a iz 2018. U okviru tog postupka ministar se mora savjetovati s povjerenikom za informiranje kad predlaže donošenje uredbe o primjerenosti Ujedinjene Kraljevine ([73]). Nakon što je ministar donese, ta se uredba upućuje Parlamentu i podliježe postupku „negativnog vijećanja" (*negative resolution procedure*), u okviru kojeg oba doma Parlamenta mogu preispitati uredbu i izglasati prijedlog o ukidanju uredbe u roku od 40 dana ([74]).

(78) Prema članku 17.B stavku 1. DPA-a iz 2018. uredbe o primjerenosti moraju se preispitivati u razmacima koji nisu dulji od četiri godine, a ministar mora kontinuirano pratiti promjene u trećim zemljama i međunarodnim organizacijama koje bi mogle utjecati na odluke o donošenju uredbi o primjerenosti ili na izmjenu ili ukidanje takvih uredbi. Ako ministar utvrdi da određena zemlja ili organizacija više ne osigurava primjerenu razinu zaštite osobnih podataka, mora, u mjeri u kojoj je to potrebno, izmijeniti ili ukinuti uredbu i pokrenuti savjetovanje s predmetnom trećom zemljom ili međunarodnom organizacijom kako bi riješili problem nedostatka primjerene razine zaštite. Ti postupovni aspekti odražavaju i odgovarajuće zahtjeve iz Uredbe (EU) 2016/679.

([71]) Uz iznimku članka 48. Uredbe (EU) 2016/679 za koji je Ujedinjena Kraljevina odlučila da ga neće uključiti u Opću uredbu o zaštiti podataka Ujedinjene Kraljevine. U tom smislu najprije treba podsjetiti da je standard za koji se smatra da pruža odgovarajuću razinu zaštite standard „načelne istovjetnosti", a ne identičnosti, kako je pojasnio Sud EU-a (*Schrems I*, točke 73. i 74.) i priznao Europski odbor za zaštitu podataka (EDPB) (Referentni dokument o primjerenosti, str. 3.). Stoga, kako je objasnio EDPB u Referentnom dokumentu o primjerenosti, „cilj nije da se europsko zakonodavstvo odražava točku po točku, nego da se uspostave bitni, odnosno temeljni zahtjevi tog zakonodavstva". U tom je smislu važno napomenuti da, iako pravni poredak Ujedinjene Kraljevine formalno ne sadržava odredbu istovjetnu članku 48., isti je učinak zajamčen drugim pravnim odredbama i načelima, odnosno da se kao odgovor na zahtjev suda ili upravnog tijela treće zemlje za pristup osobnim podacima ti podaci mogu prenijeti u tu treću zemlju samo ako postoji međunarodni sporazum na temelju kojeg se predmetna sudska presuda ili upravna odluka treće zemlje priznaje ili izvršava u Ujedinjenoj Kraljevini ili ako se taj postupak temelji na jednom od mehanizama prijenosa predviđenih u poglavlju V. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine. Konkretnije, da bi se izvršila strana presuda, sudovi u Ujedinjenoj Kraljevini moraju se moći pozvati na precedentno pravo ili zakon koji dopušta njezinu izvršivost. Međutim, ni precedentno pravo (vidjeti *Adams i drugi protiv Cape Industries Plc.*, [1990] 2 W.L.R. 657) ni zakoni ne predviđaju izvršenje stranih presuda kojima se zahtijeva prijenos podataka ako na snazi nije međunarodni sporazum. Slijedom toga, na temelju prava Ujedinjene Kraljevine zahtjevi za pristup podacima nisu provedivi bez takvog međunarodnog sporazuma. Nadalje, svaki prijenos osobnih podataka trećim zemljama, uključujući prijenos na zahtjev stranog suda ili upravnog tijela, i dalje podliježe ograničenjima iz poglavlja V. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine koja su identična odgovarajućim odredbama Uredbe (EU) 2016/679 te se stoga zahtijeva da se temelji na jednom od razloga za prijenos dostupnih na temelju poglavlja V. u skladu s posebnim uvjetima kojima podliježe na temelju tog poglavlja.

([72]) Tijela Ujedinjene Kraljevine objasnila su da se opis zemlje ili međunarodne organizacije odnosi na situaciju u kojoj bi bilo nužno provesti posebno i djelomično utvrđivanje primjerenosti s usmjerenim ograničenjima (na primjer, uredbe o primjerenosti koje se odnose samo na određene vrste prijenosa podataka).

([73]) Vidjeti Memorandum o razumijevanju između ministra za digitalizaciju, kulturu, medije i sport i Ureda povjerenika za informiranje o ulozi ICO-a u vezi s novom procjenom primjerenosti Ujedinjene Kraljevine, dostupan na: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([74]) Ako se to izglasa, uredba će naposljetku prestati imati daljnji pravni učinak.

(79) Ako ne postoje uredbe o primjerenosti, međunarodni prijenosi mogući su ako voditelj obrade ili izvršitelj obrade osigura odgovarajuće zaštitne mjere u skladu s člankom 46. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine. Te zaštitne mjere slične su onima iz članka 46. Uredbe (EU) 2016/679. Uključuju pravno obvezujuće i provedive instrumente između tijela javne vlasti ili javnih tijela, obvezujuća korporativna pravila ([75]), standardne klauzule o zaštiti podataka, odobrene kodekse ponašanja, odobrene mehanizme certificiranja i, uz odobrenje povjerenika za informiranje, ugovorne klauzule između voditelja obrade (ili izvršitelja obrade) ili administrativne dogovore između tijela javne vlasti. Međutim, pravila su izmijenjena u smislu postupka kako bi funkcionirala unutar okvira Ujedinjene Kraljevine, točnije, standardne klauzule o zaštiti podataka može donositi ministar (članak 17.C) ili povjerenik za informiranje (članak 119.A) u skladu s DPA-om iz 2018.

(80) Ako ne postoji odluka o primjerenosti ili odgovarajuće zaštitne mjere, prijenos je moguć samo na temelju odstupanja utvrđenih u članku 49. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine ([76]). Općom uredbom o zaštiti podataka Ujedinjene Kraljevine nisu uvedene nikakve bitne izmjene tih odstupanja u usporedbi s odgovarajućim pravilima iz Uredbe (EU) 2016/679. Na temelju Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, kao i na temelju Uredbe (EU) 2016/679, na određena odstupanja može se pozvati samo ako je prijenos povremen ([77]). Nadalje, Ured povjerenika za informiranje u svojim smjernicama o međunarodnim prijenosima pojašnjava: „Trebali biste ih koristiti samo kao prava ‚izuzeća' od općeg pravila prema kojem ne biste trebali provoditi ograničeni prijenos osim ako je obuhvaćen odlukom o primjerenosti ili su uspostavljene odgovarajuće zaštitne mjere" ([78]). Kad je riječ o prijenosima koji su nužni iz važnih razloga javnog interesa (članak 49. stavak 1. točka (d)), ministar može donijeti uredbe kojima će odrediti okolnosti u kojima prijenos osobnih podataka trećoj zemlji ili međunarodnoj organizaciji nije nužan iz važnih razloga javnog interesa. Nadalje, ministar uredbama može ograničiti prijenos kategorije osobnih podataka trećoj zemlji ili međunarodnoj organizaciji ako prijenos nije moguć na temelju uredbe o primjerenosti, a ministar smatra da je ograničenje nužno iz važnih razloga javnog interesa. Zasad nisu donesene takve uredbe.

(81) Taj okvir za međunarodne prijenose postao je primjenjiv na kraju prijelaznog razdoblja ([79]). Međutim, u točki 4. Priloga 21. DPA-u iz 2018. (uvedenoj Uredbom DPPEC) predviđa se da se na kraju prijelaznog razdoblja s određenim prijenosima osobnih podataka postupa kao da se temelje na uredbi o primjerenosti. Ti prijenosi uključuju prijenose državi EGP-a, teritoriju Gibraltara, instituciji, tijelu, uredu ili agenciji Unije uspostavljenoj Ugovorom o Europskoj uniji ili na temelju njega te trećim zemljama na koje se na kraju prijelaznog razdoblja primjenjivala odluka o primjerenosti EU-a. Stoga se prijenosi u te zemlje mogu nastaviti kao i prije povlačenja Ujedinjene Kraljevine iz EU-a. Nakon kraja prijelaznog razdoblja ministar mora preispitati te nalaze o

([75]) Opća uredba o zaštiti podataka Ujedinjene Kraljevine zadržava pravila iz članka 47. Uredbe (EU) 2016/679 i izvršene su samo izmjene potrebne da bi se pravila uklopila u domaći kontekst, na primjer zamjena upućivanja na nadležno nadzorno tijelo upućivanjem na povjerenika za informiranje, brisanje upućivanja na mehanizam konzistentnosti iz stavka 1. i brisanje cijelog stavka 3.

([76]) Na temelju članka 49. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine prijenosi su mogući ako je ispunjen jedan od sljedećih uvjeta: (a) ispitanik je izričito pristao na predloženi prijenos nakon što je bio obaviješten o mogućim rizicima takvih prijenosa za ispitanika zbog nepostojanja odluke o primjerenosti i odgovarajućih zaštitnih mjera; (b) prijenos je nužan za izvršavanje ugovora između ispitanika i voditelja obrade ili provedbu predugovornih mjera na zahtjev ispitanika; (c) prijenos je nužan radi sklapanja ili izvršavanja ugovora sklopljenog u interesu ispitanika između voditelja obrade i druge fizičke ili pravne osobe; (d) prijenos je nužan iz važnih razloga javnog interesa; (e) prijenos je nužan za postavljanje, ostvarivanje ili obranu pravnih zahtjeva; (f) prijenos je nužan za zaštitu životno važnih interesa ispitanika ili drugih osoba ako ispitanik fizički ili pravno ne može dati privolu; (g) prijenos se obavlja iz registra koji prema nacionalnom pravu služi pružanju informacija javnosti i koji je otvoren na uvid javnosti ili bilo kojoj osobi koja može dokazati neki opravdani interes, ali samo u mjeri u kojoj su ispunjeni uvjeti propisani u nacionalnom pravu za uvid u tom posebnom slučaju. Nadalje, ako nije primjenjiv nijedan prethodno navedeni uvjet, prijenos se može ostvariti samo ako se ne ponavlja, ako se odnosi samo na ograničen broj ispitanika, ako je nužan za potrebe uvjerljivih, legitimnih interesa voditelja obrade koji nisu podređeni interesima ili pravima i slobodama ispitanika, a voditelj obrade procijenio je sve okolnosti prijenosa podataka te je na temelju te procjene predvidio odgovarajuće zaštitne mjere u pogledu zaštite osobnih podataka.

([77]) U uvodnoj izjavi 111. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine određeno je da su prijenosi povezani s ugovorima ili pravnim zahtjevima mogući samo ako se odvijaju povremeno.

([78]) Smjernice Ureda povjerenika za informiranje o međunarodnim prijenosima, dostupne na: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7.

([79]) U razdoblju od najviše šest mjeseci koje završava najkasnije 30. lipnja 2021. primjenjivost tog novog okvira mora se tumačiti s obzirom na članak 782. Sporazuma o trgovini i suradnji između Europske unije i Europske zajednice za atomsku energiju, s jedne strane, i Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske, s druge strane (L 444/14 od 31.12.2020.) („Sporazum o trgovini i suradnji između EU-a i Ujedinjene Kraljevine"), dostupan na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:22020A1231(01)&from=HR.

primjerenosti u roku od četiri godine, tj. do kraja prosinca 2024. Prema objašnjenju koje su dala tijela Ujedinjene Kraljevine, iako ministar treba provesti to preispitivanje do kraja prosinca 2024., prijelazne odredbe ne sadržavaju odredbu o vremenskom ograničenju valjanosti, pa relevantne prijelazne odredbe neće automatski prestati imati učinak ako se preispitivanje ne dovrši do kraja prosinca 2024.

(82) Naposljetku, kad je riječ o budućem razvoju sustava međunarodnih prijenosa Ujedinjene Kraljevine – donošenjem novih uredaba o primjerenosti, sklapanjem međunarodnih sporazuma ili razvojem drugih mehanizama prijenosa – Komisija će pomno pratiti situaciju, procijeniti upotrebljavaju li se različiti mehanizmi prijenosa na način kojim se osigurava kontinuitet zaštite i, prema potrebi, poduzeti odgovarajuće mjere za uklanjanje mogućih negativnih učinaka na takav kontinuitet (vidjeti uvodne izjave od 278. do 287.). Budući da EU i Ujedinjena Kraljevina imaju slična pravila o međunarodnim prijenosima, očekuje se da bi se problematična odstupanja mogla izbjeći i suradnjom te razmjenom informacija i iskustava, među ostalim između ICO-a i EDPB-a.

2.5.8. *Odgovornost*

(83) Na temelju načela odgovornosti subjekti koji obrađuju podatke moraju uspostaviti odgovarajuće tehničke i organizacijske mjere kako bi djelotvorno ispunili svoje obveze u pogledu zaštite podataka te mogli dokazati da su ispunjene, prije svega nadležnom nadzornom tijelu.

(84) Načelo odgovornosti predviđeno Uredbom (EU) 2016/679 zadržano je u članku 5. stavku 2. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine bez bitnih izmjena, a isto vrijedi i za članak 24. o obvezama voditelja obrade, članak 25. o tehničkoj i integriranoj zaštiti podataka i članak 30. o evidenciji aktivnosti obrade. Zadržani su i članci 35. i 36. o procjeni učinka na zaštitu podataka i prethodnom savjetovanju s nadzornim tijelom. Članci od 37. od 39. Uredbe (EU) 2016/679 o imenovanju i zadaćama službenika za zaštitu podataka zadržani su u Općoj uredbi o zaštiti podataka Ujedinjene Kraljevine bez bitnih izmjena. Nadalje, odredbe članaka 40. i 42. Uredbe (EU) 2016/679 o kodeksima ponašanja i certificiranju zadržane su u Općoj uredbi o zaštiti podataka Ujedinjene Kraljevine ([80]).

2.6. **Nadzor i provedba**

2.6.1. *Neovisni nadzor*

(85) Kako bi se u praksi osigurala primjerena razina zaštite podataka, trebalo bi uspostaviti neovisno nadzorno tijelo s ovlastima za praćenje i provedbu usklađenosti s pravilima o zaštiti podataka. Ono bi pri obavljanju dužnosti i izvršavanju ovlasti trebalo djelovati potpuno neovisno i nepristrano.

(86) U Ujedinjenoj Kraljevini nadzor i provedbu usklađenosti s Općom uredbom o zaštiti podataka Ujedinjene Kraljevine i DPA-om iz 2018. obavlja povjerenik za informiranje. Povjerenik za informiranje je tijelo pojedinac (*corporation sole*): zaseban pravni subjekt koji se sastoji od jedne osobe. Povjerenika za informiranje u radu podupire ured. Ured povjerenice za informiranje (ICO) 31. ožujka 2020. imao je 768 članova stalnog osoblja ([81]). Povjerenika za informiranje sponzorira Ministarstvo za digitalizaciju, kulturu, medije i sport ([82]).

(87) Neovisnost povjerenika izričito je utvrđena u članku 52. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, u kojem nema bitnih izmjena članka 52. stavaka od 1. do 3. Opće uredbe o zaštiti podataka. Povjerenik mora djelovati potpuno neovisno pri obavljanju dužnosti i izvršavanju ovlasti u skladu s Općom uredbom o zaštiti

([80]) Upućivanja su prema potrebi zamijenjena upućivanjima na tijela Ujedinjene Kraljevine. Na primjer, na temelju članka 17. DPA-a iz 2018. povjerenik za informiranje ili nacionalno akreditacijsko tijelo Ujedinjene Kraljevine mogu akreditirati osobu koja ispunjava zahtjeve utvrđene u članku 43. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine za praćenje usklađenosti s certifikatom.

([81]) Godišnje izvješće i financijski izvještaji povjerenice za informiranje za 2019.–2020., dostupno na: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

([82]) Njihov je odnos uređen sporazumom o upravljanju. Točnije, glavne odgovornosti Ministarstva za digitalizaciju, kulturu, medije i sport kao ministarstva sponzora uključuju: osiguravanje da povjerenik za informiranje raspolaže primjerenim financiranjem i resursima, zastupanje interesa povjerenika za informiranje pred Parlamentom i drugim Vladinim odjelima, osiguravanje da je uspostavljen stabilan nacionalni okvir za zaštitu podataka te davanje smjernica i potpore Uredu povjerenika za informiranje u korporativnim pitanjima kao što su pitanja povezana s imovinom, ugovori o zakupu i javna nabava (Sporazum o upravljanju za 2018.–2021., dostupan na: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

podataka Ujedinjene Kraljevine, mora biti slobodan od vanjskog utjecaja (izravnog ili neizravnog) te ne smije tražiti ni primati upute ni od koga. Povjerenik se mora suzdržati i od svih radnji koje nisu u skladu s njegovim dužnostima i za vrijeme mandata ne smije se baviti nikakvom neusklađenom djelatnošću, bez obzira na to je li plaćena.

(88) Uvjeti za imenovanje i razrješenje povjerenika za informiranje utvrđeni su u Prilogu 12. DPA-u iz 2018. Povjerenika za informiranje imenuje Njezino Veličanstvo na preporuku vlade na temelju poštenog i otvorenog natječaja. Kandidat mora imati odgovarajuće kvalifikacije, vještine i kompetencije. U skladu s Kodeksom upravljanja za imenovanje javnih službenika (*Governance Code on Public Appointments*) ([83]) savjetodavni odbor za procjenu sastavlja popis kandidata koji se mogu imenovati. Prije nego što ministar za digitalizaciju, kulturu, medije i sport donese konačnu odluku, odgovarajući posebni odbor Parlamenta mora provesti preispitivanje prije imenovanja. Stajalište odbora javno se objavljuje ([84]).

(89) Mandat povjerenika za informiranje traje do sedam godina. Osobu se ne može imenovati povjerenikom za informiranje više od jednom. Njezino Veličanstvo povjerenika za informiranje može razriješiti dužnosti na molbu obaju domova Parlamenta ([85]). Zahtjev za razrješenje povjerenika za informiranje ne može se podnijeti nijednom domu Parlamenta ako ministar ne dostavi izvješće u kojem navodi da je uvjeren da je povjerenik za informiranje teško povrijedio dužnosti i/ili da povjerenik više ne ispunjava uvjete koji se zahtijevaju za izvršavanje funkcija povjerenika ([86]).

(90) Tri su izvora financiranja povjerenika za informiranje: i. naknade za zaštitu podataka koje plaćaju voditelji obrade, koje se određuju uredbom ministra ([87]) (Uredba o zaštiti podataka (naknade i informacije) iz 2018.) i čine 85–90 % godišnjeg proračuna Ureda ([88]), ii. subvencija koju Vlada plaća povjereniku za informiranje; subvencija se uglavnom koristi za financiranje troškova poslovanja povjerenika za informiranje u pogledu zadaća koje nisu povezane sa zaštitom podataka ([89]) i iii. naknada koje se naplaćuju za usluge ([90]). Trenutačno se ne naplaćuju takve naknade.

(91) Opće funkcije povjerenika za informiranje u pogledu obrade osobnih podataka na koje se primjenjuje Opća uredba o zaštiti podataka Ujedinjene Kraljevine utvrđene su u članku 57. te uredbe i u velikoj mjeri odražavaju odgovarajuća pravila iz Uredbe (EU) 2016/679. Njegove funkcije uključuju praćenje i provedbu Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, promicanje javne svijesti, rješavanje pritužbi koje podnesu ispitanici, provođenje istraga itd. Osim toga, u članku 115. DPA-a iz 2018. utvrđene su opće funkcije povjerenika, koje uključuju dužnost savjetovanja Parlamenta, vlade i drugih institucija i tijela o zakonodavnim i upravnim mjerama koje se odnose na zaštitu prava i sloboda pojedinaca s obzirom na obradu osobnih podataka te ovlast da na vlastitu inicijativu ili na zahtjev daje mišljenja Parlamentu, vladi ili drugim institucijama i tijelima te javnosti o svim pitanjima povezanima

([83]) Kodeks upravljanja za imenovanje javnih službenika, dostupan na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf.

([84]) Drugo izvješće zasjedanja Odbora za kulturu, medije i sport Zastupničkog doma u razdoblju 2015.–2016., dostupno na: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([85]) „Molba" (*address*) je prijedlog upućen Parlamentu čija je svrha obavijestiti vladara o mišljenju Parlamenta o određenom pitanju.

([86]) Točka 3. podtočka 3. Priloga 12. DPA-u iz 2018.

([87]) Članak 137. DPA-a iz 2018., vidjeti uvodnu izjavu 17.

([88]) Članci 137. i 138. DPA-a iz 2018. sadržavaju niz zaštitnih mjera kako bi se osigurala primjerena visina tih naknada. Konkretnije, u članku 137. stavku 4. navode se pitanja koja ministar mora uzeti u obzir pri donošenju uredbi kojima se određuje iznos koji različite organizacije moraju plaćati. Drugo, u članku 138. stavku 1. i članku 182. DPA-a iz 2018. zahtijeva se i da se ministar prije donošenja uredbi savjetuje s povjerenikom za informiranje i drugim predstavnicima osoba na koje će te uredbe vjerojatno utjecati kako bi mogao uzeti u obzir njihova mišljenja. Osim toga, na temelju članka 138. stavka 2. DPA-a iz 2018. povjerenik za informiranje dužan je preispitivati funkcioniranje uredbi o naknadama i može ministru podnositi prijedloge izmjena tih uredbi. Naposljetku, uredbe podliježu postupku „pozitivnog vijećanja" (*affirmative resolution procedure*) i ne mogu se donijeti dok ih rezolucijom ne potvrde oba doma Parlamenta, osim ako se uredbe donose samo kako bi se u obzir uzelo povećanje indeksa maloprodajnih cijena (u tom će se slučaju na njih primjenjivati postupak „negativnog vijećanja" (*negative resolution procedure*)).

([89]) U Sporazumu o upravljanju pojašnjeno je da „ministar na temelju točke 9. Priloga 12. DPA-u iz 2018. može izvršavati plaćanja povjereniku za informiranje iz novca koji je osigurao Parlament. Nakon savjetovanja s povjerenikom za informiranje Ministarstvo za digitalizaciju, kulturu, medije i sport isplatit će povjereniku odgovarajuće iznose (subvencija) za administrativne troškove Ureda povjerenika za informiranje i izvršavanje funkcija povjerenika povezanih s nizom posebnih funkcija, uključujući slobodu informiranja" (Sporazum o upravljanju za 2018.–2021., točka 1.12., vidjeti bilješku 82.).

([90]) Vidjeti članak 134. DPA-a iz 2018.

sa zaštitom osobnih podataka. Kako bi se sačuvala neovisnost pravosuđa, povjerenik za informiranje nije ovlašten izvršavati svoje funkcije u vezi s obradom osobnih podataka koju provodi pojedinac koji djeluje u sudbenom svojstvu ili sud u okviru svoje sudske nadležnosti. Međutim, nadzor nad sudstvom osiguravaju specijalizirana tijela (vidjeti uvodne izjave od 99. do 103.).

2.6.2. *Izvršenje, uključujući sankcije*

(92) Ovlasti povjerenika za informiranje utvrđene su u članku 58. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, kojim nisu uvedene bitne izmjene odgovarajućeg članka Uredbe (EU) 2016/679. U DPA-u iz 2018. utvrđena su dodatna pravila o načinu izvršavanja tih ovlasti. Točnije, povjerenik je ovlašten: (a) izdavanjem zahtjeva za dostavu informacija naložiti voditelju obrade i izvršitelju obrade (a u određenim okolnostima i bilo kojoj drugoj osobi) da dostave potrebne informacije („zahtjev za dostavu informacija") ([91]), (b) provoditi istrage i revizije izdavanjem zahtjeva za provjeru, kojim se od voditelja obrade ili izvršitelja obrade može zahtijevati da povjereniku dopusti ulazak u određene prostorije, obavljanje inspekcije ili pregleda dokumenata ili opreme, obavljanje razgovora s osobama koje obrađuju osobne podatke u ime voditelja obrade itd. („zahtjev za provjeru") ([92]), (c) na drugi način dobiti pristup dokumentima itd. voditelja obrade i izvršitelja obrade i pristup njihovim prostorijama u skladu s člankom 154. DPA-a iz 2018. („ovlasti ulaska i inspekcije"), (d) izvršavati korektivne ovlasti, među ostalim, izdavanjem upozorenja i opomena, ili davati naloge u obliku zahtjeva za izvršenje, kojim se od voditelja obrade/izvršitelja obrade zahtijeva da poduzmu određene mjere ili da se suzdrže od njihova poduzimanja, uključujući nalaganje voditelju obrade ili izvršitelju obrade da učini sve što je navedeno u članku 58. stavku 2. točkama od (c) do (g) i točki (j) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine („zahtjev za izvršenje") ([93]), (e) izricati upravne novčane kazne u obliku rješenja o kazni („rješenje o kazni") ([94]). Potonje se mogu izreći i ako tijelo javne vlasti ne poštuje odredbe Opće uredbe o zaštiti podataka Ujedinjene Kraljevine ([95]).

(93) U okviru politike regulatornog djelovanja ICO-a utvrđuju se okolnosti u kojima će on izdavati zahtjev za dostavu informacija, zahtjev za provjeru, zahtjev za izvršenje ili rješenje o kazni ([96]). Zahtjevom za izvršenje koji se daje kao odgovor na propust voditelja obrade ili izvršitelja obrade mogu se uvesti samo zahtjevi koje povjerenik smatra primjerenima za potrebe ispravljanja propusta. Zahtjev za izvršenje i rješenje o kazni mogu se izdati voditelju obrade ili izvršitelju obrade s obzirom na povrede iz poglavlja II. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine (načela obrade) i članaka od 12. do 22. (prava ispitanika), članaka od 25. do 39. (obveze voditelja obrade i izvršitelja obrade) i članaka od 44. do 49. (međunarodni prijenosi) te uredbe. Zahtjev za izvršenje može se izdati i ako voditelj obrade nije ispunio zahtjev za plaćanje naknade iz uredbe donesene na temelju članka 137. DPA-a iz 2018. Osim toga, zahtjev za izvršenje može se izdati tijelu za praćenje iz članka 41. ili pružatelju certifikata ako ne ispuni svoje obveze na temelju Opće uredbe o zaštiti podataka Ujedinjene Kraljevine. Osobi koja nije poštovala zahtjev za dostavu informacija, zahtjev za provjeru ili zahtjev za izvršenje može se izdati i rješenje o kazni.

(94) Rješenjem o kazni od osobe se zahtijeva da plati povjereniku za informiranje iznos naveden u obavijesti. Pri odlučivanju o tome treba li osobi izdati rješenje o kazni i određivanju iznosa te kazne povjerenik za informiranje mora uzeti u obzir pitanja navedena u članku 83. stavcima 1. i 2. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, koja su ista kao i odgovarajuća pravila u Uredbi (EU) 2016/679 ([97]). Najveći iznos upravnih novčanih kazni u slučaju nepoštovanja obveza iz članka 83. stavka 4. iznosi 8 700 000 GBP, a za nepoštovanja obveza iz članka 83. stavka 5. taj je iznos 17 500 000 GBP. Ako je riječ o poduzetniku, povjerenik za informiranje kazne

([91]) Članak 142. DPA-a iz 2018. (podložno ograničenjima iz članka 143. DPA-a iz 2018.).
([92]) Članak 146. DPA-a iz 2018. (podložno ograničenjima iz članka 147. DPA-a iz 2018.).
([93]) Članci od 149. do 151. DPA-a iz 2018. (podložno ograničenjima iz članka 152. DPA-a iz 2018.).
([94]) Članak 155. DPA-a iz 2018. i članak 83. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine.
([95]) To proizlazi iz članka 155. stavka 1. DPA-a iz 2018. u vezi s člankom 149. stavcima 2. i 5. DPA-a iz 2018., kao i iz članka 156. stavka 4. DPA-a iz 2018., kojim se ograničava izricanje rješenja o kazni samo u odnosu na povjerenike krunskog imanja (*Crown Estate Commissioners*) i voditelje obrade za kraljevsku obitelj u skladu s člankom 209. stavkom 4. DPA-a iz 2018.
([96]) Politika regulatornog djelovanja, dostupno na: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([97]) Među ostalim prirodu i težinu povrede (uzimajući u obzir narav, opseg i svrhu obrade o kojoj je riječ kao i broj ispitanika i razinu štete koju su pretrpjeli), ima li povreda obilježje namjere ili nepažnje, sve radnje koje je voditelj obrade poduzeo kako bi ublažio štetu koju su pretrpjeli ispitanici, stupanj odgovornosti voditelja obrade ili izvršitelja obrade (uzimajući u obzir tehničke i organizacijske mjere koje su primijenili), sve relevantne prijašnje povrede voditelja obrade ili izvršitelja obrade, stupanj suradnje s povjerenikom, kategorije osobnih podataka na koje povreda utječe, sve ostale otegotne ili olakotne čimbenike koji su primjenjivi na okolnosti slučaja, kao što su financijska dobit ostvarena povredom ili gubici izbjegnuti, izravno ili neizravno, tom povredom.

može izreći i u obliku postotka godišnjeg prometa na svjetskoj razini ako je taj iznos veći. Kao i u istovjetnim odredbama Uredbe (EU) 2016/679, ti su iznosi određeni kao 2 % u članku 83. stavku 4. i 4 % u članku 83. stavku 5. U slučaju nepoštovanja zahtjeva za dostavu informacija, zahtjeva za provjeru ili zahtjeva za izvršenje najveći iznos kazne koji se može izreći u rješenju o kazni iznosi 17 500 000 GBP ili, u slučaju poduzetnika, 4 % godišnjeg prometa na svjetskoj razini, ovisno o tome koji je iznos veći.

(95) Općom uredbom o zaštiti podataka Ujedinjene Kraljevine zajedno s DPA-om iz 2018. ojačane su i druge ovlasti povjerenika za informiranje. Na primjer, zahvaljujući zahtjevima za provjeru povjerenik sad može provoditi obvezne revizije svih voditelja obrade i izvršitelja obrade, dok je na temelju prethodnog propisa (Zakon o zaštiti podataka iz 1998.) tu ovlast imao samo za središnje državne organizacije i zdravstvene organizacije, dok su drugi subjekti morali pristati na reviziju.

(96) Od uvođenja Uredbe (EU) 2016/679 Ured povjerenika za informiranje rješava približno 40 000 pritužbi ispitanika godišnje ([98]), a uz to provodi približno 2 000 istraga po službenoj dužnosti ([99]). Većina pritužbi povezana je s pravima na pristup podacima i otkrivanje podataka. Nakon istraga povjerenik poduzima mjere provedbe u velikom nizu sektora. Točnije, prema najnovijem godišnjem izvješću povjerenice za informiranje (2019.–2020.) ([100]), u razdoblju izvješćivanja povjerenica je izdala 54 zahtjeva za dostavu informacija, 8 zahtjeva za provjeru, 7 zahtjeva za izvršenje, 4 opomene, 15 novčanih kazni i pokrenula je 8 kaznenih progona ([101]).

(97) To uključuje nekoliko većih novčanih kazni izrečenih na temelju Uredbe (EU) 2016/679 i DPA-a iz 2018. Točnije, povjerenica za informiranje u listopadu 2020. izrekla je britanskom zračnom prijevozniku kaznu od 20 milijuna GBP za povredu podataka koja je utjecala na više od 400 000 klijenata. Krajem listopada 2020. međunarodni hotelski lanac kažnjen je s 18,4 milijuna GBP jer nije čuvao sigurnima osobne podatke milijuna klijenata, a u studenome 2020. britanski pružatelj usluga koji preko interneta prodaje ulaznice za događanja kažnjen je s 1,25 milijuna GBP jer nije zaštitio podatke o plaćanju klijenata ([102]).

(98) Osim izvršnih ovlasti povjerenika za informiranje opisanih u uvodnoj izjavi 92., određena kršenja zakonodavstva o zaštiti podataka čine kaznena djela i stoga se na njih mogu primjenjivati kaznene sankcije (članak 196. DPA-a iz 2018.). To se, na primjer, odnosi na namjerno ili slučajno prikupljanje ili otkrivanje osobnih podataka bez pristanka voditelja obrade, omogućavanje otkrivanja osobnih podataka drugoj osobi bez pristanka voditelja obrade ([103]), ponovnu identifikaciju anonimiziranih osobnih podataka bez pristanka voditelja obrade odgovornog za anonimizaciju osobnih podataka ([104]), namjerno ometanje povjerenika u izvršavanju njegovih ovlasti povezanih s pregledom osobnih podataka u skladu s međunarodnim obvezama ([105]), davanje lažnih izjava kao odgovor na zahtjev za dostavu informacija ili uništavanje informacija povezanih sa zahtjevima za dostavu informacija i zahtjevima za provjeru ([106]).

([98]) Prema informacijama koje su dostavila tijela Ujedinjene Kraljevine, u razdoblju izvješćivanja obuhvaćenom Godišnjim izvješćem povjerenice za informiranje za 2019.–2020 povrede nisu utvrđene u približno 25 % slučajeva, u približno 29 % slučajeva od ispitanika se tražilo da se prvi put obrati voditelju obrade podataka, da pričeka odgovor voditelja obrade ili da nastavi dijalog s voditeljem obrade, u približno 17 % slučajeva nije utvrđena povreda, ali voditelju obrade podataka dan je savjet, u približno 25 % slučajeva povjerenica za informiranje utvrdila je povredu i dala savjet voditelju obrade podataka ili je zahtijevala od njega da poduzme određene mjere, u približno 3 % slučajeva utvrđeno je da pritužba nije obuhvaćena područjem primjene Uredbe (EU) 2016/679, a u približno 1 % slučajeva predmeti su upućeni drugom tijelu za zaštitu podataka u okviru Europskog odbora za zaštitu podataka.

([99]) Ured povjerenika za informiranje može pokrenuti te istrage na temelju informacija koje primi iz različitih izvora, uključujući obavijesti o povredi osobnih podataka, upućivanja iz drugih tijela javne vlasti Ujedinjene Kraljevine ili stranih tijela za zaštitu podataka i pritužbe pojedinaca ili organizacija civilnog društva.

([100]) Godišnje izvješće i financijski izvještaji povjerenice za informiranje za 2019.–2020. (vidjeti bilješku 81.).

([101]) Prema prethodnom godišnjem izvješću, koje se odnosilo na razdoblje 2018.–2019., povjerenica za informiranje izdala je u razdoblju izvješćivanja 22 rješenja o kazni na temelju DPA-a iz 1998., a ukupna vrijednost kazni bila je 3 010 610 GBP, uključujući dvije kazne od 500 000 GBP (najveća kazna dopuštena DPA-om iz 1998.). Važna je istraga koju je povjerenica za informiranje provela 2018., u kojoj je istražila upotrebu analize podataka u političke svrhe nakon otkrića slučaja Cambridge Analytica. Nakon istrage objavljeno je izvješće o politici, donesen je skup preporuka, Facebooku je izrečena kazna od 500 000 GBP, a poduzeću Aggregate IQ (kanadski posrednik podataka) izdan je zahtjev za izvršenje u kojem mu je naloženo da izbriše osobne podatke koje ima o građanima i rezidentima Ujedinjene Kraljevine (vidjeti Godišnje izvješće i financijske izvještaje povjerenice za informiranje za 2018.–2019. dostupne na: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf).

([102]) Sažetak poduzetih mjera izvršenja dostupan je na internetskim stranicama Ureda povjerenika za informiranje na: https://ico.org.uk/action-weve-taken/enforcement/.

([103]) Članak 170. DPA-a iz 2018.

([104]) Članak 171. DPA-a iz 2018.

([105]) Članak 119. DPA-a iz 2018.

([106]) Članci 144. i 148. DPA-a iz 2018.

2.6.3. *Nadzor nad sudstvom*

(99) Nadzor nad obradom osobnih podataka koju provode sudovi i pravosuđe dvostran je. Ako nositelj sudačke dužnosti ili sud ne djeluje u okviru sudske nadležnosti, nadzor obavlja Ured povjerenika za informiranje (ICO). Ako voditelj obrade djeluje u okviru sudske nadležnosti, ICO ne može izvršavati svoje nadzorne funkcije ([107]), pa nadzor provode posebna tijela. To odražava pristup iz Uredbe (EU) 2016/679 (članak 55. stavak 3.).

(100) Točnije, u drugom slučaju nadzor nad sudovima u Engleskoj i Walesu te Prvostupanjskim sudom i Višim sudom u Engleskoj i Walesu obavlja Odbor za sudsku zaštitu podataka ([108]). Osim toga, vrhovni sudac (*Lord Chief Justice*) i visoki predsjednik sudova (*Senior President of Tribunals*) objavili su Obavijest o zaštiti osobnih podataka ([109]), u kojoj je navedeno kako sudovi u Engleskoj i Walesu obrađuju osobne podatke za sudbenu funkciju. Sličnu obavijest objavili su i suci Sjeverne Irske ([110]) i Škotske ([111]).

(101) Osim toga, vrhovni sudac Sjeverne Irske imenovao je suca Visokog suda koji u Sjevernoj Irskoj djeluje kao sudac za nadzor podataka ([112]). Objavljene su i smjernice za suce Sjeverne Irske o tome kako postupati u slučaju gubitka ili mogućeg gubitka podataka i postupku za rješavanje svih pitanja koja iz toga mogu proizaći ([113]).

(102) U Škotskoj je predsjednik Vrhovnog građanskog suda (*Lord President*) imenovao suca za nadzor podataka, koji ispituje sve pritužbe u vezi sa zaštitom podataka. To je utvrđeno na temelju pravila o pravosudnim pritužbama koja odražavaju pravila utvrđena za Englesku i Wales ([114]).

(103) Naposljetku, na Vrhovnom sudu jedan od njegovih sudaca predlaže se za funkciju nadziranja zaštite podataka.

2.6.4. *Sudska zaštita*

(104) Kako bi se osigurala primjerena zaštita, a posebno ostvarivanje prava pojedinca, ispitaniku bi trebalo pružiti učinkovitu upravnu i sudsku zaštitu, uključujući naknadu štete.

([107]) Članak 117. DPA-a iz 2018.

([108]) Odbor je odgovoran za davanje smjernica i osposobljavanje sudaca. Bavi se i pritužbama ispitanika na obradu osobnih podataka koju obavljaju sudovi i pojedinci koji djeluju u sudbenom svojstvu. Svrha je Odbora pružiti sredstvo kojim se mogu riješiti sve pritužbe. Ako podnositelj pritužbe nije zadovoljan odlukom Odbora i dostavi dodatne dokaze, Odbor bi mogao preispitati svoju odluku. Iako sam Odbor ne izriče financijske sankcije, ako smatra da je došlo do dovoljno teškog kršenja DPA-a iz 2018., može uputiti slučaj Uredu za preispitivanje sudačkog postupanja (*Judicial Conduct Investigation Office*, JCIO), koji će ispitati pritužbu. Ako se potvrdi osnovanost pritužbe, lord kancelar (*Lord Chancellor*) i vrhovni sudac (ili viši sudac kojem je delegirano da djeluje u njegovo ime) trebaju odlučiti koju bi mjeru trebalo poduzeti protiv nositelja sudačke dužnosti. To bi moglo uključivati, prema stupnju ozbiljnosti: službeni savjet, službeno upozorenje, opomenu i, naposljetku, razrješenje dužnosti. Ako pojedinac nije zadovoljan načinom na koji je JCIO ispitao pritužbu, može se dalje žaliti Ombudsmanu za sudska imenovanja i postupanje (vidjeti https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Ombudsman je ovlašten tražiti od JCIO-a da ponovno ispita pritužbu i može predložiti da se podnositelju pritužbe plati naknada ako smatra da je podnositelj pretrpio štetu kao rezultat nepravilnosti u postupanju.

([109]) Obavijest vrhovnog suca i visokog predsjednika sudova o zaštiti osobnih podataka dostupna je na: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([110]) Obavijest o zaštiti osobnih podataka koju je objavio vrhovni sudac Sjeverne Irske dostupna je na: https://judiciaryni.uk/data-privacy

([111]) Obavijest o zaštiti osobnih podataka za škotske sudove dostupna je na: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([112]) Sudac za nadzor podataka sucima daje smjernice i ispituje povrede i/ili pritužbe na obradu osobnih podataka koju provode sudovi ili pojedinci koji djeluju u sudbenom svojstvu.

([113]) Ako se smatra da je pritužba ili povreda teška, upućuje se službeniku za pravosudne pritužbe radi daljnje istrage u skladu s Kodeksom prakse za pritužbe koji je objavio vrhovni sudac Sjeverne Irske. Ishod takve pritužbe mogao bi biti: bez daljnjeg djelovanja, savjet, osposobljavanje ili mentorstvo, neslužbeno upozorenje, službeno upozorenje, konačno upozorenje, ograničenje prakse ili upućivanje sudu predviđenom zakonom. Kodeks dobre prakse za pritužbe koji je objavio vrhovni sudac Sjeverne Irske dostupan je na: 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]) Sve pritužbe koje su utemeljene ispituje sudac za nadzor podataka i upućuju se predsjedniku Vrhovnog građanskog suda, koji je ovlašten izdati savjet, službeno upozorenje ili opomenu ako smatra da je to potrebno (jednaka pravila postoje za članove sudova i dostupna su na: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

(105) Prvo, ispitanik ima pravo podnijeti pritužbu povjereniku za informiranje ako smatra da u vezi s osobnim podacima koji se odnose na njega postoji kršenje Opće uredbe o zaštiti podataka Ujedinjene Kraljevine ([115]). Pravila iz članka 77. Uredbe (EU) 2016/679 o tom pravu zadržana su u Općoj uredbi o zaštiti podataka Ujedinjene Kraljevine bez bitnih izmjena. Isto vrijedi i za članak 57. stavak 1. točku (f) i članak 57. stavak 2. u kojima su utvrđene zadaće povjerenika povezane s rješavanjem pritužbi. Kako je opisano u uvodnim izjavama od 92. do 98., povjerenik za informiranje ovlašten je ocjenjivati usklađenost voditelja obrade i izvršitelja obrade s Općom uredbom o zaštiti podataka Ujedinjene Kraljevine i DPA-om iz 2018., zahtijevati od njih da poduzmu potrebne korake u slučaju neusklađenosti ili da se suzdrže od njih i izricati novčane kazne.

(106) Drugo, u Općoj uredbi o zaštiti podataka Ujedinjene Kraljevine i DPA-u iz 2018. predviđa se pravo na pravni lijek protiv povjerenika za informiranje. Prema članku 78. stavku 1. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine pojedinac ima pravo na učinkovit pravni lijek protiv pravno obvezujuće odluke povjerenika koja se na njega odnosi. U kontekstu sudskog preispitivanja sudac ispituje odluku koja se osporava u zahtjevu i razmatra je li povjerenik za informiranje postupio zakonito. Nadalje, prema članku 78. stavku 2. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, ako povjerenik ne riješi na odgovarajući način pritužbu koju je podnio ispitanik ([116]), podnositelj pritužbe ima pristup sudskom pravnom lijeku. Može se obratiti Prvostupanjskom sudu, koji će naložiti povjereniku da poduzme odgovarajuće korake kao odgovor na pritužbu ili obavijesti podnositelja pritužbe o ostvarenom napretku u pogledu pritužbe ([117]). Osim toga, svaka osoba kojoj povjerenik izda bilo koji od navedenih zahtjeva ili rješenja (zahtjev za dostavu informacija, provjeru ili izvršenje ili rješenje o kazni) može podnijeti žalbu Prvostupanjskom sudu ([118]). Ako smatra da odluka povjerenika nije u skladu sa zakonom ili da je povjerenik za informiranje trebao drukčije izvršavati diskrecijske ovlasti, Sud mora prihvatiti žalbu ili zamijeniti zahtjev, rješenje ili odluku koju je povjerenik za informiranje izdao ili donio drugim zahtjevom, rješenjem ili odlukom.

(107) Treće, pojedinci mogu dobiti sudsku zaštitu protiv voditelja obrade i izvršitelja obrade izravno pred sudovima na temelju članka 79. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine i članka 167. DPA-a iz 2018. Ako je sud, na zahtjev ispitanika, uvjeren da je došlo do povrede prava ispitanika na temelju zakonodavstva o zaštiti podataka, može naložiti voditelju obrade, ili izvršitelju obrade koji djeluje u ime tog voditelja, da poduzme mjere navedene u nalogu ili da se suzdrži od poduzimanja mjera navedenih u nalogu.

(108) Nadalje, na temelju članka 82. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine i članka 168. DPA-a iz 2018. svaka osoba koja je pretrpjela materijalnu ili nematerijalnu štetu zbog kršenja Opće uredbe o zaštiti podataka Ujedinjene Kraljevine ima pravo na naknadu od voditelja obrade ili izvršitelja obrade za pretrpljenu štetu. Pravila o naknadi i odgovornosti iz članka 82. stavaka od 1. do 5. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine ista su kao i odgovarajuća pravila iz Uredbe (EU) 2016/679. Na temelju članka 168. DPA-a iz 2018. nematerijalna šteta uključuje i duševnu bol. Na temelju članka 80. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine ispitanik ima i pravo ovlastiti predstavničko tijelo ili organizaciju da povjereniku podnese pritužbu u njegovo ime (na temelju članka 77. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine) i da ostvari prava iz članka 78. (pravo na učinkovit sudski pravni lijek protiv povjerenika), članka 79. (pravo na učinkovit pravni lijek protiv voditelja obrade ili izvršitelja obrade) i članka 82. (pravo na naknadu štete i odgovornost) Opće uredbe o zaštiti podataka Ujedinjene Kraljevine u ime ispitanika.

(109) Četvrto, uz prethodno opisane oblike sudske zaštite svaka osoba koja smatra da su tijela javne vlasti prekršila njezina prava, uključujući prava na privatnost i zaštitu podataka, može dobiti sudsku zaštitu pred sudovima Ujedinjene Kraljevine na temelju Zakona o ljudskim pravima iz 1998. ([119]) Pojedinac koji tvrdi da je tijelo javne vlasti djelovalo (ili namjerava djelovati) na način koji nije u skladu s pravom iz Konvencije, a time i nezakonito na temelju članka 6. stavka 1. Zakona o ljudskim pravima iz 1998., može pokrenuti postupak protiv tog tijela pred odgovarajućim sudom ili se može pozvati na predmetna prava u svim sudskim postupcima ako jest (ili bi bio) žrtva nezakonite radnje.

(110) Ako utvrdi da je neka radnja tijela javne vlasti nezakonita, sud može u okviru svojih ovlasti odobriti mjeru ili pravni lijek, ili izdati nalog, kako smatra da je pravedno i primjereno ([120]). Sud može odlučiti i da odredba iz primarnog zakonodavstva nije u skladu s pravom iz Konvencije.

([115]) Članak 77. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine.

([116]) U članku 166. DPA-a iz 2018. konkretno se navode sljedeće situacije: (a) povjerenik nije poduzeo odgovarajuće korake kako bi odgovorio na pritužbu; (b) povjerenik nije dostavio podnositelju pritužbe informacije o napretku ili ishodu pritužbe prije isteka roka od tri mjeseca koji počinje teći od dana kad je povjerenik primio pritužbu; ili (c) ako povjerenik u tom roku nije završio s ispitivanjem pritužbe te o tome nije obavijestio podnositelja pritužbe u narednom razdoblju od tri mjeseca.

([117]) Članak 78. stavak 2. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine i članak 166. DPA-a iz 2018.

([118]) Članak 78. stavak 1. Opće uredbe o zaštiti podataka Ujedinjene Kraljevine i članak 162. DPA-a iz 2018.

([119]) Članak 7. stavak 1. Zakona o ljudskim pravima iz 1998. Prema članku 7. stavku 7. osoba je žrtva nezakonite radnje samo ako bi bila žrtva u smislu članka 34. Europske konvencije o ljudskim pravima ako bi se pred Europskim sudom za ljudska prava pokrenuo postupak koji se odnosi na tu radnju.

([120]) Članak 8. stavak 1. Zakona o ljudskim pravima iz 1998.

(111) Naposljetku, nakon što iscrpi sve nacionalne pravne lijekove, pojedinac može dobiti sudsku zaštitu pred Europskim sudom za ljudska prava za povrede prava zajamčenih Europskom konvencijom o ljudskim pravima.

3. PRISTUP TIJELA JAVNE VLASTI U UJEDINJENOJ KRALJEVINI OSOBNIM PODACIMA PRENESENIMA IZ EUROPSKE UNIJE I NJIHOVA UPOTREBA TIH PODATAKA

(112) Komisija je procijenila i pravni okvir Ujedinjene Kraljevine za prikupljanje i upotrebu osobnih podataka prenesenih poslovnim subjektima u Ujedinjenoj Kraljevini koje tijela javne vlasti Ujedinjene Kraljevine obavljaju u svrhu javnog interesa, osobito za potrebe kaznenog progona i nacionalne sigurnosti (dalje u tekstu „pristup vlade"). Pri procjeni ispunjavaju li uvjeti pod kojima je omogućen pristup vlade podacima prenesenima Ujedinjenoj Kraljevini na temelju ove Odluke test „načelne istovjetnosti" u skladu s člankom 45. stavkom 1. Uredbe (EU) 2016/679, kako je tumači Sud Europske unije s obzirom na Povelju o temeljnim pravima, Komisija je posebno uzela u obzir kriterije u nastavku.

(113) Prvo, svako ograničenje prava na zaštitu osobnih podataka mora biti predviđeno zakonom, a u samoj se pravnoj osnovi kojom se dopušta zadiranje u takvo pravo mora definirati doseg ograničenja ostvarivanja predmetnog prava ([121]).

(114) Drugo, da bi se ispunio zahtjev proporcionalnosti, prema kojem se odstupanja od zaštite osobnih podataka i ograničenja te zaštite u demokratskom društvu moraju primjenjivati samo ako je to nužno za ostvarenje specifičnih ciljeva od općeg interesa koji su jednakovrijedni onima koje priznaje Unija, u predmetnom propisu treće zemlje kojim se dopušta zadiranje u to pravo moraju biti utvrđena jasna i precizna pravila o dosegu i primjeni predmetnih mjera i moraju se uvesti minimalne zaštitne mjere tako da osobe čiji su podaci preneseni raspolažu dostatnim jamstvima koja omogućuju djelotvornu zaštitu njihovih osobnih podataka od rizika zlouporabe ([122]). U propisu se osobito mora navesti u kojim se okolnostima i pod kojim uvjetima može donijeti mjera koja omogućuje obradu tih podataka ([123]), a ispunjenje takvih zahtjeva mora se podvrgnuti neovisnom nadzoru ([124]).

(115) Treće, taj propis mora biti pravno obvezujući na temelju nacionalnog prava, a ti pravni zahtjevi moraju biti obvezujući za tijela i izvršivi pred sudovima protiv tijela predmetne treće zemlje ([125]). Točnije, ispitanici moraju imati mogućnost pokretanja sudskog postupka pred neovisnim i nepristranim sudom radi pristupa svojim osobnim podacima ili ispravka ili brisanja tih podataka ([126]).

3.1. Opći pravni okvir

(116) Pristup vlade u Ujedinjenoj Kraljevini, u okviru izvršavanja ovlasti tijela javne vlasti, mora se provoditi uz potpuno poštovanje zakona. Ujedinjena Kraljevina ratificirala je Europsku konvenciju o ljudskim pravima (vidjeti uvodnu izjavu 9.) i sva su tijela javne vlasti u Ujedinjenoj Kraljevini obvezna postupati u skladu s Konvencijom ([127]). U članku 8. Konvencije navedeno je da svako miješanje u privatnost mora biti u skladu sa zakonom, u svrhu jednog od ciljeva utvrđenih u članku 8. stavku 2. i proporcionalno s obzirom na taj cilj. Člankom 8. zahtijeva se i da je miješanje „predvidivo", tj. da ima jasnu, pristupačnu pravnu osnovu i da su u zakonu dostupne odgovarajuće zaštitne mjere radi sprečavanja zloupotrebe.

(117) Osim toga, Europski sud za ljudska prava u svojoj je sudskoj praksi odredio da se na svako zadiranje u pravo na privatnost i zaštitu podataka treba primjenjivati učinkovit, neovisan i nepristran sustav nadzora koji mora predvidjeti sudac ili drugo neovisno tijelo ([128]) (npr. upravno ili parlamentarno tijelo).

([121]) Vidjeti predmet *Schrems II*, točke 174. i 175. te navedenu sudsku praksu. Kad je riječ o pristupu tijela javne vlasti država članica, vidjeti i predmet C-623/17 *Privacy International*, ECLI:EU:C:2020:790, točku 65. i spojene predmete C-511/18, C-512/18 i C-520/18 *La Quadrature du Net i dr.*, ECLI:EU:C:2020:791, točku 175.

([122]) Vidjeti predmet *Schrems II*, točke 176. i 181. te navedenu sudsku praksu. Kad je riječ o pristupu tijela javne vlasti država članica, vidjeti i predmet *Privacy International*, točku 68. i predmet *La Quadrature du Net i dr.*, točku 132.

([123]) Vidjeti predmet *Schrems II*, točku 176. Kad je riječ o pristupu tijela javne vlasti država članica, vidjeti i predmet *Privacy International*, točku 68. i predmet *La Quadrature du Net i dr.*, točku 132.

([124]) Vidjeti predmet *Schrems II*, točku 179.

([125]) Vidjeti predmet *Schrems II*, točke 181. i 182.

([126]) Vidjeti predmet *Schrems I*, točku 95. i predmet *Schrems II*, točku 194. Sud Europske unije u tom je pogledu posebno istaknuo da poštovanje članka 47. Povelje o temeljnim pravima, u kojem se jamči pravo na djelotvoran pravni lijek pred neovisnim i nepristranim sudom, „pridonosi razini zaštite koja se zahtijeva u okviru Unije [i to poštovanje] mora utvrditi Komisija prije nego što donese odluku o primjerenosti na temelju članka 45. stavka 1. [Uredbe (EU) 2016/679]" (*Schrems II*, točka 186.).

([127]) Članak 6. Zakona o ljudskim pravima iz 1998.

([128]) Europski sud za ljudska prava, *Klass i drugi protiv Njemačke*, zahtjev br. 5029/71, točke 17.–51.

(118) Nadalje, pojedincima se mora pružiti djelotvoran pravni lijek, a Europski sud za ljudska prava pojasnio je da ga mora ponuditi neovisno i nepristrano tijelo koje je donijelo svoj poslovnik, koje se sastoji od članova koji moraju imati ili su prethodno imali visoki položaj u pravosuđu ili su iskusni pravnici te da ne smije postojati teret dokazivanja koji se mora savladati da bi se tom tijelu podnio zahtjev. Kad ispituje pritužbe pojedinaca, neovisno i nepristrano tijelo trebalo bi imati pristup svim relevantnim informacijama, uključujući zapečaćene materijale. Naposljetku, trebalo bi imati ovlasti otklanjanja neusklađenosti ([129]).

(119) Ujedinjena Kraljevina ratificirala je i Konvenciju Vijeća Europe za zaštitu osoba glede automatizirane obrade osobnih podataka (Konvencija br. 108), a 2018. potpisala je i Protokol o izmjeni Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka (poznat kao „Konvencija br. 108+") ([130]). U članku 9. Konvencije br. 108 navedeno je da su odstupanja od općih načela zaštite podataka (članak 5. Svojstvo podataka), pravila za posebne kategorije podataka (članak 6. Posebne kategorije podataka) i prava ispitanika (članak 8. Dodatna jamstva za subjekt podataka) dopuštena samo ako je takvo odstupanje predviđeno pravom stranke i ako je to u demokratskom društvu nužna mjera u korist zaštite državne sigurnosti, javne sigurnosti, monetarnih interesa države ili suzbijanja kaznenih djela ili zaštite ispitanika ili prava i slobode drugih ([131]).

(120) Ujedinjena Kraljevina stoga u okviru članstva u Vijeću Europe, poštovanja Europske konvencije o ljudskim pravima i priznavanja nadležnosti Europskog suda za ljudska prava podliježe nizu obveza iz međunarodnog prava koje oblikuju njezin sustav pristupa vlade tako da se temelji na načelima, zaštitnim mjerama i pravima pojedinaca sličnima onima zajamčenima pravom Unije i primjenjivima u državama članicama. Kako je istaknuto u uvodnoj izjavi 19., kontinuirano poštovanje tih pravnih instrumenata stoga je osobito važan element procjene na kojoj se temelji ova Odluka.

(121) Nadalje, DPA-om iz 2018. jamče se posebne zaštitne mjere i prava u pogledu zaštite podataka ako podatke obrađuju tijela javne vlasti, uključujući tijela kaznenog progona i tijela za nacionalnu sigurnost.

(122) Točnije, sustav za obradu osobnih podataka u kontekstu kaznenog progona utvrđen je u dijelu 3. DPA-a iz 2018., koji je donesen radi prenošenja Direktive (EU) 2016/680. Dio 3. DPA-a iz 2018. primjenjuje se na obradu osobnih podataka koju vrše nadležna tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje ([132]).

(123) Pojam „nadležno tijelo" definiran je u članku 30. DPA-a kao osoba navedena u Prilogu 7. DPA-u iz 2018. te bilo koja druga osoba u mjeri u kojoj ima zakonski propisane funkcije u obavljanju bilo koje od svrha kaznenog progona ([133]). Kako je objašnjeno u nastavku (vidjeti uvodnu izjavu 139.), određena nadležna tijela (npr. Nacionalna agencija za kriminal (*National Crime Agency*)) mogu se, pod određenim uvjetima, koristiti ovlastima predviđenima Zakonom o istražnim ovlastima iz 2016. (IPA iz 2016.). U tom će se slučaju zaštitne mjere predviđene u okviru IPA-e iz 2016. primjenjivati uz zaštitne mjere predviđene u dijelu 3. DPA-a iz 2018. Obavještajne službe (Tajna obavještajna služba (*Secret Intelligence Service*), Sigurnosna služba (*Security Service*) i Vladin komunikacijski stožer (*Government Communications Headquarters*)) nisu „nadležna tijela" ([134]) obuhvaćena područjem primjene dijela 3. DPA-a iz 2018. pa se pravila iz tog dijela ne primjenjuju ni na jednu od njihovih aktivnosti. Poseban dio DPA-a iz 2018. (dio 4.) posvećen je obradi osobnih podataka koju provode obavještajne službe (za više pojedinosti vidjeti uvodnu izjavu 125.).

([129]) Europski sud za ljudska prava, *Kennedy protiv Ujedinjene Kraljevine*, zahtjev br. 26839/05, (*Kennedy*), točke 167. i 190.

([130]) Više informacija o Europskoj konvenciji o ljudskim pravima i njezinu uključivanju u pravo Ujedinjene Kraljevine putem Zakona o ljudskim pravima iz 1998. te o Konvenciji br. 108 nalazi se u uvodnoj izjavi 9.

([131]) Usto, prema članku 11. Konvencije br. 108+ ograničenja određenih posebnih prava i obveza iz Konvencije za potrebe nacionalne sigurnosti ili sprečavanja, istrage i progona kaznenih djela te izvršenja kaznenih sankcija dopuštena su samo ako je takvo ograničenje predviđeno zakonom, ako se njime poštuje bit temeljnih prava i sloboda i ako ono predstavlja nužnu i proporcionalnu mjeru u demokratskom društvu. Aktivnosti obrade u svrhe nacionalne sigurnosti i obrane moraju biti podložne i neovisnom i učinkovitom preispitivanju i nadzoru u skladu s unutarnjim zakonodavstvom predmetne stranke Konvencije.

([132]) Članak 31. DPA-a iz 2018.

([133]) Nadležna tijela navedena u Prilogu 7. ne obuhvaćaju samo policijske snage već i sve vladine odjele pod izravnim nadzorom ministarstva Ujedinjene Kraljevine te druga tijela s istražnim funkcijama (npr. Porezna i carinska uprava Ujedinjene Kraljevine (*Commissioner for Her Majesty's Revenue and Customs*), Nacionalna agencija za kriminal, Velška porezna uprava (*Welsh Revenue Authority*), Nadležno tijelo za tržišno natjecanje i tržišta (*Competition and Markets Authority*) ili Zemljišnoknjižni ured za Englesku i Wales (*Her Majesty's Land Register*)), državna odvjetništva, druge agencije nadležne za kazneno pravosuđe i druge ovlaštenike ili organizacije koji obavljaju aktivnosti kaznenog progona (među ostalim, u Prilogu 7. DPA-u iz 2018. navedeni su ravnatelji državnih odvjetništva, ravnatelj državnog odvjetništva Sjeverne Irske ili povjerenik za informiranje).

([134]) Članak 30. stavak 2. DPA-a iz 2018.

(124) Slično Direktivi (EU) 2016/680, u dijelu 3. DPA-a iz 2018. utvrđena su načela zakonitosti i poštenosti ([135]), ograničavanja svrhe ([136]), smanjenja količine podataka ([137]), točnosti ([138]), ograničenja pohrane ([139]) i sigurnosti ([140]). Propisom su uvedene specifične obveze u pogledu transparentnosti ([141]) i pojedincima se daju pravo na pristup ([142]), ispravak i brisanje ([143]) te pravo da se na njih ne odnosi automatizirano donošenje odluka ([144]). Nadležna tijela moraju uvesti i tehničku i integriranu zaštitu podataka, voditi evidenciju aktivnosti obrade, a za određene postupke obrade provesti procjenu učinka na zaštitu podataka i unaprijed se savjetovati s povjerenikom za informiranje ([145]). Prema članku 56. DPA-a iz 2018. moraju dokazati usklađenost. Nadalje, moraju uspostaviti odgovarajuće mjere kojima će osigurati sigurnost obrade ([146]) i podliježu specifičnim obvezama u slučaju povrede podataka, uključujući obavješćivanje povjerenika za informiranje i ispitanika o takvim povredama ([147]). Kao i u Direktivi (EU) 2016/680, zahtijeva se i da voditelj obrade (osim ako je riječ o sudu ili drugom pravosudnom tijelu koje djeluje u okviru sudske nadležnosti) imenuje službenika za zaštitu podataka ([148]) koji voditelju obrade pomaže da poštuje svoje obveze i da prati njihovo poštovanje ([149]). Nadalje, propisom se uvode posebni zahtjevi za međunarodne prijenose osobnih podataka trećim zemljama ili međunarodnim organizacijama u svrhe kaznenog progona radi osiguravanja kontinuiteta zaštite ([150]). Na isti datum kad i ovu Odluku, Komisija je donijela odluku o primjerenosti na temelju članka 36. stavka 3. Direktive (EU) 2016/680, u kojoj je utvrdila da sustav zaštite podataka primjenjiv na obradu koju vrše tijela kaznenog progona u Ujedinjenoj Kraljevini osigurava razinu zaštite koja je u načelu istovjetna onoj koja je osigurana Direktivom (EU) 2016/680.

(125) Dio 4. DPA-a iz 2018. primjenjuje se na svu obradu koju vrše obavještajne službe ili koja se vrši u njihovo ime. Točnije, u njemu se utvrđuju glavna načela zaštite podataka (zakonitost, poštenost i transparentnost ([151]), ograničavanje svrhe ([152]), smanjenje količine podataka ([153]), točnost ([154]), ograničenje pohrane ([155]) i sigurnost ([156])), uvode se uvjeti za obradu posebnih kategorija podataka ([157]), predviđaju se prava ispitanika ([158]), zahtijeva se

([135]) Članak 35. DPA-a iz 2018.
([136]) Članak 36. DPA-a iz 2018.
([137]) Članak 37. DPA-a iz 2018.
([138]) Članak 38. DPA-a iz 2018.
([139]) Članak 39. DPA-a iz 2018.
([140]) Članak 40. DPA-a iz 2018.
([141]) Članak 44. DPA-a iz 2018.
([142]) Članak 45. DPA-a iz 2018.
([143]) Članci 46. i 47. DPA-a iz 2018.
([144]) Članci 49. i 50. DPA-a iz 2018.
([145]) Članci od 56. do 65. DPA-a iz 2018.
([146]) Članak 66. DPA-a iz 2018.
([147]) Članci od 67. do 68. DPA-a iz 2018.
([148]) Članci od 69. do 71. DPA-a iz 2018.
([149]) Članci od 67. do 68. DPA-a iz 2018.
([150]) Dio 3. poglavlje 5. DPA-a iz 2018.
([151]) Prema članku 86. stavku 6. DPA-a iz 2018. kako bi se utvrdila poštenost i transparentnost obrade, u obzir se mora uzeti metoda kojom su podaci dobiveni. U tom je smislu zahtjev za poštenost i transparentnost ispunjen ako su podaci dobiveni od osobe koja je zakonito ovlaštena ili dužna dostaviti te podatke.
([152]) Prema članku 87. DPA-a iz 2018. svrhe obrade moraju biti posebne, izričite i zakonite. Podaci se ne smiju obrađivati na način koji nije u skladu sa svrhama u koje su prikupljeni. Prema članku 87. stavku 3. DPA-a iz 2018. daljnja usklađena obrada osobnih podataka dopuštena je samo ako je voditelj obrade zakonski ovlašten obrađivati podatke u tu svrhu i ako je obrada nužna i proporcionalna toj drugoj svrsi. Obradu bi trebalo smatrati usklađenom ako se obavlja u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe i ako se na nju primjenjuju odgovarajuće zaštitne mjere (članak 87. stavak 4. DPA-a iz 2018.).
([153]) Osobni podaci moraju biti primjereni, relevantni i ne smiju biti pretjerani (članak 88. DPA-a iz 2018.).
([154]) Osobni podaci moraju biti točni i ažurirani (članak 89. DPA-a iz 2018.).
([155]) Osobni podaci moraju se čuvati samo onoliko dugo koliko je potrebno (članak 90. DPA-a iz 2018.).
([156]) Šesto načelo zaštite podataka nalaže da se osobni podaci moraju obrađivati na način koji uključuje poduzimanje odgovarajućih sigurnosnih mjera za rizike koji proizlaze iz obrade osobnih podataka. Ti rizici uključuju (ali nisu ograničeni na) slučajan ili neovlašten pristup osobnim podacima ili njihovo uništavanje, gubitak, uporabu, izmjenu ili otkrivanje (članak 91. DPA-a iz 2018.). U članku 107. zahtijeva se i sljedeće: 1. svaki voditelj obrade mora provesti odgovarajuće sigurnosne mjere koje odgovaraju rizicima koji proizlaze iz obrade osobnih podataka; i 2. u slučaju automatizirane obrade svaki voditelj obrade i izvršitelj obrade mora provesti preventivne mjere ili mjere ublažavanja na temelju procjene rizika.
([157]) Članak 86. stavak 2. točka (b) i Prilog 10. DPA-u iz 2018.
([158]) Dio 4. poglavlje 3. DPA-a iz 2018., osobito: pravo na pristup, ispravak i brisanje, pravo na ulaganje prigovora na obradu i pravo ispitanika da ne podliježe automatiziranom donošenju odluka, pravo na intervenciju u automatizirano donošenje odluka i pravo na obavijest o donošenju odluka. Osim toga, voditelj obrade mora ispitaniku dati informacije o obradi njegovih osobnih podataka. Kako je objašnjeno u smjernicama ICO-a o obradi podatka koju provode obavještajne službe, pojedinci mogu ostvariti sva svoja prava (uključujući zahtjev za ispravak) podnošenjem pritužbe ICO-u ili pokretanjem sudskog postupka (vidjeti Smjernice ICO-a za obradu podataka izdane obavještajnim službama, dostupne na sljedećoj poveznici: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

tehnička zaštita podataka ([159]) i uređuju se međunarodni prijenosi osobnih podataka ([160]). ICO je nedavno izdao detaljne smjernice o obradi podataka koju provode obavještajne agencije u skladu s dijelom 4. DPA-a iz 2018. ([161])

(126) Isto tako, u članku 110. DPA-a iz 2018. predviđa se izuzeće od određenih odredbi iz dijela 4. DPA-a iz 2018. ([162]) kad je to izuzeće potrebno radi zaštite nacionalne sigurnosti. Na to se izuzeće može pozvati na temelju analize za svaki pojedinačni slučaj ([163]). Kako su objasnila tijela Ujedinjene Kraljevine i kako potvrđuje sudska praksa, „voditelj obrade mora uzeti u obzir stvarne posljedice za nacionalnu sigurnost ili obranu ako bi morao poštovati određenu odredbu o zaštiti podataka i može li opravdano poštovati uobičajeno pravilo bez utjecaja na nacionalnu sigurnost ili obranu" ([164]). ICO nadzire je li izuzeće primijenjeno na odgovarajući način ([165]).

(127) Nadalje, u odnosu na mogućnost ograničavanja primjene prethodno utvrđenih odredbi u skladu s člankom 111. DPA-a iz 2018. radi zaštite „nacionalne sigurnosti" voditelj obrade može podnijeti zahtjev za potvrdu koju potpisuje ministar koji je član kabineta ili glavni krunski odvjetnik (*Attorney General*), kojom se potvrđuje da je ograničavanje tih prava nužna i proporcionalna mjera za zaštitu nacionalne sigurnosti ([166]).

(128) Vlada Ujedinjene Kraljevine objavila je smjernice kao pomoć voditeljima obrade kad razmatraju hoće li podnijeti zahtjev za potvrdu o nacionalnoj sigurnosti na temelju DPA-a iz 2018., u kojima je osobito istaknuto da svako ograničavanje prava ispitanika radi zaštite nacionalne sigurnosti mora biti proporcionalno i nužno ([167]). Sve potvrde o nacionalnoj sigurnosti moraju biti objavljene na internetskim stranicama ICO-a ([168]).

([159]) Članak 103. DPA-a iz 2018.

([160]) Članak 109. DPA-a iz 2018. Prijenosi osobnih podataka međunarodnim organizacijama ili zemljama izvan Ujedinjene Kraljevine mogući su ako je prijenos nužna i proporcionalna mjera koja se provodi u svrhe zakonom propisanih funkcija voditelja obrade ili u drugu svrhu predviđenu u određenim člancima Zakona o sigurnosnim službama iz 1989. i Zakona o obavještajnim službama iz 1994.

([161]) Smjernice ICO-a, vidjeti bilješku 158.
Članak 30. DPA-a iz 2018. i Prilog 7. DPA-u iz 2018.

([162]) U članku 110. stavku 2. DPA-a iz 2018. navedene su odredbe od kojih je dopušteno izuzeće. One uključuju načela zaštite podataka (osim načela zakonitosti), prava ispitanika, obvezu obavješćivanja povjerenika za informiranje o povredi podataka, ovlasti povjerenika za informiranje povezane s inspekcijom u skladu s međunarodnim obvezama, određene izvršne ovlasti povjerenika za informiranje, odredbe prema kojima su određena kršenja zaštite podataka kazneno djelo i odredbe o posebnim svrhama obrade kao što su novinarske, akademske ili umjetničke svrhe.

([163]) Vidjeti *Baker protiv Secretary of State*, bilješka 61.

([164]) Okvir za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, odjeljak H: Okvir za zaštitu podataka i istražne ovlasti s obzirom na nacionalnu sigurnost, str. 15.–16. (vidjeti bilješku 31.). Vidjeti i predmet *Baker protiv Secretary of State* (vidjeti bilješku 61.), u kojem je sud ukinuo potvrdu o nacionalnoj sigurnosti koju je izdao ministar unutarnjih poslova (*Home Secretary*) i koja potvrđuje primjenu iznimke radi nacionalne sigurnosti jer je smatrao da nije postojao razlog za opću iznimku od obveze odgovora na zahtjeve za pristup podacima te da dopuštanje takve iznimke u svim okolnostima bez pojedinačne analize svakog slučaja premašuje ono što je nužno i proporcionalno za zaštitu nacionalne sigurnosti.

([165]) Vidjeti Memorandum o razumijevanju između ICO-a i obavještajne zajednice Ujedinjene Kraljevine u kojem je navedeno sljedeće: „Po zaprimanju pritužbe ispitanika ICO se treba uvjeriti da je pitanje pravilno riješeno i, prema potrebi, da su sva izuzeća primijenjena na odgovarajući način." Memorandum o razumijevanju između Ureda povjerenika za informiranje i obavještajne zajednice Ujedinjene Kraljevine, točka 16., dostupno na: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf

([166]) DPA-om iz 2018. ukinuta je mogućnost izdavanja potvrde na temelju članka 28. stavka 2. Zakona o zaštiti podataka iz 1998. Međutim, mogućnost izdavanja „starih potvrda" i dalje postoji ako postoji prethodno osporavanje na temelju Zakona iz 1998. (vidjeti točku 17. dijela 5. Priloga 20. DPA-u iz 2018.). Ipak, ta se mogućnost čini vrlo rijetkom i primjenjivat će se samo u ograničenim slučajevima, kao što je, na primjer, ako ispitanik dovodi u pitanje primjenu izuzeća radi nacionalne sigurnosti u pogledu obrade podataka koju je tijelo javne vlasti provelo u skladu sa Zakonom iz 1998. Treba napomenuti da će se u tim slučajevima u cijelosti primjenjivati članak 28. DPA-a iz 1998., uključujući stoga mogućnost da ispitanik osporava potvrdu pred Sudom.

([167]) Smjernice Vlade Ujedinjene Kraljevine o potvrdama o nacionalnoj sigurnosti na temelju Zakona o zaštiti podataka iz 2018., dostupne na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf Prema objašnjenju koje su dostavila tijela Ujedinjene Kraljevine, iako je potvrda uvjerljiv dokaz da je izuzeće primjenjivo (na podatke ili obradu opisanu u potvrdi), ona ne ukida zahtjev da voditelj obrade na pojedinačnoj osnovi razmotri je li potrebno pozvati se na izuzeće.

([168]) U skladu s člankom 130. DPA-a iz 2018. ICO može odlučiti da neće objaviti tekst ili dio teksta potvrde ako bi to bilo protivno interesu nacionalne sigurnosti ili bi bilo u suprotnosti s javnim interesom ili bi moglo ugroziti sigurnost bilo koje osobe. Međutim, u tim će slučajevima ICO objaviti činjenicu da je potvrda izdana.

(129) Potvrda bi trebala imati ograničeno trajanje koje nije dulje od pet godina kako bi je izvršna vlast redovito preispitivala ([169]). U potvrdi se navode osobni podaci ili kategorije osobnih podataka na koje se izuzeće primjenjuje i odredbe iz DPA-a iz 2018. na koje se izuzeće primjenjuje ([170]).

(130) Važno je napomenuti da potvrde o nacionalnoj sigurnosti ne pružaju dodatni razlog za ograničavanje prava na zaštitu podataka zbog nacionalne sigurnosti. Drugim riječima, voditelj obrade ili izvršitelj obrade može se pozvati na potvrdu samo ako je zaključio da je nužno pozvati se na izuzeće radi nacionalne sigurnosti koje se, kako je prethodno objašnjeno, mora primjenjivati na pojedinačnoj osnovi ([171]). Čak i ako se potvrda o nacionalnoj sigurnosti primjenjuje na predmetno pitanje, ICO može istražiti je li pozivanje na izuzeće radi nacionalne sigurnosti bilo opravdano u konkretnom slučaju ([172]).

(131) Sve osobe na koje izdavanje potvrde izravno utječe mogu podnijeti žalbu Višem sudu ([173]) protiv potvrde ([174]) ili, ako su u potvrdi podaci identificirani općim opisom, osporiti primjenu potvrde na konkretne podatke ([175]). Sud će preispitati odluku o izdavanju potvrde i odlučiti jesu li postojali opravdani razlozi za izdavanje potvrde ([176]). Može razmotriti širok niz pitanja, uključujući nužnost, proporcionalnost i zakonitost, a pritom mora uzeti u obzir učinak na prava ispitanika i uspostaviti ravnotežu s potrebom zaštite nacionalne sigurnosti. Stoga Sud može utvrditi da se potvrda ne primjenjuje na konkretne osobne podatke koji su predmet žalbe ([177]).

(132) Drugi skup mogućih ograničenja odnosi se na ona koja se primjenjuju, na temelju Priloga 11. DPA-u iz 2018., na određene odredbe iz dijela 4. DPA-a iz 2018. ([178]) radi zaštite drugih važnih ciljeva od općeg javnog interesa ili zaštićenih interesa kao što su parlamentarni imunitet, odvjetnička tajna, vođenje sudskog postupka ili bojna pripravnost oružanih snaga ([179]). Primjena tih odredbi izuzeta je za određene kategorije informacija („izuzeća na temelju razreda") ili je izuzeta u mjeri u kojoj bi primjena tih odredbi vjerojatno dovela u pitanje zaštićeni interes („izuzeća na temelju ugrožavanja") ([180]). Na izuzeća na temelju ugrožavanja moguće je pozvati se samo ako bi primjena navedenih odredbi o zaštiti podataka vjerojatno dovela u pitanje predmetni posebni interes. Stoga primjena izuzeća uvijek mora biti opravdana upućivanjem na relevantno ugrožavanje do kojeg bi vjerojatno došlo u

([169]) Smjernice Vlade Ujedinjene Kraljevine o potvrdama o nacionalnoj sigurnosti, točka 15., vidjeti bilješku 167.

([170]) Smjernice Vlade Ujedinjene Kraljevine o potvrdama o nacionalnoj sigurnosti, točka 5., vidjeti bilješku 167.

([171]) Vidjeti bilješku 164.

([172]) U članku 102. DPA-a iz 2018. zahtijeva se da voditelj obrade može dokazati da je poštovao DPA iz 2018. To znači da bi obavještajna služba trebala ICO-u dokazati da je pri pozivanju na izuzeće uzela u obzir posebne okolnosti slučaja. ICO objavljuje i evidenciju potvrda o nacionalnoj sigurnosti, koja je dostupna na: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([173]) Viši sud nadležan je za saslušanje žalbi na odluke nižih upravnih sudova i posebno je nadležan za izravne žalbe na odluke određenih vladinih tijela.

([174]) Članak 111. stavak 3. DPA-a iz 2018.

([175]) Članak 111. stavak 5. DPA-a iz 2018.

([176]) U predmetu *Baker protiv Secretary of State* (vidjeti bilješku 61.) Sud za informacije ukinuo je potvrdu o nacionalnoj sigurnosti koju je izdao ministar unutarnjih poslova jer je Sud smatrao da nije postojao razlog za opću iznimku od obveze odgovora na zahtjeve za pristup podacima te da dopuštanje takve iznimke u svim okolnostima bez analize za svaki pojedinačni slučaj premašuje ono što je nužno i proporcionalno za zaštitu nacionalne sigurnosti.

([177]) Smjernice Vlade Ujedinjene Kraljevine o potvrdama o nacionalnoj sigurnosti, točka 25., vidjeti bilješku 167.

([178]) To uključuje: i. načela zaštite podataka iz dijela 4., osim zahtjeva za zakonitost obrade na temelju prvog načela i činjenice da obrada mora ispunjavati jedan od relevantnih uvjeta utvrđenih u prilozima 9. i 10.; ii. prava ispitanika; i iii. dužnosti povezane s prijavljivanjem povreda ICO-u.

([179]) U dijelu 4. DPA-a iz 2018. predviđa se pravni okvir koji se primjenjuje na sve vrste obrade osobnih podataka koju provode obavještajne agencije (a ne samo na provedbu njihovih zadaća nacionalne sigurnosti). Stoga se dio 4. primjenjuje i na obradu podataka koju provode obavještajne agencije, primjerice za potrebe upravljanja ljudskim resursima, u kontekstu sporova ili u kontekstu javne nabave. Ograničenja navedena u Prilogu 11. uglavnom bi se trebala primjenjivati u tim drugim kontekstima. Na primjer, u kontekstu sudskog postupka sa zaposlenikom može se pozvati na ograničenje za potrebe „sudskog postupka" ili se u kontekstu javne nabave može pozvati na ograničenje za potrebe „pregovaranja" itd. To je uzeto u obzir u smjernicama ICO-a o obradi podataka koju provode obavještajne službe, u kojima se navode pregovori o nagodbi između obavještajne agencije i bivšeg zaposlenika koji podnosi tužbu za povredu prava iz radnog odnosa kao primjer za primjenu ograničenja iz Priloga 11. (vidjeti bilješku 161.). Treba napomenuti i da su ista ograničenja dostupna drugim tijelima javne vlasti u skladu s Prilogom 2. dijelu 2. DPA-a iz 2018.

([180]) Prema Okviru za objašnjenja Ujedinjene Kraljevine izuzeća „na temelju razreda" jesu: i. informacije o dodjeli časti i odličja Krune; ii. odvjetnička tajna; iii. povjerljivi podaci o zaposlenju, osposobljavanju ili obrazovanju; i iv. ispitni radovi i ocjene. Izuzeća „na temelju ugrožavanja" odnose se na sljedeća pitanja: i. sprečavanje ili otkrivanje kaznenog djela; uhićenje i kazneni progon počiniteljâ; ii. parlamentarni imunitet; iii. sudski postupak; iv. bojnu pripravnost oružanih snaga Krune; v. gospodarsku dobrobit Ujedinjene Kraljevine; vi. pregovore s ispitanikom; vii. znanstveno ili povijesno istraživanje ili statističke svrhe; viii. arhiviranje u javnom interesu. Okvir za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, odjeljak H: Nacionalna sigurnost, str. 13., vidjeti bilješku 31.

pojedinačnom slučaju. Na izuzeća na temelju razreda moguće je pozvati se samo u pogledu posebne, usko definirane kategorije informacija za koju je odobreno izuzeće. Ona su prema svrsi i učinku slična određenim izuzećima od Opće uredbe o zaštiti podataka Ujedinjene Kraljevine (na temelju Priloga 2. DPA-u iz 2018.), koja odražavaju izuzeća predviđena člankom 23. Opće uredbe o zaštiti podataka.

(133) Iz prethodno navedenog proizlazi da su u primjenjivim pravnim odredbama Ujedinjene Kraljevine, kako su ih tumačili i sudovi i povjerenik za informiranje, uspostavljena ograničenja i uvjeti koji osiguravaju da ta izuzeća i ograničenja ostanu u granicama onog što je nužno i proporcionalno za zaštitu nacionalne sigurnosti.

3.2. **Pristup tijela javne vlasti Ujedinjene Kraljevine podacima i njihova uporaba za potrebe kaznenog progona**

(134) U pravu Ujedinjene Kraljevine nalazi se niz ograničenja pristupa osobnim podacima i njihove uporabe za potrebe kaznenog progona te se u tom području pružaju mehanizmi nadzora i sudske zaštite koji su u skladu sa zahtjevima iz uvodnih izjava od 113. do 115. ove Odluke. Uvjeti u kojima je takav pristup moguć i zaštitne mjere koje se primjenjuju na upotrebu tih ovlasti detaljno su procijenjeni u odjeljcima u nastavku.

3.2.1. *Pravne osnove i primjenjiva ograničenja/zaštitne mjere*

(135) U skladu s načelom zakonitosti zajamčenim člankom 35. DPA-a iz 2018. obrada osobnih podataka u bilo koju svrhu kaznenog progona zakonita je samo ako se temelji na pravu te ako je ispitanik dao privolu za obradu u tu svrhu ([181]) ili je obrada nužna za izvršavanje zadaće koju u tu svrhu obavlja nadležno tijelo.

3.2.1.1. Nalozi za pretragu i nalozi za dostavljanje

(136) U pravnom okviru Ujedinjene Kraljevine prikupljanje osobnih podataka od poslovnih subjekata, uključujući one koji bi obrađivali podatke prenesene iz EU-a na temelju sadašnje odluke o primjerenosti, za potrebe kaznenog progona dopušteno je na temelju naloga za pretragu ([182]) i naloga za dostavljanje ([183]).

(137) Naloge za pretragu izdaje sud, obično na zahtjev istražitelja. Oni istražitelju dopuštaju ulazak u određene prostore kako bi pronašao materijal ili pojedince relevantne za njegovu istragu i da zadrži sve za što je odobrena pretraga, uključujući sve relevantne dokumente ili materijale koji sadržavaju osobne podatke ([184]). Nalogom za dostavljanje, koji isto mora izdati sud, od osobe navedene u nalogu zahtijeva se da dostavi ili omogući pristup materijalu u njezinu posjedu ili pod njezinom

([181]) Čini se da privola nije relevantna u scenariju primjerenosti jer u situaciji prijenosa tijelo kaznenog progona iz Ujedinjene Kraljevine neće izravno prikupljati podatke od ispitanika iz EU-a na temelju privole.

([182]) Relevantna pravna osnova nalazi se u članku 8. i dalje PACE-a iz 1984. (Zakon o policiji i kaznenim dokazima) (za Englesku i Wales), članku 10. i dalje Uredbe o policiji i kaznenim dokazima (Sjeverna Irska) iz 1989., a za Škotsku se izvodi iz precedentnog prava (vidjeti članak 46. Zakona o kaznenom pravosuđu (Škotska) iz 2016. i članak 23.B Kaznenog zakona (konsolidirano) (Škotska)). Za naloge za pretragu izdane nakon uhićenja pravnu osnovu čini članak 18. PACE-a iz 1984. (za Englesku i Wales), članak 20. i dalje Uredbe o policiji i kaznenim dokazima (Sjeverna Irska) iz 1989., a za Škotsku se pravna osnova izvodi iz precedentnog prava (vidjeti članak 46. Zakona o kaznenom pravosuđu (Škotska) iz 2016.). Tijela Ujedinjene Kraljevine pojasnila su da naloge za pretragu izdaje sud na zahtjev istražitelja. Oni istražitelju dopuštaju ulazak u određene prostore kako bi pronašao materijal ili pojedince relevantne za njegovu istragu; za izvršenje naloga često će biti potrebna pomoć policijskog službenika.

([183]) Ako se istraga odnosi na pranje novca (uključujući oduzimanje i građanski postupak naplate), relevantnu pravnu osnovu za podnošenje zahtjeva za nalog za dostavljanje čine članak 345. i dalje Zakona o oduzimanju nezakonito stečene imovine iz 2002. za Englesku, Wales i Sjevernu Irsku te članak 380. i dalje tog zakona za Škotsku. Ako se istraga odnosi na druga pitanja osim pranja novca, zahtjev za nalog za dostavljanje može se podnijeti na temelju članka 9. i Priloga 1. PACE-u iz 1984. za Englesku i Wales te članka 10. i dalje Uredbe o policiji i kaznenim dokazima (Sjeverna Irska) iz 1989. za Sjevernu Irsku. Za Škotsku se izvodi iz precedentnog prava (vidjeti članak 46. Zakona o kaznenom pravosuđu (Škotska) iz 2016. i članak 23.B Kaznenog zakona (konsolidirano) (Škotska)). Tijela Ujedinjene Kraljevine pojasnila su da se nalogom za dostavljanje od osobe navedene u tom nalogu zahtijeva da dostavi ili omogući pristup materijalu u njezinu posjedu ili pod njezinom kontrolom (vidjeti točku 4. Priloga 1. PACE-u iz 1984.).

([184]) Na primjer, u člancima 8. i 18. PACE-a iz 1984. nalaze se ovlasti za zapljenu i zadržavanje svega za što je pretraga odobrena.

kontrolom. Podnositelj zahtjeva mora sudu opravdati zašto je nalog za pretragu ili nalog za dostavljanje nužan te zašto je u javnom interesu. Nekoliko je zakonskih ovlasti koje dopuštaju izdavanje naloga za pretragu i naloga za dostavljanje. Svaka odredba povezana je sa zakonski utvrđenim uvjetima koji se moraju ispuniti da bi se izdao nalog za pretragu ([185]) ili dostavljanje ([186]).

(138) Nalozi za dostavljanje i nalozi za pretragu mogu se osporiti sudskim preispitivanjem ([187]). Kad je riječ o zaštitnim mjerama, sva tijela kaznenog progona obuhvaćena područjem primjene dijela 3. DPA-a iz 2018. mogu pristupiti osobnim podacima, što je oblik obrade, samo u skladu s načelima i zahtjevima utvrđenima u DPA-u iz 2018. (vidjeti prethodne uvodne izjave 122. i 124.). Stoga bi

([185]) Na primjer, u članku 8. PACE-a regulira se ovlast mirovnog suca (*justice of the peace*) da odobri nalog za pretragu, a u članku 18. ovlast policijskog službenika da pretraži određene prostore. U prvom slučaju (članak 8.), da bi izdao nalog za pretragu, mirovni sudac mora biti uvjeren da postoje opravdani razlozi da vjeruje sljedeće: i. počinjeno je kazneno djelo; ii. u prostorima je prisutan materijal koji će vjerojatno biti vrlo važan (samostalno ili zajedno s drugim materijalima) za istragu kaznenog djela; iii. materijal je vjerojatno relevantan dokaz; iv. ne sastoji se i ne uključuje elemente na koje se primjenjuje odvjetnička tajna, isključeni materijal (*excluded material*) ili materijal u okviru posebnog postupka (*special procedure material*); i v. ne bi bilo moguće ući u prostore bez upotrebe naloga. U drugom slučaju člankom 18. policijskom službeniku dopušta se da pretraži prostore osobe uhićene za kazneno djelo kako bi pronašao materijal, osim materijala na koji se primjenjuje odvjetnička tajna, ako ima opravdane razloge za sumnju da se u prostorima nalaze dokazi koji su povezani s tim kaznenim djelom ili drugim sličnim ili povezanim kaznenim djelom. Takva pretraga mora biti ograničena na otkrivanje tog materijala i u pisanom je obliku mora odobriti policijski službenik koji ima barem čin inspektora, osim ako je pretraga potrebna za istragu kaznenog djela. U tom se slučaju nakon pretrage mora što prije obavijestiti policijskog službenika koji ima barem čin inspektora. Moraju se evidentirati razlozi za pretragu i dokazno sredstvo koje se traži. Nadalje, u člancima 15. i 16. PACE-a iz 1984. zakonski su utvrđene zaštitne mjere koje se moraju poštovati kada se podnosi zahtjev za nalog za pretragu. U članku 15. navedeni su zahtjevi primjenjivi na dobivanje naloga za pretragu (uključujući sadržaj zahtjeva koji podnosi policijski službenik i činjenicu da se u nalogu mora navesti, među ostalim, propis na temelju kojeg se nalog izdaje te se u najvećoj mogućoj mjeri moraju identificirati predmeti i osobe koji se traže u prostorima koje treba pretražiti). Članak 16. regulira način na koji se mora provoditi pretraga na temelju naloga (na primjer: u članku 16. stavku 5. predviđa se da službenik koji izvršava nalog stanaru dâ primjerak naloga za pretragu, u članku 16. stavku 11. zahtijeva se da se nalog nakon izvršenja čuva 12 mjeseci, člankom 16. stavkom 12. stanaru se daje pravo da u tom razdoblju pregleda nalog ako želi). Ti članci pomažu osigurati usklađenost s člankom 8. Europske konvencije o ljudskim pravima (vidjeti, na primjer, predmet *Kent Pharmaceuticals protiv Director of the Serious Fraud Office* [2002] EWHC 3023 (QB) at [30] by Lord Woolf CJ). Ako se ne poštuju te zaštitne mjere, pretraga se može proglasiti nezakonitom (primjeri uključuju *R (Brook) protiv Preston Crown Court* [2018] EWHC 2024 (Admin), [2018] ACD 95; *R (Superior Import / Export Ltd) protiv Revenue and Customs Commissioners* [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115; *R (F) protiv Blackfriars Crown Court* [2014] EWHC 1541 (Admin)). Članci 15. i 16. PACE-a iz 1984. dopunjeni su Kodeksom B PACE-a, kodeksom dobre prakse koji regulira izvršavanje policijskih ovlasti za pretraživanje prostora.

([186]) Na primjer, kad se izdaje nalog za dostavljanje na temelju Zakona o oduzimanju nezakonito stečene imovine iz 2002., osim što je potrebna opravdana osnova kako bi se ispunili uvjeti utvrđeni u članku 346. stavku 2. tog zakona, potreban je i opravdan razlog za vjerovanje da osoba posjeduje ili ima pod kontrolom navedeni materijal i da je materijal vjerojatno vrlo važan. Još jedan zahtjev za izdavanje naloga za dostavljanje postojanje je opravdanog razloga za vjerovanje da je u javnom interesu da se materijal nabavi ili da mu se omogući pristup uzimajući u obzir (a) vjerojatnu korist za istragu ako se materijal nabavi i (b) okolnosti u kojima osoba, za koju je u zahtjevu navedeno da vjerojatno posjeduje ili ima pod kontrolom materijal, drži svoje informacije. Slično tome, sud koji razmatra zahtjev za nalog za dostavljanje na temelju Priloga 1. PACE-u iz 1984. mora se uvjeriti da su ispunjeni specifični uvjeti. Točnije, u Prilogu 1. PACE-u utvrđene su dvije zasebne skupine uvjeta, a jedna od njih mora biti ispunjena da bi sudac mogao izdati nalog za dostavljanje. Prva skupina zahtijeva da sudac zbog opravdanog razloga vjeruje: i. da je počinjeno kazneno djelo, ii. da se materijal koji se traži u prostorima sastoji od ili uključuje materijal u okviru posebnog postupka, ali ne isključeni materijal, iii. da će materijal vjerojatno biti vrlo važan za istragu, samostalno ili zajedno s drugim materijalima, iv. da je materijal vjerojatno relevantan dokaz, v. da se do materijala pokušalo doći na drugi način ili da se to nije pokušalo jer drugi načini sigurno ne bi bili uspješni; i vi. nakon što je uzeo uz obzir korist za istragu i okolnosti u kojima pojedinac posjeduje materijal, da je u javnom interesu da se materijal nabavi ili da mu se omogući pristup. Druga skupina uvjeta zahtijeva: ii. da se u prostorima nalazi materijal koji se sastoji od materijala u okviru posebnog postupka ili isključenog materijala, ii. da nije bilo zabrane pretrage koja se provodi na temelju propisa donesenih prije PACE-a za materijal u okviru posebnog postupka, isključeni materijal ili materijal pod odvjetničkom tajnom, mogao bi se izdati nalog za pretragu materijala; i iii. to bi bilo primjereno.

([187]) Sudsko preispitivanje je pravni postupak kojim se odluke javnog tijela mogu osporiti pred Visokim sudom. Sudovi „preispituju" odluku koja se osporava i odlučuju može li se tvrditi da je odluka pravno manjkava ako se uzmu u obzir koncepti/načela javnog prava. Glavne su osnove za sudsko preispitivanje nezakonitost, nerazumnost, postupovna nepravilnost, legitimna očekivanja i ljudska prava. Nakon uspješnog sudskog preispitivanja sud može naložiti nekoliko pravnih lijekova, a najčešće je rješenje o ukidanju (kojim se ukida ili poništava izvorna odluka, tj. odluka o izdavanju naloga za pretragu), a u nekim okolnostima to može uključivati i financijsku naknadu. Dodatne pojedinosti o sudskom preispitivanju u Ujedinjenoj Kraljevini dostupne su u publikaciji *Judge Over Your Shoulder – a guide to good decision-making* (Razmišljanje suca – vodič za dobro odlučivanje) Pravnog odjela Vlade (*Government Legal Department*), dostupnoj na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf

zahtjev koji podnese bilo koje tijelo kaznenog progona trebao biti u skladu s načelom prema kojem svrhe obrade moraju biti posebne, izričite i zakonite ([188]) te prema kojem osobni podaci koje obrađuje nadležno tijelo moraju biti relevantni za tu svrhu i ne smiju biti pretjerani ([189]).

3.2.1.2. Istražne ovlasti za potrebe kaznenog progona

(139) U svrhu sprečavanja ili otkrivanja samo teških kaznenih djela ([190]) određena tijela kaznenog progona, primjerice Nacionalna agencija za kriminal ili načelnik policije ([191]), mogu se koristiti ciljanim istražnim ovlastima na temelju IPA-e iz 2016. U tom će se slučaju zaštitne mjere predviđene u okviru IPA-e iz 2016. primjenjivati uz zaštitne mjere predviđene u dijelu 3. DPA-a iz 2018. Ta tijela kaznenog progona mogu se osloniti na sljedeće posebne istražne ovlasti: ciljano presretanje (dio 2. IPA-e iz 2016.), pribavljanje podataka o komunikacijama (dio 3. IPA-e iz 2016.), zadržavanje podataka o komunikacijama (dio 4. IPA-e iz 2016.) i ciljano ometanje opreme (dio 5. IPA-e iz 2016.). Presretanje obuhvaća pribavljanje sadržaja komunikacije ([192]), dok svrha pribavljanja i zadržavanja podataka o komunikacijama nije dobivanje sadržaja komunikacije, već podataka o sudionicima, vremenu, mjestu i načinu komunikacije. To obuhvaća, na primjer, vrijeme i trajanje komunikacije, telefonski broj ili e-adresu pošiljatelja i primatelja komunikacije, a ponekad i lokaciju uređaja putem kojih se komunicira, pretplatnika telefonske usluge ili račun s detaljnim ispisom ([193]). Ometanje opreme niz je tehnika za dobivanje različitih podataka s opreme, koja uključuje računala, tablete i pametne telefone te kabele, žice i uređaje za pohranu ([194]).

(140) Ovlasti ciljanog presretanja mogu se koristiti i kad je to „potrebno u svrhu provođenja odredbi instrumenta uzajamne pomoći EU-a ili međunarodnog sporazuma o uzajamnoj pomoći" (takozvani „nalog za uzajamnu pomoć" ([195])). Nalozi za uzajamnu pomoć daju se samo za presretanje, ali ne i za pribavljanje podataka o komunikacijama ili ometanje opreme. Te su ciljane ovlasti uređene Zakonom o istražnim ovlastima iz 2016. (IPA iz 2016.) ([196]), koji zajedno sa Zakonom o regulaciji istražnih ovlasti iz 2000. (RIPA) za Englesku, Wales i Sjevernu Irsku te Zakonom o regulaciji istražnih ovlasti (Škotska) iz 2000. (RIPSA) za Škotsku čini pravnu osnovu i određuje primjenjiva ograničenja i zaštitne mjere za upotrebu takvih ovlasti. U IPA-i iz 2016. predviđen je i sustav za upotrebu masovnih istražnih ovlasti, ali one nisu dostupne tijelima kaznenog progona (mogu ih koristiti samo obavještajne agencije) ([197]).

([188]) Članak 36. stavak 1. DPA-a Ujedinjene Kraljevine iz 2018.

([189]) Članak 37. DPA-a Ujedinjene Kraljevine iz 2018.

([190]) U članku 263. stavku 1. IPA-e iz 2016. navedeno je da „teško kazneno djelo" znači kazneno djelo za koje je opravdano očekivati da će odrasla osoba bez prijašnjih osuda biti osuđena na kaznu zatvora od tri godine ili više ili radnja koja uključuje nasilje, dovodi do velike financijske koristi ili je riječ o radnji velikog broja osoba. Nadalje, u svrhu pribavljanja podataka o komunikacijama na temelju dijela 4. IPA-e iz 2016., u članku 87. stavku 10.B navedeno je da „teško kazneno djelo" znači kazneno djelo za koje se može izreći kazna zatvora od 12 mjeseci ili više ili kazneno djelo koje počini osoba koja nije pojedinac ili koje kao sastavni dio uključuje slanje komunikacije ili povredu privatnosti osobe.

([191]) Konkretno, nalog za ciljano presretanje mogu tražiti sljedeća tijela kaznenog progona: glavni direktor Nacionalne agencije za kriminal (*National Crime Agency*), načelnik Metropolske policije, šef Policijske službe Sjeverne Irske, šef Policijske službe Škotske, Porezna i carinska uprava Ujedinjene Kraljevine, šef Obrambene obavještajne agencije (*Defence Intelligence*) i osoba koja je nadležno tijelo zemlje ili područja izvan Ujedinjene Kraljevine za potrebe instrumenta uzajamne pomoći EU-a ili međunarodnog sporazuma o uzajamnoj pomoći (članak 18. stavak 1. IPA-e iz 2016.).

([192]) Vidjeti članak 4. IPA-e iz 2016.

([193]) Vidjeti članak 261. stavak 5. IPA-e iz 2016. i Kodeks dobre prakse za masovno pribavljanje podataka o komunikacijama, dostupan na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, točka 2.9.

([194]) Kodeks dobre prakse za ometanje opreme dostupan je na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, točka 2.2.

([195]) Nalozi za uzajamnu pomoć ovlašćuju tijelo Ujedinjene Kraljevine da pomogne tijelu izvan državnog područja Ujedinjene Kraljevine pri presretanju i otkrivanju materijala koji se presreće takvom tijelu u skladu s međunarodnim instrumentom uzajamne pomoći (članak 15. stavak 4. IPA-e iz 2016.).

([196]) Zakon o istražnim ovlastima iz 2016. (vidjeti: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) zamijenio je više zakona o presretanju komunikacija, ometanju opreme i pribavljanju podataka o komunikacijama, osobito dio I. RIPA-e iz 2000. koji je prethodno bio opći zakonodavni okvir za upotrebu istražnih ovlasti tijela kaznenog progona i tijela nacionalne sigurnosti.

([197]) Članak 138. stavak 1., članak 158. stavak 1., članak 178. stavak 1., članak 199. stavak 1. IPA-e iz 2016.

(141) Kako bi izvršavala te ovlasti, nadležna tijela moraju dobiti nalog ([198]) koji izdaje nadležno tijelo ([199]), a odobrava neovisni pravosudni povjerenik (*judicial commissioner*) ([200]) (takozvani „postupak dvostruke zaštite"). Da bi se dobio taj nalog, moraju se provjeriti nužnost i proporcionalnost ([201]). Budući da su te ciljane istražne ovlasti predviđene IPA-om iz 2016. iste kao i one dostupne nacionalnim sigurnosnim agencijama, uvjeti, ograničenja i zaštitne mjere primjenjivi na te ovlasti detaljno su opisani u odjeljku o pristupu tijela javne vlasti Ujedinjene Kraljevine osobnim podacima i njihovoj uporabi za potrebe nacionalne sigurnosti (vidjeti uvodnu izjavu 177. i dalje).

3.2.2. *Daljnja uporaba prikupljenih informacija*

(142) Razmjena podataka tako da ih tijelo kaznenog progona šalje drugom tijelu u svrhe u koje podaci nisu prvotno prikupljeni (tzv. „daljnja razmjena") podložno je određenim uvjetima.

(143) Slično odredbama članka 4. stavka 2. Direktive (EU) 2016/680, člankom 36. stavkom 3. DPA-a iz 2018. određeno je da je daljnja obrada (bilo da je obavlja prvotni ili neki drugi voditelj obrade) osobnih podataka koje je prikupilo nadležno tijelo u svrhu kaznenog progona dopuštena za bilo koju drugu svrhu kaznenog progona ako je voditelj obrade zakonski ovlašten za obradu u drugu svrhu te ako je obrada nužna i proporcionalna toj svrsi ([202]). U tom se slučaju sve zaštitne mjere predviđene dijelom 3. DPA-a iz 2018., na koji se upućuje u uvodnim izjavama 122. i 124., primjenjuju na obradu koju obavlja tijelo primatelj.

(144) U pravnom poretku Ujedinjene Kraljevine više zakona izričito dopušta takvu daljnju razmjenu. Točnije, i. Zakon o digitalnom gospodarstvu iz 2017. dopušta razmjenu podataka između tijela javne vlasti u nekoliko svrha, na primjer u slučaju svih prijevara na štetu javnog sektora koje bi uključivale gubitak ili rizik od gubitka za tijela javne vlasti ([203]) ili u slučaju duga prema tijelu javne vlasti ili Kruni ([204]), ii. Zakon o kaznenim djelima i sudovima iz 2013. dopušta razmjenu informacija s Nacionalnom agencijom za kriminal (NCA) ([205]) u svrhu suzbijanja, istrage i kaznenog progona teških kaznenih djela i organiziranog kriminala, iii. Zakon o teškim kaznenim djelima iz 2007. dopušta tijelima javne vlasti da otkriju informacije organizacijama za borbu protiv prijevara za potrebe sprečavanja prijevara ([206]).

(145) U tim je zakonima izričito predviđeno da bi razmjena informacija trebala biti u skladu s načelima određenima u DPA-u iz 2018. Osim toga, Nacionalna agencija za policiju (*College of Policing*) izdala je odobrenu profesionalnu praksu za razmjenu informacija ([207]) kako bi pomogla policiji da ispuni

([198]) U dijelu 2. poglavlju 2. IPA-e iz 2016. predviđen je određeni broj slučajeva u kojima je presretanje moguće bez naloga. To uključuje: presretanje uz privolu pošiljatelja ili primatelja, presretanje u administrativne ili izvršne svrhe, presretanje u određenim institucijama (zatvori, psihijatrijske bolnice i ustanove za zadržavanje imigranata) te presretanje koje se provodi u skladu s relevantnim međunarodnim sporazumom.

([199]) U većini slučajeva naloge na temelju IPA-e iz 2016. izdaje ministar, dok su škotski ministri ovlašteni izdavati naloge za ciljano presretanje, naloge za uzajamnu pomoć i naloge za ciljano ometanje opreme ako se osobe ili prostori koje treba presresti i oprema koja se ometa nalaze u Škotskoj (vidjeti članke 22. i 103. IPA-e iz 2016.). U slučaju ciljanog ometanja opreme načelnik za kazneni progon (*law enforcement chief*) (opisan u dijelovima 1. i 2. Priloga 6. IPA-i iz 2016.) može izdati nalog na temelju uvjetâ iz članka 106. IPA-e iz 2016.

([200]) Pravosudni povjerenici pomažu povjereniku za istražne ovlasti (IPC), neovisnom tijelu koje izvršava funkcije nadzora nad istražnim ovlastima koje primjenjuju obavještajne agencije (za više pojedinosti vidjeti uvodnu izjavu 162. i dalje).

([201]) Osobito vidjeti članke 19. i 23. IPA-e iz 2016.

([202]) Članak 36. stavak 3. DPA-a iz 2018.

([203]) Članak 56. Zakona o digitalnom gospodarstvu iz 2017., dostupan na: https://www.legislation.gov.uk/ukpga/2017/30/section/56

([204]) Članak 48. Zakona o digitalnom gospodarstvu iz 2017.

([205]) Članak 7. Zakona o kaznenim djelima i sudovima iz 2013., dostupan na: https://www.legislation.gov.uk/ukpga/2013/22/section/7

([206]) Članak 68. Zakona o teškim kaznenim djelima iz 2007., dostupan na: https://www.legislation.gov.uk/ukpga/2007/27/contents

([207]) Odobrena profesionalna praksa za razmjenu informacija, dostupna na: https://www.app.college.police.uk/app-content/information-management/sharing-police-information

svoje obveze u pogledu zaštite podataka na temelju Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, DPA-a i Zakona o ljudskim pravima iz 1998. Usklađenost razmjene s primjenjivim pravnim okvirom za zaštitu podataka obvezno podliježe sudskom preispitivanju ([208]).

(146) Nadalje, slično odredbama članka 9. Direktive (EU) 2016/680, u DPA-u iz 2018. predviđeno je da se osobni podaci prikupljeni u bilo koju svrhu kaznenog progona mogu obrađivati u svrhu koja nije kazneni progon ako je obrada odobrena pravom ([209]).

(147) Ta vrsta razmjene obuhvaća dva scenarija: 1. tijelo kaznenog progona razmjenjuje podatke s tijelom za izvršavanje zakonodavstva koje se ne bavi kaznenim progonom osim obavještajne agencije (na primjer, financijsko ili porezno tijelo, tijelo za tržišno natjecanje, ured za skrb o mladima itd.) i 2. tijelo kaznenog progona razmjenjuje podatke s obavještajnom agencijom. U prvom scenariju obrada osobnih podataka bit će obuhvaćena područjem primjene Opće uredbe o zaštiti podataka Ujedinjene Kraljevine te dijela 2. DPA-a iz 2018. Komisija je procijenila zaštitne mjere predviđene Općom uredbom o zaštiti podataka Ujedinjene Kraljevine te dijelom 2. DPA-a iz 2018. u uvodnim izjavama od 12. do 111. i zaključila je da Ujedinjena Kraljevina osigurava primjerenu razinu zaštite osobnih podataka koji se prenose iz Europske unije u Ujedinjenu Kraljevinu u okviru područja primjene Uredbe (EU) 2016/679.

(148) U drugom scenariju, u kojem je riječ o razmjeni podataka koje je prikupilo tijelo kaznenog progona s obavještajnom agencijom za potrebe nacionalne sigurnosti, pravna osnova koja omogućuje takvu razmjenu je članak 19. Zakona o borbi protiv terorizma iz 2008. (CTA iz 2008.) ([210]). Na temelju tog zakona sve osobe mogu dati informacije bilo kojoj obavještajnoj službi u svrhu obavljanja bilo koje funkcije te službe, uključujući „nacionalnu sigurnost".

(149) Kad je riječ o uvjetima pod kojima se podaci mogu razmjenjivati u svrhe nacionalne sigurnosti, Zakon o obavještajnim službama ([211]) i Zakon o sigurnosnim službama ([212]) ograničavaju mogućnost obavještajnih službi da prikupljaju podatke na ono što je nužno za obavljanje njihovih zakonski propisanih funkcija. Tijela kaznenog progona koja žele razmijeniti podatke s obavještajnim službama morat će uzeti u obzir nekoliko čimbenika/ograničenja povrh zakonski propisanih funkcija tijela koje su utvrđene u Zakonu o obavještajnim službama i Zakonu o sigurnosnim službama ([213]). U članku 20. Zakona o borbi protiv terorizma iz 2008. pojašnjava se da sve razmjene podataka na temelju članka 19. i dalje moraju biti u skladu sa zakonodavstvom o zaštiti podataka, što znači da se primjenjuju sva ograničenja i zahtjevi iz dijela 3. DPA-a iz 2018. Nadalje, budući da su nadležna tijela tijela javne vlasti za potrebe Zakona o ljudskim pravima iz 1998., moraju djelovati u skladu s pravima iz Konvencije, uključujući članak 8. EKLJP-a. Ta ograničenja osiguravaju da su sve razmjene podataka između tijela kaznenog progona i obavještajnih službi usklađene sa zakonodavstvom o zaštiti podataka i EKLJP-om.

([208]) Na primjer, vidjeti predmet *M, R protiv the Chief Constable of Sussex Police* [2019] EWHC 975 (Admin), u kojem se od Visokog suda tražilo da preispita razmjenu podataka između policije i Partnerstva za smanjenje gospodarskog kriminala (BCRP), organizacije koja je ovlaštena upravljati programima obavijesti o isključenju, kojima se osobama zabranjuje da uđu u poslovne prostore članova tog partnerstva. Sud je preispitao razmjenu podataka, koja se odvijala na temelju sporazuma čija je svrha bila zaštita javnosti i sprečavanje kaznenih djela, te je naposljetku zaključio da je većina aspekata razmjene podataka bila zakonita, osim određenih osjetljivih informacija koje su policija i BCRP međusobno dijelili. Drugi je primjer predmet *Cooper protiv NCA* [2019] EWCA Civ 16 u kojem je Žalbeni sud (*Court of Appeal*) potvrdio zakonitost razmjene podataka između policije i Agencije za borbu protiv teškog organiziranog kriminala (*Serious Organised Crime Agency*, SOCA), tijela kaznenog progona koje je trenutačno dio Nacionalne agencije za kriminal.

([209]) Članak 36. stavak 4. DPA-a iz 2018.

([210]) Zakon o borbi protiv terorizma iz 2008., dostupan na: https://www.legislation.gov.uk/ukpga/2008/28/section/19

([211]) Zakon o obavještajnim službama iz 1994., dostupan na: https://www.legislation.gov.uk/ukpga/1994/13/contents

([212]) Zakon o sigurnosnim službama iz 1989., dostupan na: https://www.legislation.gov.uk/ukpga/1989/5/contents

([213]) U članku 2. stavku 2. Zakona o obavještajnim službama iz 1994. navedeno je: „Šef obavještajne službe odgovoran je za učinkovitost te službe i njegova je dužnost osigurati: (a) da su uspostavljeni mehanizmi koji osiguravaju da obavještajna služba nabavlja samo podatke koji su nužni za pravilno obavljanje njezinih funkcija i da informacije otkriva samo ako je to nužno: i. u tu svrhu; ii. u interesu nacionalne sigurnosti; iii. u svrhu sprečavanja ili otkrivanja teških kaznenih djela; ili iv. za potrebe kaznenih postupaka; i (b) da obavještajna služba ne poduzima nikakve mjere radi promicanja interesa neke političke stranke u Ujedinjenoj Kraljevini", dok je u članku 2. stavku 2. Zakona o sigurnosnim službama iz 1989. navedeno: „Glavni direktor odgovoran je za učinkovitost službe i njegova je dužnost osigurati: (a) da su uspostavljeni mehanizmi koji osiguravaju da služba nabavlja samo podatke koji su nužni za pravilno obavljanje njezinih funkcija i da ih otkriva samo ako je to nužno u tu svrhu ili u svrhu [sprečavanja ili otkrivanja] teških kaznenih djela [ili za potrebe kaznenih postupaka]; i (b) da služba ne poduzima nikakve mjere radi promicanja interesa neke političke stranke; i (c) da su uspostavljeni mehanizmi, dogovoreni s glavnim direktorom Nacionalne agencije za kriminal, za koordinaciju aktivnosti službe usmjerenih na ostvarivanje članka 1. stavka 4. ovog Zakona s aktivnostima policijskih snaga, Nacionalne agencije za kriminal i drugih tijela kaznenog progona".

(150) Ako nadležno tijelo namjerava dijeliti osobne podatke obrađene na temelju dijela 3. DPA-a iz 2018. s tijelima kaznenog progona treće zemlje, primjenjuju se posebni zahtjevi ([214]). Točnije, takvi su prijenosi mogući ako se temelje na uredbama o primjerenosti koje je donio ministar ili, ako takve uredbe ne postoje, ako se osiguraju odgovarajuće zaštitne mjere. U članku 75. DPA-a iz 2018. navedeno je da su uspostavljene odgovarajuće zaštitne mjere ako su utvrđene pravnim instrumentom koji obvezuje predviđenog primatelja ili ako voditelj obrade, nakon što procijeni sve okolnosti povezane s prijenosima te vrste osobnih podataka trećoj zemlji ili međunarodnoj organizaciji, zaključi da postoje odgovarajuće zaštitne mjere za zaštitu podataka.

(151) Ako se prijenos ne temelji na uredbi o primjerenosti ili odgovarajućim zaštitnim mjerama, moguć je samo u nekim određenim okolnostima, takozvanim „posebnim okolnostima" ([215]). To su slučajevi u kojima je prijenos nužan: (a) kako bi se zaštitili vitalni interesi ispitanika ili druge osobe, (b) kako bi se zaštitili legitimni interesi ispitanika, (c) za sprečavanje neposredne i ozbiljne prijetnje javnoj sigurnosti države članice ili treće zemlje, (d) u pojedinačnim slučajevima u neku od svrha kaznenog progona; ili (e) u pojedinačnim slučajevima u pravnu svrhu (na primjer, u vezi sa sudskim postupkom ili radi dobivanja pravnog savjeta). Potrebno je napomenuti da se točke (d) i (e) ne primjenjuju ako prava i slobode ispitanika nadilaze javni interes za prijenos. Ta skupina okolnosti odgovara posebnim situacijama i uvjetima koji predstavljaju „odstupanja" na temelju članka 38. Direktive (EU) 2016/680.

(152) Nadalje, IPA-om iz 2016. uvedene su dodatne zaštitne mjere kad se materijal koji su tijela kaznenog progona pribavila na temelju naloga kojim je odobreno presretanje ili ometanje opreme predaje trećoj zemlji. Točnije, takvo otkrivanje definirano kao „otkrivanje stranim tijelima" dopušteno je samo ako tijelo koje izdaje nalog smatra da su uspostavljene posebne odgovarajuće zaštitne mjere koje ograničavaju broj osoba kojima se podaci otkrivaju, opseg u kojem se neki materijal otkriva ili stavlja na raspolaganje te opseg u kojem se neki materijal kopira i broj izrađenih primjeraka. Osim toga, tijelo koje izdaje nalog može smatrati da su potrebni odgovarajući mehanizmi kako bi se osiguralo da se svaki primjerak bilo kojeg dijela tog materijala uništi čim više ne bude relevantnih razloga za njegovo zadržavanje (ako se ne uništi ranije) ([216]).

(153) Naposljetku, specifičan oblik daljnjih prijenosa iz Ujedinjene Kraljevine Sjedinjenim Američkim Državama u budućnosti bi se mogao odvijati na temelju Sporazuma između Vlade Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske i Vlade Sjedinjenih Američkih Država o pristupu elektroničkim podacima u svrhu sprečavanja teških kaznenih djela („Sporazum između Ujedinjene Kraljevine i SAD-a" ili „Sporazum") ([217]), koji je sklopljen u listopadu 2019. ([218]) Iako Sporazum između Ujedinjene Kraljevine i SAD-a u trenutku donošenja ove Odluke još nije stupio na snagu, njegovo skoro stupanje na snagu moglo bi utjecati na daljnje prijenose SAD-u podataka koji su prvo preneseni Ujedinjenoj Kraljevini na temelju ove Odluke. Točnije, na podatke prenesene iz EU-a pružateljima usluga u Ujedinjenoj Kraljevini mogli bi se primjenjivati nalozi za dostavljanje elektroničkih dokaza koje izdaju nadležna tijela kaznenog progona u SAD-u te bi oni na temelju tog sporazuma postali primjenjivi u Ujedinjenoj Kraljevini kad Sporazum stupi na snagu. Zbog toga je za ovu Odluku važno procijeniti uvjete i zaštitne mjere koji se moraju ispuniti da bi se takvi nalozi mogli izdati i izvršiti.

([214]) Vidjeti dio 3. poglavlje 5. DPA-a iz 2018.

([215]) Članak 76. DPA-a iz 2018.

([216]) Članci 54. i 130. IPA-e iz 2016. Tijela koja izdaju nalog moraju uzeti u obzir potrebu za uvođenjem posebnih zaštitnih mjera za materijal koji se predaje stranim tijelima kako bi se osiguralo da su podaci zaštićeni u smislu zadržavanja, uništavanja i otkrivanja, a te su zaštitne mjere slične onima iz članaka 53. i 129. IPA-e iz 2016.

([217]) Sporazum između Vlade Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske i Vlade Sjedinjenih Američkih Država o pristupu elektroničkim podacima u svrhu sprečavanja teških kaznenih djela, dostupan na: 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]) To je prvi sporazum donesen na temelju američkog Zakona o objašnjenju zakonite prekomorske uporabe podataka (CLOUD). Zakon CLOUD je američki savezni zakon donesen 23. ožujka 2018. i u njemu se, izmjenom Zakona o pohranjenoj komunikaciji iz 1986., pojašnjava da pružatelji usluga u SAD-u moraju poštovati naloge SAD-a da otkriju podatke o sadržaju i podatke koji se ne odnose na sadržaj, neovisno o tome gdje su takvi podaci pohranjeni. Zakon CLOUD omogućuje i sklapanje izvršnih sporazuma sa stranim vladama, na temelju kojih bi američki pružatelji usluga mogli isporučivati podatke o sadržaju izravno tim stranim vladama (tekst Zakona CLOUD dostupan je na: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

(154) Stoga je važno istaknuti, prvo, da je Sporazum primjenjiv samo na kaznena djela koja su kažnjiva kaznom zatvora u najduljem trajanju od najmanje tri godine (definirana kao „teška kaznena djela") ([219]), uključujući „terorističku aktivnost". Drugo, podaci obrađeni u drugoj jurisdikciji mogu se na temelju tog sporazuma dobiti samo nakon izdavanja „naloga […] koji podliježe preispitivanju ili nadzoru na temelju domaćeg prava stranke koja izdaje nalog, a koje obavlja sud, sudac ili drugo neovisno tijelo prije ili za vrijeme postupka koji se odnosi na izvršenje naloga" ([220]). Treće, svi se nalozi moraju „temeljiti na zahtjevima za opravdano obrazloženje koje se temelji na jasnim i vjerodostojnim činjenicama, posebnosti, zakonitosti i ozbiljnosti povezanima s ponašanjem koje se istražuje" ([221]) te moraju „biti usmjereni na specifične račune i identificirati specifičnu osobu, račun, adresu ili osobni uređaj ili neki drugi specifični identifikator" ([222]). Četvrto, podaci dobiveni na temelju tog sporazuma ostvaruju zaštitu ekvivalentnu posebnim zaštitnim mjerama predviđenima takozvanim „Krovnim sporazumom između EU-a i SAD-a" ([223]) – sveobuhvatnim sporazumom o zaštiti podataka koji su EU i SAD sklopili u prosincu 2016. i u kojem su utvrđene zaštitne mjere i prava primjenjivi na prijenose podataka u kontekstu suradnje u području kaznenog progona – a sve su te zaštitne mjere uključene u Sporazum između Ujedinjene Kraljevine i SAD-a upućivanjem *mutatis mutandis*, osobito kako bi se uzela u obzir posebna priroda prijenosâ (tj. prijenosi od privatnih subjekata tijelima kaznenog progona, a ne prijenosi među tijelima kaznenog progona) ([224]). U Sporazumu između Ujedinjene Kraljevine i SAD-a izričito je navedeno da će se zaštita ekvivalentna onoj koja je predviđena Krovnim sporazumom između EU-a i SAD-a primjenjivati „na sve osobne podatke koji nastanu pri izvršavanju naloga koji podliježu ovom Sporazumu kako bi se osigurala ekvivalentna zaštita" ([225]).

(155) Na podatke prenesene tijelima SAD-a na temelju Sporazuma između Ujedinjene Kraljevine i SAD-a stoga bi se trebala primjenjivati zaštita predviđena instrumentom prava Unije, uz nužne prilagodbe koje odražavaju prirodu prijenosa o kojima je riječ. Tijela Ujedinjene Kraljevine dalje su potvrdila da će se zaštita iz Krovnog sporazuma primjenjivati na sve osobne podatke koji nastanu ili se čuvaju na temelju Sporazuma, neovisno o prirodi i vrsti tijela koje podnosi zahtjev (npr. i savezna i državna tijela kaznenog progona u SAD-u), pa se ekvivalentna zaštita mora osigurati u svim slučajevima. Međutim, tijela Ujedinjene Kraljevine objasnila su i da Ujedinjena Kraljevina i SAD još raspravljaju o pojedinostima konkretne provedbe zaštitnih mjera za podatke. U kontekstu razgovora sa službama Europske komisije o ovoj Odluci tijela Ujedinjene Kraljevine potvrdila su da će dopustiti da Sporazum stupi na snagu tek nakon što se uvjere da je njegova provedba u skladu s predviđenim pravnim obvezama, uključujući jasnoću u pogledu usklađenosti sa standardima zaštite podataka za sve podatke koji se traže na temelju tog sporazuma. Budući da stupanje Sporazuma na snagu može utjecati na razinu zaštite koja je procijenjena u ovoj Odluci, Ujedinjena Kraljevina trebala bi Europskoj komisiji priopćiti sve informacije i daljnja pojašnjenja o načinu na koji će SAD ispunjavati svoje obveze na temelju Sporazuma čim oni budu dostupni, a u svakom slučaju prije stupanja na snagu Sporazuma, kako bi se osiguralo pravilno praćenje ove Odluke u skladu s člankom 45. stavkom 4. Uredbe (EU) 2016/679. Posebna pozornost posvetit će se primjeni i prilagodbi zaštite iz Krovnog sporazuma na posebnu vrstu prijenosa obuhvaćenu Sporazumom između Ujedinjene Kraljevine i SAD-a.

(156) Općenito, sve relevantne promjene u pogledu stupanja na snagu i primjene Sporazuma na odgovarajući će se način uzeti u obzir u kontekstu kontinuiranog praćenja ove Odluke, među ostalim s obzirom na nužne posljedice do kojih će doći u slučaju bilo kakvih naznaka da više nije osigurana razina zaštite koja je u načelu istovjetna.

3.2.3. *Nadzor*

(157) Ovisno o ovlastima koje nadležna tijela koriste pri obradi osobnih podataka za potrebe kaznenog progona (na temelju DPA-a iz 2018. ili IPA-e iz 2016.) različita tijela osiguravaju nadzor nad primjenom tih ovlasti. Konkretnije, povjerenik za informiranje nadzire obradu osobnih podataka kad je obuhvaćena područjem primjene dijela 3. DPA-a

([219]) Članak 1. stavak 14. Sporazuma.
([220]) Članak 5. stavak 2. Sporazuma.
([221]) Članak 5. stavak 1. Sporazuma.
([222]) Članak 4. stavak 5. Sporazuma. Dodatni i stroži standard primjenjuje se na presretanje u stvarnom vremenu: nalozi moraju imati ograničeno trajanje, koje ne smije biti dulje od onog koje je opravdano nužno za ostvarenje svrhe naloga, i izdaju se samo ako se iste informacije opravdano ne bi mogle dobiti na manje nametljiv način (članak 5. stavak 3. Sporazuma).
([223]) Sporazum između Sjedinjenih Američkih Država i Europske unije o zaštiti osobnih informacija u vezi sa sprečavanjem, istragom, otkrivanjem i progonom kaznenih djela, SL L 336, 10.12.2016., str. 3.–13., dostupan na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:22016A1210(01)&from=HR
([224]) Članak 9. stavak 1. Sporazuma.
([225]) Članak 9. stavak 1. Sporazuma.

iz 2018. ([226]) Neovisan i sudski nadzor nad primjenom istražnih ovlasti na temelju IPA-e iz 2016. osigurava Ured povjerenika za istražne ovlasti (IPCO) ([227]) (taj se dio razmatra u uvodnim izjavama od 250. do 255.). Osim toga, dodatni nadzor osiguravaju Parlament i druga tijela.

3.2.3.1. Nadzor nad dijelom 3. DPA-a iz 2018.

(158) Opće funkcije povjerenika za informiranje, čija su neovisnost i organizacija objašnjeni u uvodnoj izjavi 87., u vezi s obradom osobnih podataka koji su obuhvaćeni dijelom 3. DPA-a iz 2018., utvrđene su u Prilogu 13. DPA-u iz 2018. Glavne su zadaće Ureda povjerenika za informiranje praćenje i provedba dijela 3. DPA-a iz 2018., podizanje razine osviještenosti javnosti, savjetovanje Parlamenta, vlade i drugih institucija i tijela. Kako bi se sačuvala neovisnost pravosuđa, povjerenik za informiranje nije ovlašten izvršavati svoje funkcije u vezi s obradom osobnih podataka koju provodi pojedinac koji djeluje u sudbenom svojstvu ili sud u okviru svoje sudske nadležnosti. U tim bi okolnostima druga tijela izvršavala nadzorne funkcije, kako je objašnjeno u uvodnim izjavama od 99. do 103.

(159) Povjerenik ima opće istražne, korektivne i savjetodavne ovlasti te ovlasti za izdavanje odobrenja u vezi s obradom osobnih podataka na koje se odnosi dio 3. Konkretno, povjerenik ima ovlasti obavijestiti voditelja obrade ili izvršitelja obrade o navodnom kršenju dijela 3. DPA-a iz 2018., izdati upozorenja ili opomenu voditelju obrade ili izvršitelju obrade koji je prekršio odredbe dijela 3. tog zakona te na vlastitu inicijativu ili na zahtjev dati mišljenje Parlamentu, Vladi ili drugim institucijama i tijelima, kao i javnosti o svim pitanjima povezanima sa zaštitom osobnih podataka ([228]).

(160) Nadalje, povjerenik ima ovlasti izdavati zahtjeve za dostavu informacija ([229]), zahtjeve za provjeru ([230]) i zahtjeve za izvršenje ([231]) kao i ovlast pristupa dokumentima voditelja obrade ili izvršitelja obrade, pristupa njihovim prostorijama ([232]) i izricanja upravnih novčanih kazni u obliku rješenja o kazni ([233]). U okviru politike regulatornog djelovanja Ureda povjerenika za informiranje utvrđuju se okolnosti u kojima on izdaje zahtjeve za dostavu informacija, provjeru i izvršenje te rješenja o kazni ([234]) (vidjeti i uvodnu izjavu 93. i uvodne izjave 101. i 102. Direktive (EU) 2016/680 o odlukama o primjerenosti).

(161) Prema posljednjim godišnjim izvješćima (za 2018.–2019. ([235]), 2019.–2020. ([236])) povjerenica za informiranje provela je niz istraga i poduzela mjere izvršenja u pogledu obrade podataka koju provode tijela kaznenog progona. Na primjer, povjerenica je provela istragu i u listopadu 2019. objavila mišljenje u vezi s primjenom tehnologije prepoznavanja lica na javnim mjestima kojom se služe tijela kaznenog progona. Istraga je bila usmjerena, među ostalim, na uporabu tehnologije za prepoznavanje lica u stvarnom vremenu kojom se služe policija južnog Walesa i londonska Metropolska policija. Povjerenica za informiranje istražila je i „matricu za bande" ([237]) Metropolske policije i utvrdila niz teških kršenja zakona o zaštiti podataka koja bi mogla narušiti povjerenje javnosti u matricu i način na koji su podaci korišteni. U studenome 2018. povjerenica za informiranje izdala je zahtjev za izvršenje, a Metropolska policija potom je poduzela mjere potrebne za povećanje sigurnosti i odgovornosti te osiguravanje proporcionalnog korištenja podataka. Još jedan primjer mjere izvršenja u tom području jest novčana kazna od 325 000 GBP koju je povjerenica u svibnju 2018. izdala

([226]) Članak 116. DPA-a iz 2018.
([227]) Vidjeti IPA-u iz 2016., a posebno poglavlje 1. dio 8.
([228]) Točka 2. Priloga 13. DPA-u iz 2018.
([229]) Zahtjevi kojima se voditelju obrade i izvršitelju obrade (i u određenim okolnostima bilo kojoj drugoj osobi) nalaže da dostave potrebne informacije (članak 142. DPA-a iz 2018.).
([230]) Zahtjevi kojima se omogućuje provođenje istraga i revizije, kojima se od voditelja obrade ili izvršitelja obrade može zahtijevati da dopusti ulazak povjerenika u određene prostorije, provjeru ili pregled dokumenata ili opreme, razgovor s ljudima koji obrađuju osobne podatke u ime voditelja obrade (članak 146. DPA-a iz 2018.).
([231]) Obavijesti kojima se omogućuje izvršavanje korektivnih ovlasti kojima se od voditelja obrade/izvršitelja obrade zahtijeva da poduzmu određene mjere ili se suzdrže od njihova poduzimanja (članak 149. DPA-a iz 2018.).
([232]) Članak 154. DPA-a iz 2018.
([233]) Članak 155. DPA-a iz 2018.
([234]) Politika regulatornog djelovanja, vidjeti bilješku 96.
([235]) Godišnje izvješće i financijski izvještaji povjerenice za informiranje za 2018.–2019., vidjeti bilješku 101.
([236]) Godišnje izvješće i financijski izvještaji povjerenice za informiranje za 2019.–2020., vidjeti bilješku 82.
([237]) Baza podataka u kojoj su evidentirane obavještajne informacije o navodnim članovima banda i žrtvama kaznenih djela povezanih s bandama.

Državnom tužiteljstvu Ujedinjene Kraljevine (*Crown Prosecution Service*) zbog gubitka nešifriranih DVD-ova sa snimkama policijskih saslušanja. Povjerenica za informiranje provela je i istrage o širim temama, na primjer u prvoj polovini 2020. o izvlačenju podataka iz mobilnih telefona za potrebe policije i načinu na koji policija obrađuje podatke o žrtvama. Nadalje, povjerenica trenutačno istražuje predmet koji uključuje pristup tijela kaznenog progona podacima u posjedu subjekta iz privatnog sektora, Clearview AI Inc ([238]).

(162) Osim izvršnih ovlasti povjerenika za informiranje navedenih u uvodnim izjavama (160. i 161.), određena kršenja zakonodavstva o zaštiti podataka čine kaznena djela i stoga se na njih mogu primjenjivati kaznenopravne sankcije (članak 196. DPA-a iz 2018.). To se primjenjuje, na primjer, za prikupljanje, otkrivanje ili zadržavanje osobnih podataka bez pristanka voditelja obrade i omogućavanje otkrivanja osobnih podataka drugoj osobi bez pristanka voditelja obrade" ([239]), ponovnu identifikaciju anonimiziranih osobnih podataka bez pristanka voditelja obrade odgovornog za anonimizaciju osobnih podataka ([240]), namjerno ometanje povjerenika u izvršavanju njegovih ovlasti povezanih s pregledom osobnih podataka u skladu s međunarodnim obvezama ([241]), davanje lažnih izjava kao odgovor na zahtjev za dostavu informacija ili uništavanje informacija povezanih sa zahtjevima za dostavu informacija i provjeru ([242]).

3.2.3.2. Ostala nadzorna tijela u području kaznenog progona

(163) Osim povjerenika za informiranje postoji nekoliko nadzornih tijela u području kaznenog progona s posebnim mandatima važnima za pitanja zaštite podataka. To uključuje, na primjer, povjerenika za zadržavanje i uporabu biometrijskog materijala („povjerenik za biometrijske podatke") ([243]) i povjerenika za nadzorne kamere ([244]).

3.2.3.3. Parlamentarni nadzor u području kaznenog progona

(164) Posebni odbor za unutarnje poslove osigurava parlamentarni nadzor u području kaznenog progona. Odbor se sastoji od 11 zastupnika Parlamenta iz triju najvećih političkih stranaka. Odbor ima zadaću ispitati rashode, upravljanje i politiku Ministarstva unutarnjih poslova i povezanih javnih tijela, među ostalim policije i Nacionalne agencije za kriminal – čiji rad Odbor može posebno analizirati ([245]).

([238]) Vidjeti izjavu Ureda povjerenika za informiranje dostupnu na: 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]) Članak 170. DPA-a iz 2018.

([240]) Članak 171. DPA-a iz 2018.

([241]) Članak 119. stavak 6. DPA-a iz 2018.

([242]) U financijskoj godini koja obuhvaća razdoblje od 1. travnja 2019. do 31. ožujka 2020. nakon istraga koje je proveo Ured povjerenika za informiranje izdane su četiri opomene i pokrenuto je osam kaznenih postupaka. Kazneni progon u tim predmetima pokrenut je u skladu s člankom 55. Zakona o zaštiti podataka iz 1998., člankom 77. Zakona o slobodi informiranja iz 2000. i člankom 170. Zakona o zaštiti podataka iz 2018. Optuženici su u 75 % slučajeva priznali krivnju, zbog čega nisu bili potrebni dugotrajni postupci koji su često skupi. (Godišnje izvješće i financijski izvještaji povjerenice za informiranje za 2019.–2020., vidjeti bilješku 87., str. 40.).

([243]) Povjerenik za biometrijske podatke uspostavljen je na temelju Zakona o zaštiti sloboda (PoFA) iz 2012. (vidjeti: https://www.legislation.gov.uk/ukpga/2012/9/contents). Među ostalim funkcijama, povjerenik za biometrijske podatke odlučuje o tome može li policija čuvati evidencije o profilima DNK-a i otiske prstiju prikupljene od pojedinaca koji su uhićeni, ali nisu optuženi za teže kazneno djelo (članak 63.G PACE-a iz 1984.). Nadalje, povjerenik za biometrijske podatke ima opću dužnost da preispituje zadržavanje i korištenje DNK-a i otisaka prstiju te zadržavanje zbog razloga nacionalne sigurnosti (članak 20. stavak 2. Zakona o zaštiti sloboda iz 2012.). Povjerenik za biometrijske podatke imenuje se na temelju Kodeksa za javna imenovanja (Kodeks je dostupan na sljedećoj poveznici: https://www.gov.uk/government/publications/governance-code-for-public-appointments) i iz njegovih uvjeta imenovanja jasno je da ga ministar unutarnjih poslova može razriješiti dužnosti samo pod usko definiranim okolnostima; to uključuje neizvršavanje dužnosti u trajanju od tri mjeseca, osudu za kazneno djelo ili nepoštovanje uvjeta imenovanja.

([244]) Povjerenik za nadzorne kamere uspostavljen je Zakonom o zaštiti sloboda iz 2012. i uloga mu je da podupire usklađenost s Kodeksom dobre prakse za upotrebu nadzornih kamera, preispituje provedbu tog kodeksa i daje savjete ministrima ako smatra da je potrebna izmjena tog kodeksa. Povjerenik se imenuje prema istim pravilima kao i povjerenici za biometrijske podatke i ima slične ovlasti, resurse i zaštitu od razrješenja.

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

(165) Odbor u okviru svoje nadležnosti može odabrati vlastiti predmet istrage, uključujući posebne predmete, pod uvjetom da to pitanje nije predmet sudskog postupka. Odbor može i zatražiti pisane i usmene dokaze različitih relevantnih skupina i pojedinaca. Izrađuje izvješća o svojim zaključcima i daje preporuke Vladi ([246]). Očekuje se da Vlada odgovori na svaku preporuku iz izvješća, i to u roku od 60 dana ([247]).

(166) U području nadzora Odbor je sastavio i izvješće o Zakonu o regulaciji istražnih ovlasti iz 2000. (RIPA 2000.) ([248]), u kojem je utvrđeno da RIPA iz 2000. nije bila svrsishodna. Njegovo izvješće uzeto je u obzir pri izmjeni znatnih dijelova RIPA iz 2000. u okviru IPA-e donesene 2016. Potpun popis istraga nalazi se na internetskim stranicama Odbora ([249]).

(167) Zadaće Posebnog odbora za unutarnje poslove u Škotskoj obavlja Pravosudni pododbor za policiju, a u Sjevernoj Irskoj Odbor za pravosuđe ([250]).

3.2.4. *Sudska zaštita*

(168) Kad je riječ o obradi podataka koju provode tijela kaznenog progona, mehanizmi sudske zaštite dostupni su na temelju dijela 3. DPA-a iz 2018. i IPA-e iz 2016. te Zakona o ljudskim pravima iz 1998.

(169) Tim se mehanizmima ispitanicima osiguravaju djelotvorna sredstva upravne i sudske zaštite, što im prije svega omogućuje da ostvaruju svoja prava, uključujući pravo na pristup svojim osobnim podacima te ispravak ili brisanje tih podataka.

(170) Prvo, u skladu s člankom 165. DPA-a iz 2018. ispitanik može podnijeti pritužbu povjereniku za informiranje ako smatra da u vezi s osobnim podacima koji se odnose na njega postoji kršenje dijela 3. DPA-a iz 2018. ([251]) Povjerenik za informiranje ovlašten je ocijeniti usklađenost voditelja obrade i izvršitelja obrade s DPA-om iz 2018., zahtijevati od njih da poduzmu potrebne mjere u slučaju nepridržavanja i izreći novčane kazne.

([246]) Posebni odbori, uključujući Posebni odbor za unutarnje poslove, djeluju u skladu s Poslovnikom Zastupničkog doma. Poslovnik su pravila dogovorena u Zastupničkom domu kojima se uređuje poslovanje Parlamenta. Posebni odbori imaju široku nadležnost, a u članku 152. stavku 1. utvrđuje se da se „posebni odbori imenuju za ispitivanje rashoda, upravljanja i politike glavnih ministarstava, kako je navedeno u stavku 2. ovog naloga, i povezanih javnih tijela." Na temelju toga Posebni odbor za unutarnje poslove može preispitati svaku politiku Ministarstva unutarnjih poslova koja uključuje politike (i povezano zakonodavstvo) o istražnim ovlastima. Nadalje, u članku 152. stavku 4. jasno se navodi da odbori imaju različite ovlasti, uključujući mogućnost da od osoba zatraže dokaze ili dokumente o određenom pitanju te da sastavljaju izvješća. Trenutačne i prethodne istražne radnje Odbora dostupne su na: https://committees.parliament.uk/committee/83/home-affairs-committee/.

([247]) Ovlasti Posebnog odbora za unutarnje poslove u Engleskoj i Walesu navedene su u Poslovniku Zastupničkog doma koji je dostupan na: https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

([248]) Popis je dostupan na: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm.

([249]) Popis je dostupan na: https://committees.parliament.uk/committee/83/home-affairs-committee

([250]) Pravila Pravosudnog pododbora za policiju u Škotskoj dostupna su na: https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx, a pravila Odbora za pravosuđe u Sjevernoj Irskoj navedena su na: http://www.niassembly.gov.uk/assembly-business/standing-orders/

([251]) U posljednjem godišnjem izvješću Ureda povjerenika za informiranje nalazi se raščlamba zaprimljenih i zaključenih pritužbi prema vrsti. Konkretno, broj zaprimljenih pritužbi povezanih s „policijskom i kaznenom evidencijom" iznosi 6 % ukupnog broja primljenih pritužbi (povećanje od 1 % u odnosu na prethodnu financijsku godinu). Godišnje izvješće pokazuje i da pritužbe povezane sa zahtjevima za pristup ispitanika predstavljaju najveći broj (46 % od ukupnog broja pritužbi, odnosno povećanje od 8 % u odnosu na prethodnu financijsku godinu) (godišnje izvješće Ureda povjerenika za informiranje za razdoblje 2019.–2020., str. 55., vidjeti bilješku 88.).

(171) Drugo, DPA-om iz 2018. osigurava se pravo na korištenje pravnog lijeka protiv povjerenika za informiranje ako na odgovarajući način ne riješi pritužbu koju je podnio ispitanik. Točnije, ako povjerenik ne „preispita" ([252]) pritužbu koju je podnio ispitanik, podnositelj pritužbe ima pristup sudskom pravnom lijeku, odnosno može se obratiti Prvostupanjskom sudu ([253]), koji će naložiti povjereniku da poduzme odgovarajuće korake kao odgovor na pritužbu ili obavijesti podnositelja kako napreduje postupak povezan s pritužbom ([254]). Osim toga, svaka osoba koja od povjerenika dobije bilo koji od navedenih zahtjeva ili obavijesti (zahtjev za dostavu informacija, provjeru ili izvršenje ili rješenje o kazni) može podnijeti žalbu Prvostupanjskom sudu. Ako Sud smatra da odluka povjerenika nije u skladu sa zakonom ili da je povjerenik za informiranje trebao drukčije izvršavati svoje diskrecijske ovlasti, Sud mora prihvatiti žalbu ili zamijeniti zahtjev, rješenje ili odluku koju je povjerenik za informiranje izdao ili donio drugim zahtjevom, rješenjem ili odlukom ([255]).

(172) Treće, pojedinci mogu dobiti sudsku zaštitu protiv voditelja obrade i izvršitelja obrade izravno pred sudovima. Konkretno, na temelju članka 167. DPA-a iz 2018. ispitanik može podnijeti zahtjev sudu zbog kršenja njegova prava u skladu sa zakonodavstvom o zaštiti podataka, a sud može putem naloga od voditelja obrade zatražiti da poduzme bilo koji postupak u pogledu obrade (ili se suzdrži od poduzimanja takvog postupka) kako bi ispunio zahtjeve iz DPA-a iz 2018. Nadalje, u skladu s člankom 169. DPA-a iz 2018. svaka osoba koja je pretrpjela štetu zbog kršenja zahtjeva zakonodavstva o zaštiti podataka (uključujući dio 3. DPA-a iz 2018.), osim Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, ima pravo dobiti naknadu za tu štetu od voditelja obrade ili izvršitelja obrade, osim ako voditelj obrade ili izvršitelj obrade dokaže da ni na koji način nije odgovoran za događaj koji je prouzročio štetu. Šteta obuhvaća i financijski gubitak i štetu koja ne uključuje financijski gubitak, kao što je pretrpljena duševna bol.

(173) Naposljetku, svaka osoba koja smatra da je neko tijelo javne vlasti prekršilo njezina prava, uključujući pravo na privatnost i zaštitu podataka, može dobiti sudsku zaštitu pred sudovima Ujedinjene Kraljevine na temelju Zakona o ljudskim pravima iz 1998. ([256]), a nakon što iscrpe nacionalna pravna sredstva, osoba, nevladina organizacija i skupine pojedinaca mogu dobiti sudsku zaštitu pred Europskim sudom za ljudska prava za kršenja prava zajamčenih Europskom konvencijom o ljudskim pravima ([257]) (vidjeti u uvodnoj izjavi 111.).

3.2.4.1. Mehanizmi sudske zaštite dostupni na temelju IPA-e iz 2016.

(174) Pojedinci mogu dobiti sudsku zaštitu u slučaju kršenja IPA-e iz 2016. pred Sudom za istražne ovlasti (*Investigatory Powers Tribunal*). Oblici sudske zaštite dostupni na temelju IPA-e iz 2016. opisani su u uvodnim izjavama od 263. do 269. u nastavku.

([252]) U članku 166. DPA-a iz 2018. konkretno se navode sljedeće situacije: (a) povjerenik nije poduzeo odgovarajuće korake kako bi odgovorio na pritužbu; (b) povjerenik nije dostavio podnositelju pritužbe informacije o napretku ili ishodu pritužbe prije isteka roka od tri mjeseca koji počinje teći od dana kad je povjerenik primio pritužbu; ili (c) ako povjerenik u tom roku nije završio s ispitivanjem pritužbe te o tome nije obavijestio podnositelja pritužbe u narednom razdoblju od tri mjeseca.

([253]) Prvostupanjski sud je sud nadležan za rješavanje žalbi protiv odluka koje donose državna regulatorna tijela. Za odluke povjerenika za informiranje nadležno je Opće regulatorno vijeće (*General Regulatory Chamber*), koje je nadležno za cijelu Ujedinjenu Kraljevinu.

([254]) Članak 166. DPA-a iz 2018. Primjer uspješne tužbe protiv Ureda povjerenika za informiranje pred Sudom uključivao je predmet u kojem je Ured potvrdio primitak pritužbe ispitanika, ali nije naveo koje je mjere namjeravao poduzeti te mu je stoga naloženo da u roku od 21 kalendarskog dana potvrdi ima li namjeru ispitati pritužbe i, ako je to slučaj, obavijesti podnositelja pritužbe o napretku istrage najmanje svakih 21 kalendarskih dana (presuda još nije objavljena) i predmet u kojem je Prvostupanjski sud smatrao da nije jasno je li u odgovoru Ureda podnositelju pritužbe odgovarajuće prenesen ishod pritužbe (vidjeti presudu u predmetu *Susan Milne protiv The Information Commissioner* [2020.], presuda dostupna na: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

([255]) Članci 162. i 163. DPA-a iz 2018.

([256]) Vidjeti, primjerice, presudu u predmetu *Brown protiv Commissioner of Police of the Metropolis & Anor* [2019] EWCA Civ 1724 u kojem je naknada štete u iznosu od 9 000 GBP dodijeljena na temelju DPA-a iz 1998. i Zakona o ljudskim pravima iz 1998. za neovlašteno dobivanje i zlouporabu osobnih podataka i predmetu *R (na zahtjev Bridgesa) protiv Chief Constable of South Wales* [2020] EWCA Civ 1058 u kojem je Žalbeni sud proglasio nezakonitim korištenje sustava prepoznavanja lica za potrebe policije Walesa jer je to bilo u suprotnosti s člankom 8. EKLJP-a, a procjena učinka na zaštitu podataka koju je iznio voditelj obrade nije bila u skladu s DPA-om iz 2018.

([257]) U članku 34. Europske konvencije o ljudskim pravima navodi se da „[s]ud može primati zahtjeve bilo koje fizičke osobe, nevladine organizacije ili skupine pojedinaca koji tvrde da su žrtve povrede prava priznatih u ovoj Konvenciji ili dodatnim protokolima što ih je počinila jedna visoka ugovorna stranka. Visoke ugovorne stranke obvezuju se da ni na koji način neće sprečavati djelotvorno vršenje toga prava".

3.3. **Pristup tijela javne vlasti Ujedinjene Kraljevine podacima i njihova uporaba za potrebe nacionalne sigurnosti**

(175) U pravnom poretku Ujedinjene Kraljevine obavještajne službe ovlaštene za prikupljanje elektroničkih informacija kojima raspolažu voditelji obrade ili izvršitelji obrade zbog razloga nacionalne sigurnosti u situacijama koje su relevantne za scenarij primjerenosti su Sigurnosna služba ([258]) (*Security Service*, MI5), Tajna obavještajna služba ([259]) (*Secret Intelligence Service*, SIS) i Vladin komunikacijski stožer ([260]) (*Government Communications Headquarters*, GCHQ) ([261]).

3.3.1. *Pravne osnove, ograničenja i zaštitne mjere*

(176) Ovlasti obavještajnih agencija u Ujedinjenoj Kraljevini utvrđene su IPA-om iz 2016. i RIPA-om iz 2000., kojima se, zajedno s DPA-om iz 2018., utvrđuju materijalno i osobno područje primjene tih ovlasti te ograničenja i zaštitne mjere za njihovo izvršavanje. Te ovlasti, kao i ograničenja i zaštitne mjere koji se na njih primjenjuju, detaljno su procijenjeni u sljedećim odjeljcima.

3.3.1.1. Istražne ovlasti koje se izvršavaju u kontekstu nacionalne sigurnosti

(177) IPA-om iz 2016. uspostavlja se pravni okvir za upotrebu istražnih ovlasti, tj. ovlasti presretanja podataka o komunikacijama, pristupa tim podacima i ometanja opreme. IPA-om iz 2016. uvodi se opća zabrana korištenja tehnika koje omogućuju pristup sadržaju komunikacija, pristup podacima o komunikacijama ili ometanje opreme bez zakonske ovlasti ([262]) te takvi postupci čine kaznena djela. To se odražava u činjenici da je upotreba tih istražnih ovlasti zakonita samo ako se provodi na temelju naloga ili odobrenja ([263]).

(178) U IPA-i iz 2016. utvrđena su detaljna pravila kojima se uređuju područje primjene i primjena svake istražne ovlasti te njihova posebna ograničenja i zaštitne mjere. Pravila koja se primjenjuju razlikuju se s obzirom na vrstu istražne ovlasti (presretanje komunikacije, pribavljanje i zadržavanje podataka o komunikacijama i

([258]) MI5 je u nadležnosti ministra unutarnjih poslova. U Zakonu o sigurnosnim službama iz 1989. utvrđene su funkcije službe MI5: zaštita nacionalne sigurnosti (uključujući zaštitu od prijetnji povezanih sa špijunažom, terorizmom i sabotažom, od aktivnosti agenata stranih sila i djelovanja usmjerenih na svrgavanje ili podrivanje parlamentarne demokracije političkim, industrijskim ili nasilnim sredstvima), očuvanje gospodarske dobrobiti Ujedinjene Kraljevine od vanjskih prijetnji i podupiranje aktivnosti policijskih snaga i drugih tijela kaznenog progona u sprečavanju i otkrivanju teških kaznenih djela.

([259]) SIS je pod nadležnošću ministra vanjskih poslova, a njegove su funkcije navedene u Zakonu o obavještajnim službama iz 1994. Njegove su funkcije prikupljanje i iznošenje informacija o djelovanjima ili namjerama osoba izvan Britanskih otoka i obavljanje drugih zadaća povezanih s djelovanjima ili namjerama tih osoba. Te se funkcije mogu izvršavati samo u interesu nacionalne sigurnosti, u interesima gospodarske dobrobiti Ujedinjene Kraljevine ili kao potpora sprečavanju ili otkrivanju teških kaznenih djela.

([260]) GCHQ je pod nadležnošću ministra vanjskih poslova, a njegove su funkcije navedene u Zakonu o obavještajnim službama iz 1994. One su (a) praćenje, korištenje ili ometanje elektromagnetskih i drugih emisija i opreme koja stvara takve emisije, prikupljanje i iznošenje informacija dobivenih iz takvih emisija ili opreme ili povezanih s njima te iz šifriranih materijala; (b) pružanje savjeta i pomoći oružanim snagama, vladi ili drugim organizacijama ili osobama koje se smatraju prikladnima u vezi s jezicima, uključujući terminologiju koja se koristi za tehnička pitanja i kriptografiju te druga pitanja koja se odnose na zaštitu informacija. Te se funkcije mogu izvršavati samo u interesu nacionalne sigurnosti, u interesima gospodarske dobrobiti Ujedinjene Kraljevine u odnosu na djelovanja ili namjere osoba izvan Britanskih otoka ili kao potpora sprečavanju ili otkrivanju teških kaznenih djela.

([261]) Druga javna tijela koja obavljaju funkcije relevantne za nacionalnu sigurnost su Obrambena obavještajna agencija (*Defence Intelligence*, DI), Vijeće i tajništvo za nacionalnu sigurnost (*National Security Council and Secretariat*), Zajednička obavještajna organizacija (*Joint Intelligence Organisation*) i Zajednički obavještajni odbor (*Joint Intelligence Committee*). Međutim, Zajednički obavještajni odbor i Zajednička obavještajna organizacija ne mogu koristiti istražne ovlasti na temelju IPA-e iz 2016., a Obrambena obavještajna agencija ima ograničeno područje primjene svojih ovlasti.

([262]) Zabrana se odnosi i na javne i na privatne komunikacijske mreže, kao i na javnu poštansku službu kad se presretanje provodi u Ujedinjenoj Kraljevini. Zabrana se ne primjenjuje na voditelja obrade privatne mreže ako je voditelj obrade dao izričitu ili prešutnu suglasnost za provedbu presretanja (članak 3. IPA-e iz 2016.).

([263]) U određenom ograničenom broju slučajeva moguće je zakonito presretanje bez naloga, tj. kad se radi o presretanju uz suglasnost pošiljatelja ili primatelja (članak 44. IPA-e iz 2016.), za ograničene administrativne ili izvršne svrhe (članci od 45. do 48. IPA-e), u određenim posebnim institucijama (članci od 49. do 51. IPA-e iz 2016.) i u skladu sa zahtjevima stranih tijela (članak 52. IPA-e iz 2016.).

ometanje opreme) ([264]) i na to izvršava li se ovlast u odnosu na poseban cilj ili masovno. Pojedinosti o području primjene, zaštitnim mjerama i ograničenjima svake mjere predviđene u okviru IPA-e iz 2016. opisane su u posebnom odjeljku u nastavku.

(179) Osim toga, IPA iz 2016. dopunjena je nizom zakonskih kodeksa dobre prakse koje je izdao ministar i koje su prihvatila oba doma Parlamenta ([265]) te se primjenjuju u cijeloj zemlji i njima se pružaju dodatne smjernice za korištenje tim ovlastima ([266]). Dok se ispitanici kako bi ostvarili svoja prava mogu izravno osloniti na odredbe utvrđene u IPA-i iz 2016., u točki 5. Priloga 7. IPA-i iz 2016. navodi se da su kodeksi dobre prakse prihvatljivi kao dokazi u građanskim i kaznenim postupcima te da sud ili nadzorno tijelo može uzeti u obzir svako nepridržavanje kodeksa pri utvrđivanju relevantnog pitanja u sudskim postupcima ([267]). U kontekstu procjene „kvalitete zakona" prethodnog zakonodavstva Ujedinjene Kraljevine u području nadzora, odnosno RIPA-e iz 2000., Veliko vijeće Europskog suda za ljudska prava izričito je priznalo relevantnost kodeksa dobre prakse Ujedinjene Kraljevine i prihvatilo da bi se njihove odredbe mogle uzeti u obzir pri procjeni predvidljivosti zakonodavstva kojim se dopušta nadzor ([268]).

(180) Pritom bi trebalo napomenuti i da su ciljane ovlasti (ciljano presretanje ([269]), pribavljanje podataka o komunikacijama ([270]), zadržavanje tih podataka ([271]) i ciljano ometanje opreme ([272])) dostupne nacionalnim sigurnosnim agencijama i određenim tijelima kaznenog progona ([273]), dok samo obavještajne službe mogu koristiti masovne ovlasti (tj. masovno presretanje ([274]), masovno pribavljanje podataka o komunikacijama ([275]), masovno ometanje opreme ([276]) i masovne skupove osobnih podataka ([277])).

(181) Pri odlučivanju o tome koje bi se istražne ovlasti trebale koristiti, obavještajna agencija mora poštovati „opće obveze u pogledu privatnosti" navedene u članku 2. stavku 2. točki (a) IPA-e iz 2016., koje uključuju provjeru nužnosti i proporcionalnosti. Konkretnije, u skladu s tom odredbom tijelo javne vlasti koje namjerava koristiti istražnu ovlast mora razmotriti i. može li se ono što se nastoji postići na temelju naloga, odobrenja ili zahtjeva razumno postići

([264]) Kad je riječ, na primjer, o području primjene takvih mjera, u dijelu 3. i dijelu 4. (zadržavanje i pribavljanje podataka o komunikacijama) područje primjene mjere strogo je povezano s definicijom „telekomunikacijskog operatera" na čije se korisničke podatke primjenjuje mjera. Još jedan primjer može se dati u vezi s korištenjem „masovnim" ovlastima. U tom je slučaju područje primjene tih ovlasti ograničeno na „komunikacije koje šalju ili primaju pojedinci izvan Britanskih otoka".

([265]) U Prilogu 7. IPA-i iz 2016. određuje se područje primjene kodeksa, postupak kojeg se treba pridržavati pri njihovu donošenju, pravila za njihovu reviziju te učinak kodeksa.

([266]) Kodeksi dobre prakse doneseni na temelju IPA-e iz 2016. dostupni su na: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

([267]) Sudovi koriste kodekse dobre prakse kako bi ocijenili zakonitost postupanja tijelâ. Vidjeti, na primjer, predmet *Dias protiv Cleveland Police*, [2017] UKIPtri15_586-CH u kojem se Sud za istražne ovlasti pozvao na određene odlomke Kodeksa dobre prakse za podatke o komunikacijama pri tumačenju definicije osnove za „sprečavanje ili otkrivanje zločina ili sprečavanje kršenja javnog reda" koja se primjenjuje za pribavljanje podataka o komunikacijama. Kodeks je upotrijebljen kako bi se utvrdilo je li ta osnova pogrešno upotrijebljena. Sud je potom zaključio da je sporna praksa nezakonita. Sudovi su ocijenili i razinu zaštitnih mjera dostupnih u kodeksima; vidjeti, na primjer, presudu u predmetu *Just for Law Kids protiv Secretary of State for the Home Department* [2019] EWHC 1772 (Admin) u kojoj je Visoki sud utvrdio da zakonski i podzakonski akti zajedno s internim smjernicama osiguravaju dostatne zaštitne mjere ili presudu u predmetu *R (National Council for Civil Liberties) protiv Secretary of State for the Home Department i drugih* [2019] EWHC 2057 (Admin) u kojoj je Sud utvrdio da IPA iz 2016. i Kodeks dobre prakse za ometanje opreme sadržavaju dostatne odredbe u pogledu potrebe da nalozi budu konkretni.

([268]) U predmetu *Big Brother Watch* Veliko vijeće Europskog suda za ljudska prava navelo je da je „Kodeks dobre prakse za presretanje komunikacija javni dokument koji su odobrila oba doma Parlamenta, a koji je Vlada objavila na internetu i u tiskanom obliku i koji moraju uzeti u obzir osobe koje obavljaju zadaće presretanja i sudovi (vidjeti točke 93. i 94.). Slijedom toga, Sud je prihvatio da se odredbe tog kodeksa mogu uzeti u obzir pri procjeni predvidljivosti RIPA-e (vidjeti prethodno citiranu presudu u predmetu *Kennedy*, točka 157.). U skladu s tim, Sud bi prihvatio da je domaće pravo bilo primjereno ‚dostupno'." (Vidjeti Europski sud za ljudska prava (Veliko vijeće), *Big Brother Watch i drugi protiv United Kingdom*, zahtjevi br. 58170/13, 62322/14 i 24960/15 od 25. svibnja 2021., točka 366.)

([269]) Dio 2. IPA-e iz 2016.

([270]) Dio 3. IPA-e iz 2016.

([271]) Dio 4. IPA-e iz 2016.

([272]) Dio 5. IPA-e iz 2016.

([273]) Za popis relevantnih tijela kaznenog progona koja mogu primjenjivati ciljane istražne ovlasti na temelju IPA-e iz 2016. vidjeti bilješku 139.

([274]) Članak 136. IPA-e iz 2016.

([275]) Članak 158. IPA-e iz 2016.

([276]) Članak 176. IPA-e iz 2016.

([277]) Članak 199. IPA-e iz 2016.

drugim manje nametljivim sredstvima; ii. je li razina zaštite koja se primjenjuje u odnosu na prikupljanje informacija na temelju naloga, odobrenja ili zahtjeva veća zbog posebne osjetljivosti tih informacija; iii. javni interes za integritet i sigurnost telekomunikacijskih sustava i poštanskih službi te iv. svaki drugi aspekt javnog interesa koji se odnosi na zaštitu privatnosti ([278]).

(182) Način na koji bi se ti kriteriji trebali primjenjivati i način na koji ministar i neovisni pravosudni povjerenici ocjenjuju njihovu usklađenost pri davanju odobrenja za korištenje takvih ovlasti dodatno su utvrđeni u relevantnim kodeksima dobre prakse. Konkretno, korištenje svake od tih istražnih ovlasti mora uvijek biti „proporcionalno onome što se nastoji postići, što podrazumijeva uravnoteženje između mogućeg narušavanja privatnosti (i drugih razmatranja navedenih u članku 2. stavku 2.) i potrebe za aktivnošću u istražnom ili operativnom smislu ili smislu tehničke sposobnosti". To posebno znači da bi aktivnost „trebala ponuditi realne izglede za ostvarivanje očekivane koristi i ne bi trebala biti neproporcionalna ili proizvoljna" te da „zadiranje u privatnost ne bi trebalo smatrati proporcionalnim ako bi se tražene informacije razumno mogle postići drugim manje nametljivim sredstvima" ([279]). Konkretno, poštovanje načela proporcionalnosti mora se ocijeniti uzimajući u obzir sljedeće kriterije: „i. opseg predloženog zadiranja u privatnost u odnosu na ono što se nastoji postići; ii. kako i zašto metode koje će se donijeti uzrokuju najmanje moguće zadiranje u privatnost osobe i ostalih; iii. predstavlja li aktivnost primjerenu primjenu Zakona i razuman način postizanja onoga što se nastoji postići, uzimajući u obzir sve druge razumne mogućnosti; iv. prema potrebi, koje druge metode nisu provedene ili su bile primijenjene, ali su procijenjene kao nedostatne za ispunjavanje operativnih ciljeva bez uporabe predložene istražne ovlasti" ([280]).

(183) Tijela Ujedinjene Kraljevine objasnila su da se time u praksi osigurava da obavještajna agencija, kao prvo, postavi operativni cilj (čime se ograničava prikupljanje, npr. za potrebe međunarodne borbe protiv terorizma na određenom geografskom području) i, kao drugo, na temelju tog operativnog cilja morat će razmotriti koja je tehnička opcija (npr. ciljano ili masovno presretanje, ometanje opreme, pribavljanje podataka o komunikacijama) najproporcionalnija (tj. najmanje zadire u privatnost, vidjeti članak 2. stavak 2. IPA-e) u odnosu na ono što se nastoji postići te se stoga može odobriti na temelju jedne od dostupnih zakonskih osnova.

(184) Treba istaknuti da je oslanjanje na standarde nužnosti i proporcionalnosti primijetio i pozdravio i posebni izvjestitelj UN-a za pravo na privatnost Joseph Cannataci, koji je u pogledu sustava uspostavljenog IPA-om iz 2016. izjavio da „se čini da postupci koji su uspostavljeni u okviru obavještajnih službi i tijela kaznenog progona sustavno zahtijevaju da se razmotri nužnost i proporcionalnost mjere ili operacije nadzora prije nego što je se preporuči za odobravanje i njezino preispitivanje na istim osnovama" ([281]). Ujedno je primijetio da je na sastanku s predstavnicima tijela kaznenog progona i nacionalnim sigurnosnim agencijama „postignut konsenzus da pravo na privatnost mora biti na prvom mjestu za svaku odluku koja se odnosi na mjere nadzora. Svi su razumjeli i ocijenili nužnost i proporcionalnost kao temeljna načela koja treba uzeti u obzir".

([278]) U Kodeksu dobre prakse za presretanje komunikacija navodi se da su drugi elementi provjere proporcionalnosti: „i. opseg predloženog zadiranja u privatnost u odnosu na ono što se nastoji postići; ii. kako i zašto metode koje će se donijeti uzrokuju najmanje moguće zadiranje u privatnost osobe i ostalih; iii. predstavlja li aktivnost primjerenu primjenu Zakona i razuman način postizanja onoga što se nastoji postići, uzimajući u obzir sve druge razumne mogućnosti; iv. prema potrebi, koje druge metode nisu provedene ili su bile primijenjene, ali su procijenjene kao nedostatne za ispunjavanje operativnih ciljeva bez uporabe predložene istražne ovlasti". Točka 4.16. Kodeksa dobre prakse za presretanje komunikacija dostupnog na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([279]) Vidjeti točke 4.12. i 4.15. Kodeksa dobre prakse za presretanje komunikacija dostupnog na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([280]) Vidjeti Kodeks dobre prakse za presretanje komunikacija, točka 4.16.

([281]) Izjava povodom završetka posjeta posebnog izvjestitelja za pravo na privatnost Ujedinjenoj Kraljevini Velike Britanije i Sjeverne Irske dostupna na: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, točka 1.a.

(185) Posebni kriteriji za izdavanje različitih naloga te ograničenja i zaštitne mjere utvrđeni IPA-om iz 2016. za svaku istražnu ovlast detaljno su opisani u uvodnim izjavama od 186. do 243.

3.3.1.1.1. Ciljano presretanje i ispitivanje

(186) Postoje tri vrste naloga za ciljano presretanje: nalog za ciljano presretanje ([282]), nalog za ciljani pregled i nalog za uzajamnu pomoć ([283]). Uvjeti za dobivanje tih naloga i odgovarajuće zaštitne mjere utvrđeni su u dijelu 2. poglavlju 1. IPA-e iz 2016.

(187) Nalogom za ciljano presretanje odobrava se presretanje komunikacija opisanih u nalogu pri njihovu prijenosu i dobivanje drugih podataka relevantnih za te komunikacije ([284]), uključujući sekundarne podatke ([285]). Nalogom za ciljani pregled osoba se ovlašćuje za provođenje odabira za pregled presretnutog sadržaja dobivenog na temelju naloga za masovno presretanje ([286]).

(188) Svaki nalog u skladu s dijelom 2. IPA-e iz 2016. može izdati ministar ([287]), a odobrava ga pravosudni povjerenik ([288]). U svim je slučajevima trajanje bilo koje vrste ciljanog naloga ograničeno na šest mjeseci ([289]), a za njegovu izmjenu ([290]) i produljenje ([291]) primjenjuju se posebna pravila.

(189) Prije izdavanja naloga ministar mora provjeriti njegovu nužnost i proporcionalnost ([292]). Konkretno, za nalog za ciljano presretanje i nalog za ciljani pregled ministar bi trebao provjeriti je li mjera potrebna zbog jednog od sljedećih razloga: interes nacionalne sigurnosti; sprečavanje ili otkrivanje teškog kaznenog djela; ili interesi gospodarske dobrobiti Ujedinjene Kraljevine ([293]) ako su relevantni i za interese nacionalne sigurnosti ([294]). S druge strane, nalog za uzajamnu pomoć (vidjeti prethodnu uvodnu izjavu 139.) može se izdati samo ako ministar smatra da postoje okolnosti istovjetne onima u kojima bi izdao nalog u svrhu sprečavanja i/ili otkrivanja teških kaznenih djela ([295]).

(190) Nadalje, ministar bi trebao ocijeniti je li mjera proporcionalna onome što se nastoji postići ([296]). Pri procjeni proporcionalnosti zatraženih mjera moraju se uzeti u obzir opće obveze u pogledu privatnosti utvrđene u članku 2. stavku 2. IPA-e iz 2016., posebno potreba da se procijeni može li se ono što se nastoji postići nalogom, odobrenjem

([282]) Članak 15. stavak 2. IPA-e iz 2016.
([283]) Članak 15. stavak 4. IPA-e iz 2016.
([284]) Članak 15. stavak 2. IPA-e iz 2016.
([285]) Sekundarni podaci su podaci koji su priloženi ili logički povezani s presretnutom komunikacijom i logički se mogu odvojiti od nje te ako su tako odvojeni, ne otkrivaju ništa što bi se razumno moglo smatrati značenjem komunikacije (ako postoji). Neki primjeri sekundarnih podataka uključuju konfiguracije usmjerivača ili vatrozidove ili razdoblje aktivnosti usmjerivača na mreži ako su dio presretnute komunikacije ili su joj priloženi ili logički povezani s njom. Za više pojedinosti vidjeti definiciju u članku 16. IPA-e iz 2016. i Kodeksu dobre prakse za presretanje komunikacija, točka 2.19., vidjeti bilješku 278.
([286]) Taj se pregled provodi kao iznimka od članka 152. stavka 4. IPA-e iz 2016. kojim se predviđa zabrana utvrđivanja komunikacija pojedinaca koji se nalaze na Britanskim otocima. Vidjeti uvodnu izjavu 229.
([287]) Škotski ministar odobrava nalog kad se nalog odnosi na teško kazneno djelo u Škotskoj (vidjeti članke 21. i 22. IPA-e iz 2016.), dok ministar može imenovati visokog dužnosnika za izdavanje naloga za uzajamnu pomoć ako se čini da će se presretanje primjenjivati na osobu ili prostore koji se nalaze izvan Ujedinjene Kraljevine (članak 40. IPA-e iz 2016.).
([288]) Članci 19. i 23. IPA-e iz 2016.
([289]) Članak 32. IPA-e iz 2016.
([290]) Članak 39. IPA-e iz 2016. Propisane osobe mogu izvršiti ograničene izmjene naloga pod uvjetima utvrđenima IPA-om iz 2016. Osoba koja je izdala nalog može ga u bilo kojem trenutku ukinuti. To mora učiniti ako nalog više nije potreban zbog bilo kojeg relevantnog razloga ili ako postupak odobren nalogom više nije proporcionalan onome što se nastoji postići.
([291]) Članak 33. IPA-e iz 2016. Odluku o produljenju naloga mora odobriti pravosudni povjerenik.
([292]) Članak 19. IPA-e iz 2016.
([293]) Za pojam „interesi gospodarske dobrobiti Ujedinjene Kraljevine ako su ti interesi relevantni i za nacionalnu sigurnost" Veliko vijeće Europskog suda za ljudska prava utvrdilo je u predmetu *Big Brother Watch i drugi protiv United Kingdom* (vidjeti prethodnu bilješku 268.), točka 371., da je taj pojam dovoljno usmjeren na nacionalnu sigurnost. Iako je zaključak Suda u tom predmetu bio povezan s uporabom tog pojma u RIPA-i iz 2000., isti se pojam upotrebljava i u IPA-i iz 2016.
([294]) Članak 20. stavak 2. IPA-e iz 2016.
([295]) Članak 20. stavak 3. IPA-e iz 2016.
([296]) Članak 19. stavak 1. točka (b), članak 19. stavak 2. točka (b) i članak 19. stavak 3. točka (b) IPA-e iz 2016.

ili zahtjevom razumno ostvariti drugim manje nametljivim sredstvima te je li razina zaštite koju treba primijeniti u odnosu na bilo koje prikupljanje informacija na temelju naloga viša zbog posebne osjetljivosti tih informacija (vidjeti uvodnu izjavu 181.).

(191) U tu će svrhu ministar morati uzeti u obzir sve elemente zahtjeva koje je dostavilo tijelo koje podnosi zahtjev, posebno one koji se odnose na osobe koje bi se trebale presretati i relevantnost mjere za istragu. Takvi su elementi navedeni u Kodeksu dobre prakse za presretanje komunikacija i moraju biti dovoljno konkretno opisani ([297]). Nadalje, u članku 17. IPA-e iz 2016. zahtijeva se da se u svakom nalogu izdanom u skladu s njegovim poglavljem 2. mora navesti ili opisati konkretna osoba ili skupina osoba, organizacija ili prostori koje treba presretati („cilj"). U slučaju naloga za ciljano presretanje ili naloga za ciljani pregled oni se mogu odnositi i na skupinu osoba, više od jedne osobe ili organizacije ili više od jednog skupa prostora (takozvani „tematski nalog") ([298]). U tim slučajevima u nalogu bi trebala biti opisana zajednička svrha ili aktivnost skupine osoba ili operacija/istraga i ime ili opis što većeg broja tih osoba/organizacija ili skupa prostora ako je to praktično moguće ([299]). Naposljetku, u svim se nalozima izdanima na temelju dijela 2. IPA-e iz 2016. moraju navesti adrese, brojevi, uređaji, čimbenici ili kombinacija čimbenika koji će se upotrebljavati za identifikaciju komunikacija ([300]). U tom se smislu u Kodeksu dobre prakse za presretanje komunikacija navodi da se u slučaju naloga za ciljano presretanje i naloga za ciljani pregled „u nalogu moraju navesti (ili opisati) čimbenici ili kombinacija čimbenika koji će se upotrebljavati za identifikaciju komunikacije. Ako se komunikacija mora identificirati tako da se navede telefonski broj (na primjer), broj se mora navesti tako da bude u cijelosti prikazan. Međutim, ako se za identifikaciju komunikacije upotrebljavaju vrlo složeni ili stalno promjenjivi internetski selektori, te bi selektore trebalo opisati u najvećoj mogućoj mjeri" ([301]).

(192) Važna je zaštitna mjera u tom kontekstu to što procjenu ministra u pogledu izdavanja naloga mora odobriti neovisni pravosudni povjerenik ([302]) koji će posebno provjeriti je li odluka o izdavanju naloga u skladu s načelima nužnosti i proporcionalnosti ([303]) (za status i ulogu pravosudnog povjerenika vidjeti uvodne izjave od 251. do 256. u nastavku). U IPA-i iz 2016. ujedno se pojašnjava da pri provedbi takve provjere pravosudni povjerenik mora primjenjivati ista načela koja bi primijenio sud u slučaju zahtjeva za sudsko preispitivanje ([304]). Time se osigurava da u svakom slučaju, a prije nego što dođe do pristupa podacima, neovisno tijelo sustavno provjerava poštovanje načela nužnosti i proporcionalnosti.

(193) U okviru IPA-e iz 2016. predviđeno je nekoliko posebnih i vrlo ograničenih iznimaka za provedbu ciljanih presretanja bez naloga. Ograničeni slučajevi detaljno su opisani u zakonodavstvu ([305]) i, osim onog koji se temelji na „privoli" pošiljatelja/primatelja, provode ih subjekti (privatna ili javna tijela) koji nisu nacionalne sigurnosne agencije. Osim toga, takva vrsta presretanja provodi se u svrhe koje nisu „obavještajno" prikupljanje ([306]), a za neke od njih veoma je malo vjerojatno da se prikupljanje može provesti u kontekstu scenarija „prijenosa" (na primjer u slučaju

([297]) Tražene informacije uključuju pojedinosti o pozadini (opis osoba/organizacija/skupa prostora, komunikacije koju treba presresti) i način na koji će prikupljanje tih informacija biti korisno za istragu, kao i opis postupaka koje treba odobriti. Ako nije moguće opisati osobe/organizaciju/prostore, mora se navesti objašnjenje zašto to nije moguće ili zašto je naveden samo opći opis (Kodeks dobre prakse za presretanje komunikacija, točke 5.32. i 5.34., vidjeti bilješku 278.).

([298]) Članak 17. stavak 2. IPA-e iz 2016. Vidjeti i Kodeks dobre prakse za presretanje komunikacija, točka 5.11. i dalje, vidjeti bilješku 278.

([299]) Članak 31. stavci 4. i 5. IPA-e iz 2016.

([300]) Članak 31. stavak 8. IPA-e iz 2016.

([301]) Kodeks dobre prakse za presretanje komunikacija, točke 5.37. i 5.38., vidjeti bilješku 278.

([302]) Odobrenje pravosudnog povjerenika nije potrebno ako ministar smatra da postoji hitna potreba za izdavanjem naloga (članak 19. stavak 1. IPA-e). Međutim, pravosudni povjerenik mora u kratkom roku biti obaviješten i mora odlučiti hoće li odobriti nalog. Ako ga ne odobri, nalog prestaje važiti (članci 24. i 25. IPA-e iz 2016.).

([303]) Članak 23. stavak 1. IPA-e iz 2016.

([304]) Članak 23. stavak 2. IPA-e iz 2016.

([305]) Vidjeti članke od 44. do 51. IPA-e iz 2016. i odjeljak 12. Kodeksa dobre prakse za presretanje komunikacija (vidjeti bilješku 278.).

([306]) To je, na primjer, ako je potrebno presretanje u zatvoru ili psihijatrijskoj bolnici (kako bi se provjerilo ponašanje pritvorene osobe ili pacijenta) ili od strane poštanskog ili telekomunikacijskog operatera, na primjer radi otkrivanja zloupotrebe sadržaja.

presretanja u psihijatrijskoj bolnici ili u zatvoru). S obzirom na prirodu tijela na koje se ti posebni slučajevi primjenjuju (nisu nacionalne sigurnosne agencije) primjenjivat će se sve zaštitne mjere predviđene u dijelu 2. DPA-a iz 2018. i Općoj uredbi o zaštiti podataka Ujedinjene Kraljevine, uključujući nadzor ICO-a i dostupne mehanizme sudske zaštite. Nadalje, osim zaštitnih mjera predviđenih u DPA-u iz 2018., u određenim slučajevima u okviru IPA-e iz 2016. predviđen je i *ex post* nadzor IPCO-a ([307]).

(194) Pri presretanju primjenjuju se dodatna ograničenja i zaštitne mjere s obzirom na poseban status presretenih osoba ([308]). Primjerice, presretanje informacija koje podliježu obvezi čuvanja povjerljivosti dopušteno je samo u iznimnim i uvjerljivim okolnostima, a osoba koja izdaje nalog mora uzeti u obzir javni interes u pogledu povjerljivosti informacija koje podliježu obvezi čuvanja povjerljivosti te da su uspostavljeni posebni zahtjevi za postupanje s takvim materijalom, njegovo zadržavanje i otkrivanje ([309]).

(195) Nadalje, IPA-om iz 2016. predviđaju se posebne zaštitne mjere povezane sa sigurnošću, zadržavanjem i otkrivanjem koje bi ministar trebao uzeti u obzir prije izdavanja ciljanog naloga ([310]). Konkretno, člankom 53. stavkom 5. IPA-e iz 2016. zahtijeva se da se svaki primjerak materijala prikupljenog na temelju naloga mora pohraniti na siguran način i uništiti čim više ne budu postojali relevantni razlozi za njegovo zadržavanje, dok se člankom 53. stavkom 2. IPA-e iz 2016. zahtijeva da se broj osoba kojima se materijal otkriva i opseg otkrivanja, stavljanja na raspolaganje ili kopiranja tog materijala mora ograničiti na minimum koji je potreban za propisane svrhe.

(196) Naposljetku, kad se materijal koji je presretnut na temelju naloga za ciljano presretanje ili naloga za uzajamnu pomoć prosljeđuje trećoj zemlji („otkrivanje stranim tijelima"), IPA-om iz 2016. predviđa se da ministar mora osigurati da su uspostavljeni odgovarajući dogovori kojima se jamči da u toj trećoj zemlji postoje slične zaštitne mjere u pogledu sigurnosti, zadržavanja i otkrivanja ([311]). Osim toga, u članku 109. stavku 2. DPA-a iz 2018. predviđa se da obavještajne službe mogu prenositi osobne podatke izvan državnog područja Ujedinjene Kraljevine samo ako je prijenos nužna i proporcionalna mjera za svrhu zakonom propisanih funkcija voditelja obrade ili druge svrhe predviđene u članku 2. stavku 2. točki (a) Zakona o sigurnosnim službama iz 1989. ili članku 2. stavku 2. točki (a) i članku 4. stavku 2. točki (a) Zakona o obavještajnim službama iz 1994. ([312]) Važno je napomenuti da se ti zahtjevi primjenjuju i u slučajevima u kojima se poziva na izuzeće radi nacionalne sigurnosti u skladu s člankom 110. DPA-a iz 2018. jer se u članku 110. DPA-a iz 2018. ne navodi da je članak 109. DPA-a iz 2018. jedna od odredbi koje se mogu izuzeti od primjene ako se u svrhu zaštite nacionalne sigurnosti zahtijeva izuzeće od određenih odredbi.

3.3.1.1.2. Ciljano pribavljanje i zadržavanje podataka o komunikacijama

(197) IPA-om iz 2016. ministru se dopušta da od operatera telekomunikacijskih usluga zahtijeva zadržavanje podataka o komunikacijama radi omogućavanja ciljanog pristupa za različita tijela javne vlasti, uključujući tijela kaznenog progona i obavještajne agencije. U dijelu 4. IPA-e iz 2016. predviđa se zadržavanje podataka o komunikacijama, dok se u dijelu 3. predviđa ciljano pribavljanje podataka o komunikacijama. U dijelu 3. i 4. IPA-e iz 2016. ujedno su utvrđena posebna ograničenja u pogledu upotrebe tih ovlasti i predviđaju se posebne zaštitne mjere.

([307]) Vidjeti, *a contrario*, članak 229. stavak 4. IPA-e.

([308]) Člancima od 26. do 29. IPA-e iz 2016. uvode se ograničenja za dobivanje naloga za ciljano presretanje i pregled u pogledu presretanja komunikacija koje šalje osoba koja je zastupnik u parlamentu (bilo koji parlament Ujedinjene Kraljevine) ili su joj namijenjene, presretanja informacija koje podliježu obvezi čuvanja povjerljivosti, presretanja komunikacija za koje tijelo koje provodi presretanje vjeruje da će biti komunikacije koje sadržavaju povjerljivi novinarski materijal i kad je svrha naloga utvrditi ili potvrditi izvor novinarskih informacija.

([309]) Članak 26. IPA-e iz 2016.

([310]) Članak 19. stavak 1. IPA-e iz 2016.

([311]) Članak 54. IPA-e iz 2016. Zaštitne mjere koje se odnose na otkrivanje materijala stranim tijelima dodatno su navedene u kodeksima dobre prakse: vidjeti osobito točku 9.26. i dalje i točku 9.87. Kodeksa dobre prakse za presretanje komunikacija te točku 9.33. i dalje i točku 9.41. Kodeksa dobre prakse za ometanje opreme (vidjeti bilješku 278.).

([312]) Te su svrhe: za Sigurnosnu službu sprečavanje ili otkrivanje teških kaznenih djela ili provođenje kaznenih postupaka (članak 2. stavak 2. točka (a) Zakona o sigurnosnim službama iz 1989.), za Obavještajnu službu interesi nacionalne sigurnosti, sprečavanje ili otkrivanje teških kaznenih djela ili provođenje kaznenih postupaka (članak 2. stavak 2. točka (a) Zakona o obavještajnim službama iz 1994.) i za GCHQ provođenje kaznenih postupaka (članak 4. stavak 2. točka (a) Zakona o obavještajnim službama iz 1994.). Vidjeti i Pojašnjenja DPA-a iz 2018., koja su dostupna na sljedećoj poveznici: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(198) Pojmom „podaci o komunikacijama” obuhvaćeni su sudionici, vrijeme, mjesto i način komunikacije, ali ne i sadržaj komunikacije, tj. ono što je rečeno ili napisano. Za razliku od presretanja, pribavljanje i zadržavanje podataka o komunikacijama nije usmjereno na sadržaj komunikacije, već na dobivanje informacija kao što su podaci o pretplatniku telefonske usluge ili račun s detaljnim ispisom. To bi moglo uključivati vrijeme i trajanje komunikacije, broj ili e-adresu pošiljatelja i primatelja, a ponekad i lokaciju uređaja s kojih je uspostavljena telekomunikacija ([313]).

(199) Treba napomenuti da se zadržavanje i pribavljanje podataka o komunikacijama obično neće odnositi na osobne podatke ispitanika iz EU-a koji se u skladu s ovom Odlukom prenose u Ujedinjenu Kraljevinu. Obveza zadržavanja ili otkrivanja podataka o komunikacijama u skladu s dijelovima 3. i 4. IPA-e iz 2016. obuhvaća podatke koje su prikupili telekomunikacijski operateri u Ujedinjenoj Kraljevini izravno od korisnika telekomunikacijske usluge ([314]). Ta vrsta obrade „u izravnom kontaktu s klijentom” obično ne uključuje prijenos na temelju ove Odluke, tj. prijenos od voditelja obrade/izvršitelja obrade u EU-u voditelju obrade/izvršitelju obrade u Ujedinjenoj Kraljevini.

(200) Međutim, radi potpunosti, u sljedećim se uvodnim izjavama analiziraju uvjeti i zaštitne mjere kojima se uređuju ti sustavi pribavljanja i zadržavanja.

(201) Kao premisu, valja istaknuti da su zadržavanje i ciljano pribavljanje podataka o komunikacijama dostupni nacionalnim sigurnosnim agencijama i određenim tijelima kaznenog progona ([315]). Uvjeti za zahtijevanje zadržavanja i/ili pribavljanja podataka o komunikacijama mogu se razlikovati ovisno o razlozima za traženje mjere, odnosno traži li se mjera za potrebe nacionalne sigurnosti ili kaznenog progona.

(202) Konkretno, iako je novim sustavom uveden opći zahtjev za *ex ante* odobrenje neovisnog tijela koje će se primjenjivati u svim slučajevima u kojima se podaci o komunikacijama zadržavaju i/ili pribavljaju (za potrebe kaznenog progona ili nacionalne sigurnosti), nakon presude Suda EU-a u predmetu *Tele2/Watson* ([316]) uvedene su posebne zaštitne mjere ako se mjera zahtijeva za potrebe kaznenog progona. Točnije, kad se zadržavanje ili pribavljanje podataka o komunikacijama traži za potrebe kaznenog progona, *ex ante* odobrenje uvijek mora izdati povjerenik za istražne ovlasti. To nije uvijek slučaj ako se mjera zahtijeva radi nacionalne sigurnosti jer, kako je opisano u nastavku, u određenim slučajevima takvu vrstu mjera može odobriti drugi „izdavatelj odobrenja”. Osim toga, novim sustavom uveden je prag za „teška kaznena djela” za koje se može dopustiti zadržavanje i pribavljanje podataka o komunikacijama ([317]).

([313]) Podaci o komunikacijama definirani su u članku 261. stavku 5. IPA-e iz 2016. Podaci o komunikacijama dijele se na „podatke o događajima” (bilo koji podatak kojim se identificira ili opisuje događaj, bez obzira na to navodi li se njegova lokacija, do kojeg je došlo u telekomunikacijskom sustavu ili putem njega, pri čemu se događaj sastoji od jednog ili više subjekata koji obavljaju određenu aktivnost u određenom trenutku) i „podatke o subjektu” (bilo koji podatak koji: (a) se odnosi na i. subjekt, ii. povezanost između telekomunikacijske usluge i subjekta ili iii. povezanost između bilo kojeg dijela telekomunikacijskog sustava i subjekta; (b) se sastoji od podataka kojima se identificira ili opisuje subjekt ili ih uključuje (bez obzira na to navodi li se lokacija subjekta) i (c) nisu podaci o događajima).

([314]) To proizlazi iz definicije podataka o komunikacijama iz članka 261. stavka 5. IPA-e iz 2016., prema kojoj podatke o komunikacijama čuva ili prikuplja telekomunikacijski operater te se ti podaci odnose na korisnika telekomunikacijske usluge i povezani su s pružanjem te usluge ili su sadržani u komunikaciji, čine njezin dio, priloženi su joj ili su logički povezani s njom (vidjeti i Kodeks dobre prakse za podatke o komunikacijama dostupan na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, točke od 2.22. do 2.33.). Osim toga, definicija telekomunikacijskog operatera utvrđena u članku 261. stavku 10. IPA-e iz 2016. zahtijeva da je telekomunikacijski operater osoba koja nudi ili pruža telekomunikacijsku uslugu osobama u Ujedinjenoj Kraljevini ili koja kontrolira ili pruža telekomunikacijski sustav koji se (u cijelosti ili djelomično) nalazi u Ujedinjenoj Kraljevini ili se njime upravlja iz te zemlje. Te definicije pojašnjavaju da se obveze na temelju IPA-e iz 2016. ne mogu nametnuti telekomunikacijskim operaterima čija se oprema ne nalazi u Ujedinjenoj Kraljevini ili se njome ne upravlja iz te zemlje ili koji ne nude niti pružaju usluge osobama u Ujedinjenoj Kraljevini (vidjeti i Kodeks dobre prakse za podatke o komunikacijama, točka 2.1.). Ako pretplatnici u EU-u (bez obzira na to nalaze li se u EU-u ili u Ujedinjenoj Kraljevini) koriste usluge u Ujedinjenoj Kraljevini, sve komunikacije povezane s pružanjem te usluge izravno prikuplja pružatelj usluga u Ujedinjenoj Kraljevini te se one ne prenose iz EU-a.

([315]) Relevantna tijela navedena su u Prilogu 4. IPA-i iz 2016., a uključuju policijske snage, obavještajne službe, neka ministarstva i vladine odjele, Nacionalnu agenciju za kriminal, Poreznu i carinsku upravu Ujedinjene Kraljevine, Nadležno tijelo za tržišno natjecanje i tržišta, povjerenika za informiranje, hitnu službu, vatrogasnu i spasilačku službu te tijela, na primjer u području zdravstva i sigurnosti hrane.

([316]) Spojeni predmeti C-203/15 i C-698/15, *Tele2/Watson*, ECLI:EU:C:2016:970).

([317]) Vidjeti članak 61.7. točku (b) za pribavljanje podataka o komunikacijama i članak 87.10.A za zadržavanje podataka o komunikacijama.

i. *Odobrenje za prikupljanje podataka o komunikacijama*

(203) U skladu s dijelom 3. IPA-e iz 2016. relevantna tijela javne vlasti ovlaštena su za prikupljanje podataka o komunikacijama od telekomunikacijskog operatera ili bilo koje osobe koja može prikupiti i otkriti takve podatke. U odobrenju se ne smije dopustiti presretanje sadržaja komunikacije ([318]), a prestaje važiti nakon mjesec dana ([319]) s mogućnošću produljenja uz dodatno odobrenje ([320]). Za pribavljanje podataka o komunikacijama potrebno je odobrenje povjerenika za istražne ovlasti (IPC) ([321]) (o statusu i ovlastima IPC-a vidjeti uvodne izjave 250. i 251. u nastavku). To je uvijek slučaj kad pribavljanje podataka o komunikacijama zahtijeva relevantno tijelo kaznenog progona. Međutim, u skladu s člankom 61. IPA-e iz 2016. ako se podaci prikupljaju radi interesa nacionalne sigurnosti ili gospodarske dobrobiti Ujedinjene Kraljevine sve dok je to relevantno za nacionalnu sigurnost ili ako zahtjev podnosi član obavještajne agencije na temelju članka 61. stavka 7. točke (b) ([322]), pribavljanje može odobriti ([323]) IPC ili imenovani viši službenik ([324]). Imenovani službenik mora biti neovisan u odnosu na predmetnu istragu ili operaciju te mora imati praktično znanje o načelima i zakonodavstvu o ljudskim pravima, posebno o nužnosti i proporcionalnosti ([325]). Odluka koju donosi imenovani službenik podliježe *ex post* nadzoru IPC-a (za više pojedinosti o funkcijama *ex post* nadzora IPC-a vidjeti uvodnu izjavu 254.).

(204) Odobrenje za pribavljanje podataka o komunikacijama temelji se na procjeni nužnosti i proporcionalnosti mjere. Konkretnije, nužnost mjere procjenjuje se s obzirom na osnove navedene u zakonodavstvu ([326]). Uzimajući u obzir ciljanu prirodu te mjere, ona mora biti nužna i za konkretnu istragu ili operaciju ([327]). Daljnji zahtjevi u pogledu procjene nužnosti mjera utvrđeni su u Kodeksu dobre prakse za podatke o komunikacijama ([328]). Tim se Kodeksom posebno predviđa da bi u zahtjevu koji je podnijelo tijelo podnositelj zahtjeva trebalo utvrditi tri minimalna elementa koja opravdavaju nužnost takvog zahtjeva: i. događaj koji se istražuje kao što je kazneno djelo ili lokacija ranjive nestale osobe; ii. osoba čiji se podaci traže, kao što je osumnjičenik, svjedok ili nestala osoba, i kako je ta osoba povezana s događajem; i iii. tražene podatke o komunikacijama, kao što su telefonski broj ili IP adresa, i kako su ti podaci povezani s osobom i događajem ([329]).

(205) Osim toga, pribavljanje podataka o komunikacijama trebalo bi biti proporcionalno onome što se nastoji postići ([330]). U Kodeksu dobre prakse za podatke o komunikacijama pojašnjava se da bi pri provedbi takve procjene izdavatelj odobrenja trebao uspostaviti ravnotežu između „opsega zadiranja u prava i slobode pojedinca i posebne koristi za istragu ili operaciju koju provodi relevantno tijelo javne vlasti u javnom interesu” i da, uzimajući u obzir sva

([318]) Članak 60.A stavak 6. IPA-e iz 2016.

([319]) To se razdoblje skraćuje na tri dana kad se odobrenje daje zbog hitnosti (članak 65. stavak 3.A IPA-e iz 2016.).

([320]) U skladu s člankom 65. IPA-e iz 2016. produljeno odobrenje trajat će mjesec dana od datuma isteka postojećeg odobrenja. Osoba koja je izdala odobrenje može ga u bilo kojem trenutku ukinuti ako smatra da zahtjevi više nisu ispunjeni.

([321]) Članak 60.A stavak 1. IPA-e iz 2016. Ured za izdavanje odobrenja za podatke o komunikacijama (OCDA) obavlja tu funkciju u ime IPC-a (vidjeti Kodekse dobre prakse za podatke o komunikacijama, točka 5.6.).

([322]) Zahtjev na temelju članka 61. stavka 7. točke (b) IPA-e iz 2016. odnosi se na „primjenjivu svrhu povezanu s kaznenim djelom”, što u skladu s člankom 61. stavkom 7.A IPA-e iz 2016. znači: „ako su podaci o komunikacijama u cijelosti ili djelomično podaci o događajima, u svrhu sprečavanja ili otkrivanja teških kaznenih djela; u bilo kojem drugom slučaju u svrhu sprečavanja ili otkrivanja kaznenih djela ili sprečavanja kršenja javnog reda”.

([323]) U Kodeksu dobre prakse za podatke o komunikacijama navodi se: „Ako se zahtjev koji se odnosi na nacionalnu sigurnost može donijeti u skladu s člankom 60.A ili člankom 61., odluka o tome koji je način izdavanja odobrenja najprikladniji u određenom slučaju pitanje je o kojem odlučuju pojedinačna tijela javne vlasti. Tijela javne vlasti koja žele dobiti odobrenje višeg službenika trebala bi imati uspostavljene jasne smjernice o tome kad je taj način izdavanja odobrenja primjeren.” (Kodeks dobre prakse za podatke o komunikacijama, točka 5. 19., dostupan na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

([324]) U članku 70. stavku 3. IPA-e iz 2016. nalazi se definicija „imenovanog službenika” koja se razlikuje ovisno o relevantnom tijelu javne vlasti (kako je navedeno u Prilogu 4. IPA-i iz 2016.).

([325]) Dodatne pojedinosti o neovisnosti imenovanog višeg službenika navedene su u Kodeksu dobre prakse za podatke o komunikacijama (Kodeks dobre prakse za podatke o komunikacijama, točke od 4.12. do 4.17., vidjeti bilješku 323.).

([326]) Te su osnove: i. nacionalna sigurnost; ii. sprečavanje ili otkrivanje kaznenog djela ili sprečavanje kršenja javnog reda (u slučaju „podataka o događajima” samo za teška kaznena djela); ili. interesi gospodarske dobrobiti Ujedinjene Kraljevine ako su ti interesi relevantni i za interese nacionalne sigurnosti; iv. interes javne sigurnosti; v. sprečavanje smrti ili ozljede ili bilo koje štete za tjelesno ili mentalno zdravlje osobe ili ublažavanje bilo koje ozljede ili štete za tjelesno ili mentalno zdravlje osobe; vi. pomaganje u istragama navodnih pravosudnih pogrešaka ili vii. identifikacija mrtve osobe ili osobe koja se zbog određenog stanja ne može sama identificirati (članak 61. stavak 7. IPA-e iz 2016.).

([327]) Članak 60.A stavak 1. točka (b) IPA-e iz 2016.

([328]) Kodeks dobre prakse za podatke o komunikacijama, točka 3.3. i dalje, vidjeti bilješku 323.

([329]) Kodeks dobre prakse za podatke o komunikacijama, točka 3.13., vidjeti bilješku 323.

([330]) Članak 60. stavak 1. točka (c) IPA-e iz 2016.

razmatranja pojedinog slučaja, „ozbiljan negativni učinak na prava druge osobe ili skupine osoba možda još uvijek nije opravdanje za zadiranje u prava pojedinca". Nadalje, kako bi se konkretno procijenila proporcionalnost mjere, u Kodeksu se navodi niz elemenata koje treba uključiti u zahtjev koji podnosi tijelo podnositelj zahtjeva ([331]). Nadalje, posebnu pozornost treba obratiti na vrstu podataka o komunikacijama (podatke o „subjektu" ili „događaju" ([332])) koji se trebaju pribaviti, a prednost se mora dati uporabi kategorije podataka koja manje zadire u privatnost ([333]). Kodeks dobre prakse za podatke o komunikacijama sadržava i posebne upute za odobrenja koja uključuju podatke o komunikacijama osoba određenih zanimanja (liječnici, odvjetnici, novinari, zastupnici u parlamentu ili svećenici) ([334]) koja podliježu dodatnim zaštitnim mjerama ([335]).

ii. *Zahtjev kojim se traži zadržavanje podataka o komunikacijama*

(206) U dijelu 4. IPA-e iz 2016. utvrđuju se pravila za zadržavanje podataka o komunikacijama, a posebno kriteriji kojima se ministru omogućuje izdavanje zahtjeva za zadržavanje ([336]). Zaštitne mjere uvedene IPA-om iste su i u slučaju zadržavanja podataka za potrebe kaznenog progona ili u interesu nacionalne sigurnosti.

(207) Cilj je izdavanja takvih zahtjeva za zadržavanje osigurati da telekomunikacijski operateri u razdoblju od najviše 12 mjeseci zadrže relevantne podatke o komunikacijama koji bi inače bili izbrisani nakon što im više ne budu potrebni za poslovanje ([337]). Zadržani podaci trebaju ostati dostupni u traženom roku jer bi kasnije mogli biti potrebni tijelu javne vlasti na temelju odobrenja za ciljano pribavljanje podataka o komunikacijama koje je predviđeno u dijelu 3. IPA-e iz 2016. i opisano u uvodnim izjavama od 203. do 205.

(208) Izvršavanje ovlasti zahtijevanja zadržavanja određenih podataka podliježe nizu ograničenja i zaštitnih mjera. Ministar može izdati zahtjev za zadržavanje jednom operateru ili više njih ([338]) samo ako smatra da je potreba za zadržavanjem podataka nužna na temelju jedne od propisanih svrha ([339]) i ako je proporcionalan onome što se nastoji postići ([340]). Kako

([331]) Ti podaci koje treba uključiti u zahtjeve moraju sadržavati: i. opis kako će prikupljanje podataka biti korisno za istragu ili operaciju; ii. objašnjenje relevantnosti traženih rokova, uključujući način na koji su ti rokovi razmjerni događaju koji se istražuje; iii. objašnjenje o tome kako je razina zadiranja opravdana ako se u obzir uzmu koristi koje će podaci donijeti istrazi (to bi opravdanje trebalo uključivati razmatranje toga mogu li se za postizanje cilja poduzeti manje nametljive istrage); iv. uzimanje u obzir prava (osobito prava na privatnost i, u relevantnim slučajevima, slobode izražavanja) pojedinca te uspostavljanje ravnoteže između tih prava i koristi za istragu; v. pojedinosti o vrsti kolateralnog zadiranja u privatnost do kojeg može doći te kako zatraženi rokovi utječu na takvo kolateralno zadiranje (Kodeks dobre prakse za podatke o komunikacijama, točke od 3.22. do 3.26., vidjeti bilješku 323.).

([332]) Vidjeti bilješku 313.

([333]) Kad se zahtijevaju podaci o komunikacijama kojima se više zadire u privatnost (tj. podaci o događajima), u Kodeksu se navodi da je prikladnije prvo prikupiti podatke o subjektima ili izravno prikupiti podatke o događajima u ograničenom broju osobito hitnih slučajeva (Kodeks dobre prakse za podatke o komunikacijama, točke od 6.10. do 6.14., vidjeti bilješku 323.).

([334]) Kodeks dobre prakse za podatke o komunikacijama, točke od 8.8. do 8.44., vidjeti bilješku 323.

([335]) U Kodeksu dobre prakse navodi se da „osoba koje izdaje odobrenje mora osobito pažljivo preispitati takve zahtjeve, uključujući dodatno razmatranje mogu li takvi zahtjevi imati moguće neplanirane posljedice te je li taj zahtjev najbolji način za ostvarivanje javnog interesa" (Kodeks dobre prakse za podatke o komunikacijama, točka 8.8.). Nadalje, treba voditi evidenciju o takvim zahtjevima i pri sljedećoj inspekciji o njima treba obavijestiti IPC-a (Kodeks dobre prakse za podatke o komunikacijama, točka 8.10., bilješka 323.).

([336]) Članci od 87. do 89. IPA-e iz 2016.

([337]) Na temelju članka 90. IPA-e iz 2016. telekomunikacijski operater kojem je izdan zahtjev za zadržavanje može zatražiti preispitivanje od ministra koji ga je izdao.

([338]) U skladu s člankom 87. stavkom 2. točkom (a) IPA-e iz 2016. zahtjev za zadržavanje može se odnositi na „određenog operatera ili bilo koji opis operaterâ".

([339]) Svrhe su: i. interesi nacionalne sigurnosti; ii. primjenjiva svrha povezana s kaznenim djelom (kako je definirana u članku 87. stavku 10.A IPA-e iz 2016.); iii. interesi gospodarske dobrobiti Ujedinjene Kraljevine ako su ti interesi relevantni i za interese nacionalne sigurnosti; iv. interesi javne sigurnosti; v. sprečavanje smrti ili ozljede ili bilo koje štete za tjelesno ili mentalno zdravlje osobe ili ublažavanje bilo koje ozljede ili štete za tjelesno ili mentalno zdravlje osobe; ili vi. pružanje pomoći u istragama navodnih pravosudnih grešaka (članak 87. IPA-e).

([340]) Članak 87. IPA-e iz 2016. Osim toga, u skladu s relevantnim kodeksom dobre prakse, kako bi se ocijenila proporcionalnost zahtjeva za zadržavanje, primjenjuju se kriteriji iz članka 2. stavka 2. IPA-e iz 2016., posebno zahtjev da se ocijeni je li ono što se nastoji postići zahtjevom razumno moguće ostvariti manje nametljivim sredstvima. Slično ocjeni proporcionalnosti pribavljanja podataka o komunikacijama, u Kodeksu dobre prakse za podatke o komunikacijama pojašnjava se da takva procjena uključuje „uspostavu ravnoteže između opsega zadiranja u pravo pojedinca na poštovanje njegova privatnog života i posebne koristi za istragu" (Kodeks dobre prakse za podatke o komunikacijama, točka 16.3., vidjeti bilješku 323.).

je pojašnjeno u samoj IPA-i iz 2016. ([341]), prije izdavanja zahtjeva za zadržavanje ministar mora uzeti u obzir: vjerojatne koristi od tog zahtjeva ([342]), opis telekomunikacijskih usluga, primjerenost ograničavanja podataka koji se zadržavaju navođenjem lokacije ili opisa osoba kojima su pružene telekomunikacijske usluge ([343]), mogući broj korisnika (ako su poznati) bilo koje telekomunikacijske usluge na koje se zahtjev odnosi ([344]), tehničku izvedivost ispunjavanja zahtjeva, vjerojatan trošak ispunjavanja zahtjeva, kao i svaki drugi učinak zahtjeva na telekomunikacijskog operatera (ili opis operatera) na kojeg se odnosi ([345]). Kako je detaljnije opisano u poglavlju 17. Kodeksa dobre prakse za podatke o komunikacijama, u svim zahtjevima za zadržavanje treba navesti svaku vrstu podataka koju je potrebno zadržati i kako ta vrsta podataka ispunjava ispitne zahtjeve za zadržavanje.

(209) U svim slučajevima (za potrebe nacionalne sigurnosti i kaznenog progona) odluku ministra o izdavanju zahtjeva za zadržavanje mora odobriti neovisni pravosudni povjerenik u okviru takozvanog „postupka dvostruke zaštite", koji mora posebno preispitati je li zahtjev za zadržavanje relevantnih podataka o komunikacijama nužan i proporcionalan za jednu ili više propisanih svrha ([346]).

3.3.1.1.3. Ometanje opreme

(210) Ometanje opreme sastoji se od niza tehnika korištenih za dobivanje različitih podataka s opreme ([347]), što uključuje računala, tablete i pametne telefone te kabele, žice i uređaje za pohranu ([348]). Ometanjem opreme omogućuje se prikupljanje sadržaja komunikacija i podataka o opremi ([349]).

(211) U skladu s člankom 13. stavkom 1. IPA-e iz 2016. kako bi obavještajna služba mogla koristiti ometanje opreme, mora dobiti odobrenje na temelju naloga u okviru postupka „dvostruke zaštite" koji je uspostavljen IPA-om iz 2016. pod uvjetom da postoji „poveznica s Britanskim otocima" ([350]). U skladu s objašnjenjima tijela Ujedinjene Kraljevine, u situacijama u kojima se podaci prenose iz Europske unije u Ujedinjenu Kraljevinu u okviru područja

([341]) Vidjeti članak 88. IPA-e iz 2016.

([342]) Koristi mogu biti postojeće ili očekivane i moraju biti u skladu s propisanim svrhama za koje se podaci mogu zadržati (Kodeks dobre prakse za podatke o komunikacijama, točka 17.17., vidjeti bilješku 323.).

([343]) U okviru tih razmatranja treba utvrditi je li potpuni geografski doseg zahtjeva za zadržavanje nužan i proporcionalan te je li nužno i proporcionalno uključiti ili isključiti sve posebne opise osoba (Kodeks dobre prakse za podatke o komunikacijama, točka 17.17., vidjeti bilješku 323.).

([344]) To će pomoći ministru da razmotri i razinu zadiranja u privatnost klijenata, ali i vjerojatne koristi podataka koje treba zadržati (Kodeks dobre prakse za podatke o komunikacijama, točka 17.17., vidjeti bilješku 323.).

([345]) Članak 88. IPA-e iz 2016.

([346]) Članak 89. IPA-e iz 2016.

([347]) U skladu s člankom 135. stavkom 1. i člankom 198. stavkom 1. IPA-e iz 2016. „oprema" obuhvaća opremu koja proizvodi elektromagnetske, akustične ili druge emisije i svaki uređaj koji se može upotrijebiti u kombinaciji s takvom opremom.

([348]) Kodeks dobre prakse za ometanje opreme dostupan je na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, točka 2.2.

([349]) Podaci o opremi definirani su u članku 100. IPA-e iz 2016. kao podaci sustava i podaci koji (a) su sadržani u komunikaciji, čine njezin dio, priloženi su joj ili su logički povezani s njom (s obzirom na pošiljatelja ili na drugi način) ili svaka druga pojedinačna informacija; (b) se mogu logički odvojiti od ostatka komunikacije ili pojedinačne informacije; i (c) ako bi se tako odvojili, ne bi otkrili ništa što bi se moglo razumno smatrati značenjem (ako postoji) komunikacije ili pojedinačne informacije.

([350]) Kako bi zahtjev za izdavanje naloga bio obvezan, člankom 13. stavkom 1. IPA-e iz 2016. zahtijeva se i da postupak obavještajne službe čini jedno ili više kaznenih djela na temelju članaka od 1. do 3.A Zakona o zlouporabi računala iz 1990., što bi bio slučaj u velikoj većini situacija (vidjeti Kodeks dobre prakse za ometanje opreme, točka 3.32. i točke od 3.6. do 3.9.). U skladu s člankom 13. stavkom 2. IPA-e iz 2016. „poveznica s Britanskim otocima" postoji ako (a) se bilo koji od postupaka provodi na Britanskim otocima (bez obzira na lokaciju opreme koja bi se ometala ili bi se mogla ometati), (b) obavještajna služba smatra da bi se bilo koji dio opreme koja bi se ometala ili bi se mogla ometati nalazio ili bi se mogao nalaziti na Britanskim otocima u nekom trenutku dok se provodi ometanje ili (c) je svrha ometanja prikupiti i. komunikaciju koju šalje ili prima osoba koja se nalazi ili za koju obavještajna služba smatra da se trenutačno nalazi na Britanskim otocima, ii. privatne informacije koje se odnose na osobu koja se nalazi ili za koju obavještajna služba smatra da se trenutačno nalazi na Britanskim otocima ili iii. podatke o opremi koji su dio komunikacije ili privatnih informacija iz podtočaka i. ili ii. ili su povezani s njima.

primjene ove Odluke uvijek bi trebala postojati „poveznica s Britanskim otocima” te bi svako ometanje opreme koje obuhvaća takve podatke stoga bilo podložno obveznom zahtjevu za izdavanje naloga iz članka 13. stavka 1. IPA-e iz 2016. ([351])

(212) Pravila o nalozima za ciljano ometanje opreme navedena su u dijelu 5. IPA-e iz 2016. Slično ciljanom presretanju, ciljano ometanje opreme mora se odnositi na određeni „cilj” koji se mora navesti u nalogu ([352]). Pojedinosti o tome kako treba odrediti „cilj” ovise o pitanju i vrsti opreme koja će se ometati. U članku 115. stavku 3. IPA-e navode se elementi koje bi trebalo navesti u nalogu (npr. ime osobe ili organizacije, opis lokacije), ovisno primjerice o tome odnosi li se ometanje na opremu koja pripada određenoj osobi ili organizaciji ili skupini osoba ili je te osobe ili organizacije koriste ili je u njihovu posjedu, nalazi se na određenoj lokaciji itd. ([353]) Svrha za koju se mogu izdati nalozi za ciljano ometanje opreme ovisi o tijelu javne vlasti koje podnosi zahtjev za nalog ([354]).

(213) Slično kao i za ciljano presretanje, tijelo koje izdaje nalog mora razmotriti je li mjera nužna za postizanje određene svrhe i je li proporcionalna onome što se nastoji postići ([355]). Osim toga, trebalo bi razmotriti postoje li zaštitne mjere u pogledu sigurnosti, zadržavanja i otkrivanja kao i u pogledu „otkrivanja stranim tijelima” ([356]) (vidjeti uvodnu izjavu 196.).

(214) Nalog mora odobriti pravosudni povjerenik, osim u hitnim slučajevima ([357]). U potonjem slučaju pravosudnog povjerenika potrebno je obavijestiti da je izdan nalog i on ga mora odobriti u roku od tri radna dana. Ako pravosudni povjerenik odbije odobriti nalog, taj nalog prestaje važiti i nije ga moguće produljiti ([358]). Osim toga, pravosudni povjerenik ima ovlast zahtijevati da se svi podaci koji su prikupljeni na temelju naloga izbrišu ([359]). Činjenica da je nalog hitno izdan ne utječe na *ex post* nadzor (vidjeti uvodne izjave od 244. do 255.) niti na mogućnosti pojedinaca da traže sudsku zaštitu (vidjeti uvodne izjave od 260. do 270.). Pojedinci se mogu žaliti ICO-u ili podnijeti pritužbu na neko navodno postupanje Sudu za istražne ovlasti na uobičajeni način. U svim slučajevima provjera koju provodi pravosudni povjerenik kad odlučuje o tome hoće li odobriti nalog jest provjera nužnosti i proporcionalnosti koja se primjenjuje na zahtjeve za ciljano presretanje ([360]) (vidjeti prethodnu uvodnu izjavu 192.).

([351]) Radi potpunosti treba napomenuti da čak i u situacijama u kojima ne postoji „poveznica s Britanskim otocima” te stoga korištenje ometanja opreme nije podložno obveznom zahtjevu za izdavanje naloga iz članka 13. stavka 1. IPA-e iz 2016., obavještajna služba koja planira sudjelovati u aktivnosti za koju može dobiti nalog za masovno ometanje opreme trebala bi načelno ishoditi takav nalog (vidjeti Kodeks dobre prakse za ometanje opreme, točka 3.24.). Čak i ako na temelju IPA-e iz 2016. nalog za ometanje opreme nije zakonski obvezan niti se načelno ishodi, aktivnosti obavještajnih službi podliježu brojnim uvjetima i ograničenjima u skladu s člankom 7. Zakona o obavještajnim službama iz 1994. To posebno uključuje zahtjev za odobrenje ministra, koji se mora uvjeriti da bilo koja aktivnost ne prelazi ono što je potrebno za pravilno obavljanje funkcija obavještajne službe.

([352]) Člankom 115. IPA-e iz 2016. uređuje se sadržaj naloga i u njemu se navodi da je potrebno navesti ime ili opis osoba, organizacija, lokacije ili skupine osoba koje čine „cilj”, opis vrste istrage i opis aktivnosti za koje se oprema upotrebljava. U njemu se mora opisati i vrsta opreme i postupak koji je ovlaštena poduzeti osoba kojoj je izdan nalog.

([353]) Vidjeti i Kodeks dobre prakse za ometanje opreme, točka 5.7., vidjeti bilješku 348.

([354]) Nacionalne sigurnosne agencije mogu podnijeti zahtjev za izdavanje naloga za ometanje opreme ako je to potrebno radi nacionalne sigurnosti, u svrhu otkrivanja teških kaznenih djela i/ili ako je to u interesima gospodarske dobrobiti Ujedinjene Kraljevine koji su relevantni i za interese nacionalne sigurnosti (članci 102. i 103. IPA-e iz 2016.). Ovisno o agenciji, nalog za ometanje opreme može se zatražiti za potrebe kaznenog progona ako je to nužno za otkrivanje ili sprečavanje teških kaznenih djela ili u svrhu sprečavanja smrti ili ozljede ili bilo koje štete za tjelesno ili mentalno zdravlje osobe ili ublažavanja bilo koje ozljede ili štete za tjelesno ili mentalno zdravlje osobe (vidjeti članak 106. stavke 1. i 3. IPA-e iz 2016.).

([355]) Članak 102. stavak 1. IPA-e iz 2016.

([356]) Članci od 129. do 131. IPA-e iz 2016.

([357]) Članak 109. IPA-e iz 2016.

([358]) Članak 109. stavak 4. IPA-e iz 2016.

([359]) Članak 110. stavak 3. točka (b) IPA-e iz 2016. U skladu s točkom 5.67. Kodeksa dobre prakse za ometanje opreme, hitnost se utvrđuje na temelju toga bi li bilo razumno izvedivo zatražiti odobrenje pravosudnog povjerenika za izdavanje naloga u raspoloživom roku kako bi se ispunila operativna ili istražna potreba. Hitni nalozi trebali bi biti obuhvaćeni jednom ili objema sljedećim kategorijama: i. neposredna opasnost za život ili ozbiljna šteta, na primjer ako je pojedinac otet i ako se procijeni da je njegov život u neposrednoj opasnosti ili ii. mogućnost prikupljanja obavještajnih podataka ili istraga s ograničenim vremenom za djelovanje, na primjer ako bi pošiljka droge klase A uskoro trebala stići u Ujedinjenu Kraljevinu, a tijela kaznenog progona žele ometati opremu počinitelja teškog kaznenog djela kako bi mogla izvršiti uhićenja. Vidjeti bilješku 348.

([360]) Članak 108. IPA-e iz 2016.

(215) Naposljetku, posebne zaštitne mjere primjenjive na ciljano presretanje informacija koje podliježu obvezi čuvanja povjerljivosti i novinarskih materijala (više pojedinosti vidjeti u uvodnoj izjavi 193.) primjenjuju se i na ometanje opreme u pogledu trajanja, produljenja i izmjene naloga te na presretanje komunikacije zastupnika u Parlamentu.

3.3.1.1.4. Izvršavanje masovnih ovlasti

(216) Masovne ovlasti uređene su u dijelu 6. IPA-e iz 2016. Osim toga, u kodeksima dobre prakse predviđa se više pojedinosti o upotrebi masovnih ovlasti. Iako „masovne ovlasti" nisu definirane u zakonodavstvu Ujedinjene Kraljevine, u kontekstu IPA-e iz 2016. taj je pojam opisan kao prikupljanje i zadržavanje velikih količina podataka koje je vlada prikupila na različite načine (tj. ovlasti za masovno presretanje, masovno pribavljanje, masovno ometanje opreme i masovni skupovi osobnih podataka) kojima zatim mogu pristupiti tijela. Taj je opis pojašnjen u odnosu na ono što nije „masovna ovlast", odnosno to nije isto što i takozvani „masovni nadzor" bez ograničenja ili zaštitnih mjera. Naprotiv, kako je objašnjeno u nastavku, uključuje ograničenja i zaštitne mjere osmišljene kako bi se osiguralo da se pristup podacima ne omogućava na neselektivnoj ili neopravdanoj osnovi ([361]). Konkretnije, masovne ovlasti mogu se koristiti samo ako se uspostavi veza između tehničke mjere koju nacionalna obavještajna agencija namjerava koristiti i operativnih ciljeva za koje se takva mjera traži.

(217) Nadalje, masovne ovlasti dostupne su samo obavještajnim agencijama i uvijek podliježu nalogu koji izdaje ministar i odobrava pravosudni povjerenik. Pri odabiru sredstava za prikupljanje obavještajnih podataka potrebno je razmotriti može li se predmetni cilj ostvariti „manje nametljivim sredstvima" ([362]). Taj pristup proizlazi iz okvira zakonodavstva koji se temelji na načelu proporcionalnosti i u okviru kojeg ciljano prikupljanje ima prednost u odnosu na masovno.

3.3.1.1.4.1. Masovno presretanje i masovno ometanje opreme

(218) Sustav za masovno presretanje utvrđuje se u poglavlju 1. dijela 6. IPA-e iz 2016., dok se u poglavlju 3. istog dijela uređuje masovno ometanje opreme. Budući da su ti sustavi u znatnoj mjeri jednaki, uvjeti i dodatne zaštitne mjere koji se primjenjuju na te naloge analizirani su zajedno.

i. *Uvjeti i kriteriji za izdavanje naloga*

(219) Nalog za masovno presretanje ograničen je na presretanje komunikacija pri njihovu prijenosu koje šalju ili primaju osobe izvan Britanskih otoka ([363]), takozvane „komunikacije povezane s inozemstvom" ([364]), te drugih

([361]) Prema izvješću o masovnim ovlastima koje je iznio lord David Anderson, neovisni pregledavatelj zakonodavstva o terorizmu, prije donošenja IPA-e iz 2016., „treba biti jasno da masovno prikupljanje i zadržavanje podataka nije isto što i takozvani ‚masovni nadzor'. Svi pravni sustavi koji su dostojni tog naziva uključivat će ograničenja i zaštitne mjere osmišljene upravo kako bi se osiguralo da pristup mjestima na kojima su pohranjeni osjetljivi podaci […] nije moguć na neselektivnoj ili neopravdanoj osnovi. Takva ograničenja i zaštitne mjere svakako postoje u nacrtu zakona". Lord David Anderson, Izvješće o preispitivanju masovne ovlasti, kolovoz 2016., točka 1.9. (dodano isticanje), dostupno na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF.

([362]) Članak 2.2. IPA-e iz 2016. Vidjeti, na primjer, Kodeks dobre prakse za masovno pribavljanje podataka o komunikacijama, točka 4.11., dostupan na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf.

([363]) „Britanske otoke" čine Ujedinjena Kraljevina, Kanalski otoci i Otok Man te su definirani u Prilogu 1. Zakona o tumačenju iz 1978., koji je dostupan na: https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

([364]) U skladu s člankom 136. IPA-e iz 2016. „komunikacije povezane s inozemstvom" znači: i. komunikacije koje šalju pojedinci koji se nalaze izvan Britanskih otoka ili ii. komunikacije koje primaju pojedinci koji se nalaze izvan Britanskih otoka. Taj sustav, kako potvrđuju tijela Ujedinjene Kraljevine, obuhvaća i komunikaciju između dviju osoba koje se nalaze izvan Britanskih otoka. Veliko vijeće Europskog suda za ljudska prava u predmetu *Big Brother Watch i drugi protiv United Kingdom* (vidjeti prethodnu bilješku 279.), točka 376., utvrdilo je da je slično ograničenje (koje se odnosi na „vanjske komunikacije") komunikacija koje se mogu prikupiti masovnim presretanjem na temelju RIPA-e iz 2000. bilo dostatno ograničeno i predvidljivo.

relevantnih podataka i kasniji odabir presretnutog materijala za pregled ([365]). Nalogom za masovno ometanje opreme ([366]) adresat se ovlašćuje za ometanje opreme radi prikupljanja podataka o komunikacijama povezanima s inozemstvom (uključujući sve elemente govora, glazbe, zvuka, vizualne slike ili podatke bilo kojeg opisa), podataka o opremi (podaci kojima se omogućuje ili olakšava rad poštanske službe, telekomunikacijskog sustava, telekomunikacijske usluge) ili drugih informacija ([367]).

(220) Ministar može izdati masovni nalog samo na zahtjev voditelja obavještajne službe ([368]). Nalog kojim se odobrava masovno presretanje ili masovno ometanje opreme mora se izdati samo ako je to potrebno radi interesa nacionalne sigurnosti te u svrhu sprečavanja ili otkrivanja teških kaznenih djela ili u interesu gospodarske dobrobiti Ujedinjene Kraljevine kad je to relevantno za nacionalnu sigurnost ([369]). Nadalje, u članku 142. stavku 7. IPA-e iz 2016. zahtijeva se da u nalogu za masovno presretanje mora biti navedeno više pojedinosti od pukog upućivanja na „interese nacionalne sigurnosti", „gospodarsku dobrobit Ujedinjene Kraljevine" i „sprečavanje i suzbijanje teških kaznenih djela", ali se mora uspostaviti veza između mjere koja se traži i jedne ili više operativnih svrha koje se moraju navesti u nalogu.

(221) Odabir operativne svrhe rezultat je višeslojnog procesa. U članku 142. stavku 4. predviđeno je da operativne svrhe navedene u nalogu moraju na popisu koji vode voditelji obavještajnih službi biti utvrđene kao svrhe koje oni smatraju operativnim svrhama za koje se presretnuti sadržaj ili sekundarni podaci dobiveni na temelju naloga za masovno presretanje mogu odabrati za pregled. Popis operativnih svrha mora odobriti ministar. Ministar može dati takvo odobrenje samo ako se uvjeri da je operativna svrha opisana detaljnije od opće osnove za odobravanje naloga (nacionalna sigurnost i nacionalna sigurnost ili gospodarska dobrobit ili sprečavanje teških kaznenih djela) ([370]). Na kraju svakog relevantnog tromjesečnog razdoblja ministar mora dostaviti primjerak popisa operativnih svrha parlamentarnom Odboru za obavještajne poslove i sigurnost. Naposljetku, predsjednik Vlade mora preispitati popis operativnih svrha najmanje jednom godišnje ([371]). Kao što je istaknuo Visoki sud, „[o]ne se ne trebaju smatrati neznatnim zaštitnim mjerama jer zajedno čine složeni skup odgovornosti, koje uključuju Parlament i članove vlade na najvišoj razini" ([372]).

(222) Takvim se operativnim svrhama ujedno ograničava opseg odabira materijala za presretanje za fazu pregleda. Odabir svih materijala za pregled prikupljenih na temelju masovnog naloga mora biti opravdan s obzirom na jednu ili više operativnih svrha. Tijela Ujedinjene Kraljevine objasnila su da to znači da ministar već u fazi izdavanja naloga mora ocijeniti praktične postupke za pregled te pritom navesti dovoljno pojedinosti kako bi ispunio zakonske dužnosti iz članaka 152. i 193. IPA-e iz 2016. ([373]) Pojedinosti o tim postupcima koje se dostavljaju ministru trebale bi uključivati, na primjer, informacije (ako je primjenjivo) o načinu na koji postupci za filtriranje mogu varirati u razdoblju u kojem će nalog biti valjan ([374]). Za više pojedinosti o postupku i zaštitnim mjerama koje se primjenjuju u fazama filtriranja i pregleda vidjeti uvodnu izjavu 229.

([365]) Članak 136. stavak 4. IPA-e iz 2016. Prema objašnjenjima vlade Ujedinjene Kraljevine masovno presretanje može se upotrijebiti, na primjer, za utvrđivanje prethodno nepoznatih prijetnji nacionalnoj sigurnosti Ujedinjene Kraljevine filtriranjem i analizom materijala koji se presreće kako bi se utvrdile komunikacije koje imaju obavještajnu vrijednost (Okvir za objašnjenja Ujedinjene Kraljevine, odjeljak H: Nacionalna sigurnost, str. 27.–28., vidjeti bilješku 29.). Tijela Ujedinjene Kraljevine objasnila su da se ti instrumenti mogu koristiti kako bi se uspostavile poveznice između poznatih subjekata od interesa kao i za traženje tragova aktivnosti pojedinaca koji možda još nisu poznati, ali su se pojavili u tijeku ispitnog postupka te kako bi se utvrdili obrasci aktivnosti koji mogu ukazivati na prijetnju Ujedinjenoj Kraljevini.

([366]) U skladu s člankom 13. stavkom 1. IPA-e iz 2016., obavještajna služba mora dobiti odobrenje za ometanje opreme putem naloga koji se izdaje na temelju IPA-e iz 2016. pod uvjetom da postoji „poveznica s Britanskim otocima", vidjeti uvodnu izjavu 211.

([367]) Članak 176. IPA-e iz 2016. Nalogom za masovno ometanje opreme ne može se odobriti postupak koji bi (osim u slučaju zakonske ovlasti) predstavljao nezakonito presretanje (osim u vezi s pohranjenom komunikacijom). Prema Okviru za objašnjenja Ujedinjene Kraljevine dobivene informacije mogle bi biti potrebne za utvrđivanje subjekata od interesa i obično bi bile primjerene za opsežne operacije (Okvir za objašnjenja Ujedinjene Kraljevine, odjeljak H: Nacionalna sigurnost, str. 28., vidjeti bilješku 29.).

([368]) Članak 138. stavak 1. i članak 178. stavak 1. IPA-e iz 2016.

([369]) Članak 138. stavak 2. i članak 178. stavak 2. IPA-e iz 2016.

([370]) U skladu s objašnjenjima tijela Ujedinjene Kraljevine, na primjer, operativna svrha može ograničiti područje primjene mjere na postojanje prijetnje na određenom geografskom području.

([371]) Članak 142. stavci od 4. do 10. IPA-e iz 2016.

([372]) Visoki sud, predmet *Liberty* [2019] EWHC 2057 (Admin), točka 167.

([373]) Člancima 152. i 193. IPA-e iz 2016. zahtijeva se: (a) da se odabir za pregled provodi samo u operativne svrhe navedene u nalogu, (b) da je odabir za pregled nužan i proporcionalan u svim okolnostima i (c) da se odabirom za pregled ne krši zabrana odabira materijala i utvrđuju komunikacije koje su poslale osobe za koje je poznato da se u tom trenutku nalaze na Britanskim otocima ili koje su namijenjene tim osobama.

([374]) Vidjeti Kodeks dobre prakse za presretanje komunikacija, točka 6.6., vidjeti bilješku 278.

(223) Masovna ovlast može se odobriti samo ako je proporcionalna onome što se nastoji postići ([375]). Kako je navedeno u Kodeksu dobre prakse za presretanje, svaka ocjena proporcionalnosti uključuje „postizanje ravnoteže između zadiranja u privatnost (i druga razmatranja navedena u članku 2. stavku 2.) i potrebe za aktivnošću u istražnom, operativnom smislu ili smislu tehničkih sposobnosti. Odobreni postupak trebao bi pružiti realne izglede za ostvarivanje očekivane koristi i ne bi trebao biti neproporcionalan ili proizvoljan" ([376]). Kao što je već navedeno, to u praksi znači da se provjera proporcionalnosti temelji na testu ravnoteže između onoga što se nastoji postići („operativne svrhe") i dostupnih tehničkih opcija (npr. ciljano ili masovno presretanje, ometanje opreme, pribavljanje podataka o komunikacijama), čime se daje prednost najmanje nametljivim sredstvima (vidjeti uvodne izjave 181. i 182.). Ako se cilj može ostvariti s više različitih mjera, prednost se mora dati manje nametljivim sredstvima.

(224) Dodatna zaštitna mjera za ocjenu proporcionalnosti zatražene mjere osigurava se činjenicom da ministar mora dobiti relevantne informacije potrebne za pravilnu procjenu. Konkretno, u Kodeksu dobre prakse za presretanje i Kodeksu dobre prakse za ometanje opreme zahtijeva se da bi u zahtjevu koji podnosi relevantno tijelo trebalo navesti kontekst zahtjeva, opis komunikacija koje treba presresti i telekomunikacijske operatore čija se pomoć traži, opis postupka koji treba odobriti, operativne svrhe te objašnjenje o tome zašto je postupak nužan i proporcionalan ([377]).

(225) Naposljetku je važno istaknuti da odluku ministra o izdavanju naloga mora odobriti neovisni pravosudni povjerenik koji ocjenjuje evaluaciju nužnosti i proporcionalnosti predložene mjere primjenom istih načela kojima bi se koristio sud u zahtjevu za sudsko preispitivanje ([378]). Konkretnije, pravosudni povjerenik preispitat će zaključke ministra o tome je li nalog nužan te je li postupak proporcionalan u skladu s načelima utvrđenima u članku 2. stavku 2. IPA-e iz 2016. (opće obveze povezane s privatnošću). Pravosudni povjerenik ujedno će preispitati zaključke ministra o tome je li svaka od operativnih svrha navedenih u nalogu svrha za koju je potreban ili može biti potreban odabir. Ako pravosudni povjerenik odbije odobriti odluku o izdavanju naloga, ministar može: i. prihvatiti tu odluku i na temelju toga ne izdati nalog; ili ii. uputiti predmet na odlučivanje povjereniku za istražne ovlasti (osim ako je povjerenik za istražne ovlasti taj koji je donio prvotnu odluku) ([379]).

ii. *Dodatne zaštitne mjere*

(226) IPA-om iz 2016. uvedena su dodatna ograničenja u pogledu trajanja, produljenja i izmjene masovnog naloga. Nalog mora trajati najviše šest mjeseci, a pravosudni povjerenik mora odobriti i svaku odluku o produljenju ili izmjeni (osim manjih izmjena) naloga ([380]). U Kodeksu dobre prakse za presretanju i Kodeksu dobre prakse za ometanje opreme posebno se navodi da se promjena operativnih svrha naloga smatra znatnom izmjenom naloga ([381]).

([375]) Članak 138. stavak 1. točke (b) i (c) i članak 178. točke (b) i (c) IPA-e iz 2016.

([376]) Kodeks dobre prakse za presretanje komunikacija, točka 4.10., vidjeti bilješku 278.

([377]) Kodeks dobre prakse za presretanje komunikacija, točka 6.20., vidjeti bilješku 278. i Kodeks dobre prakse za ometanje opreme, točka 6.13., vidjeti bilješku 348.

([378]) Članak 138. stavak 1. točka (g) i članak 178. stavak 1. točka (f) IPA-e iz 2016. Europski sud za ljudska prava posebno je istaknuo prethodno odobrenje neovisnog tijela kao važnu zaštitnu mjeru protiv zloupotrebe u kontekstu masovnog presretanja. Europski sud za ljudska prava (Veliko vijeće), predmet *Big Brother Watch i drugi protiv United Kingdom*, (vidjeti prethodnu bilješku 269.), točke 351. i 352. Važno je imati na umu da se ta presuda odnosila na prethodni pravni okvir (RIPA iz 2000.) koji nije sadržavao neke od zaštitnih mjera (uključujući prethodno odobrenje neovisnog pravosudnog povjerenika) koje su uvedene IPA-om iz 2016.

([379]) Članak 159. stavci 3. i 4. IPA-e iz 2016.

([380]) Članci od 143. do 146. i članci od 184. do 188. IPA-e iz 2016. U slučaju hitne izmjene ministar može izvršiti izmjenu bez odobrenja, ali mora o tome obavijestiti povjerenika, a povjerenik potom mora odlučiti hoće li tu izmjenu odobriti ili odbiti (članak 147. IPA-e iz 2016.). Nalog se mora ukinuti ako više nije nužan ili proporcionalan ili ako pregled presretnutog sadržaja, metapodataka ili drugih podataka dobivenih na temelju naloga više nije potreban ni za jednu od operativnih svrha navedenih u nalogu (članci 148. i 189. IPA-e iz 2016.).

([381]) Kodeks dobre prakse za presretanje komunikacija, točke od 6.44. do 6.47., vidjeti bilješku 278. i Kodeks dobre prakse za ometanje opreme, točka 6.48., vidjeti bilješku 348.

(227) Slično kao što je propisano za ciljano presretanje, u dijelu 6. IPA-e iz 2016. predviđa se da ministar mora osigurati da su uspostavljeni mehanizmi za pružanje zaštitnih mjera u pogledu zadržavanja i otkrivanja materijala dobivenog na temelju naloga ([382]) i za otkrivanje stranim tijelima ([383]). Konkretno, člankom 150. stavkom 5. i člankom 191. stavkom 5. IPA-e iz 2016. zahtijeva se da se svaki primjerak materijala prikupljenoga na temelju naloga mora pohraniti na siguran način i uništiti čim više ne budu postojali relevantni razlozi za njegovo zadržavanje, dok se člankom 150. stavkom 2. i člankom 191. stavkom 2. zahtijeva da se broj osoba kojima se materijal otkriva i opseg otkrivanja, stavljanja na raspolaganje ili kopiranja tog materijala mora ograničiti na minimum koji je potreban za propisane svrhe ([384]).

(228) Naposljetku, kad se materijal koji je presretnut masovnim presretanjem ili masovnim ometanjem opreme prosljeđuje trećoj zemlji („otkrivanje stranim tijelima"), IPA-om iz 2016. predviđa se da ministar mora osigurati da su uspostavljeni odgovarajući dogovori kojima se jamči da u toj trećoj zemlji postoje slične zaštitne mjere u pogledu sigurnosti, zadržavanja i otkrivanja ([385]). Osim toga, člankom 109. DPA-a iz 2018. utvrđeni su posebni zahtjevi za međunarodne prijenose osobnih podataka trećoj zemlji ili međunarodnoj organizaciji koje vrše obavještajne službe te se ne dopušta prijenos podataka zemlji ili području izvan Ujedinjene Kraljevine ili međunarodnoj organizaciji, osim ako je prijenos nužan i proporcionalan za svrhu zakonom propisanih funkcija voditelja obrade ili druge svrhe predviđene u članku 2. stavku 2. točki (a) Zakona o sigurnosnim službama iz 1989. ili članku 2. stavku 2. točki (a) i članku 4. stavku 2. točki (a) Zakona o obavještajnim službama iz 1994. ([386]) Važno je napomenuti da se ti zahtjevi primjenjuju i u slučajevima u kojima se poziva na izuzeće radi nacionalne sigurnosti u skladu s člankom 110. DPA-a iz 2018. jer se u članku 110. DPA-a iz 2018. ne navodi da je članak 109. DPA-a iz 2018. jedna od odredbi koje se mogu izuzeti od primjene ako se u svrhu zaštite nacionalne sigurnosti zahtijeva izuzeće od određenih odredbi.

(229) Nakon što se nalog odobri i podaci se masovno prikupe, ti se podaci prije pregleda moraju odabrati. Faza odabira i pregleda podliježe dodatnoj provjeri proporcionalnosti koju provodi analitičar koji na temelju operativnih svrha navedenih u nalogu (i mogućih postojećih mehanizama filtriranja) definira kriterije odabira. Kako je predviđeno člancima 152. i 193. IPA-e, pri izdavanju naloga ministar mora osigurati da su uspostavljena rješenja kojima se jamči da se odabir materijala provodi isključivo za određene operativne svrhe i da je nužan i proporcionalan u svim okolnostima. Tijela Ujedinjene Kraljevine u tom su pogledu objasnila da se materijal koji se masovno presreće odabire prije svega automatskim filtriranjem kako bi se odbacili podaci za koje nije vjerojatno da su značajni za nacionalne sigurnosne interese. Filtri će se s vremena na vrijeme mijenjati (s obzirom na promjenu modela, vrsta i protokola internetskog prometa) te će ovisiti o tehnologiji i operativnom kontekstu. Nakon te faze podaci se mogu odabrati za pregled samo ako su relevantni za operativne svrhe navedene u nalogu ([387]). Zaštitne mjere predviđene IPA-om iz 2016. za pregled prikupljenog materijala primjenjuju se na bilo koju vrstu podataka (presretani sadržaj i sekundarni podaci) ([388]). U člancima 152. i 193. IPA-e iz 2016. predviđena je i opća zabrana odabira materijala za pregled koji se odnosi na razgovore koje su poslale osobe koje se nalaze na Britanskim otocima ili koji su namijenjeni tim osobama. Ako tijela žele pregledati takav materijal, podnose zahtjev za izdavanje naloga za ciljani pregled na temelju dijela 2. i dijela 4. IPA-e iz 2016. koji izdaje ministar i odobrava pravosudni povjerenik ([389]). Ako osoba za pregled namjerno odabere presretnuti sadržaj u suprotnosti sa zahtjevima iz zakonodavstva ([390]), ona čini kazneno djelo ([391]).

([382]) Članak 156. IPA-e iz 2016.

([383]) Članci 150. i 191. IPA-e iz 2016.

([384]) Veliko vijeće Europskog suda za ljudska prava u predmetu *Big Brother Watch i drugi protiv United Kingdom* (vidjeti prethodnu bilješku 268.) potvrdilo je sustav dodatnih zaštitnih mjera za zadržavanje, pristup i otkrivanje koji je predviđen RIPA-om iz 2000., vidjeti točke od 392. do 394. i od 402. do 405. Isti sustav zaštitnih mjera predviđen je IPA-om iz 2016.

([385]) Članci 151. i 192. IPA-e iz 2016.

([386]) Za više informacija o tim svrhama vidjeti bilješku 312.

([387]) U Kodeksu dobre prakse za presretanje komunikacije u tom se pogledu navodi: „Ti sustavi obrade obrađuju podatke iz komunikacijskih veza ili signala koje je tijelo koje provodi presretanje odabralo za presretanje. Potom se na promet na tim vezama i signalima primjenjuje određeni stupanj filtriranja, osmišljen za odabir vrsta komunikacije koje imaju potencijalnu obavještajnu vrijednost, dok se istodobno odbacuju komunikacije za koje je najmanje vjerojatno da imaju obavještajnu vrijednost. Na temelju tog filtriranja, koje će se razlikovati od jednog do drugog sustava obrade, znatan dio komunikacija na tim vezama i signalima automatski će se odbaciti. Potom se mogu provesti daljnja složena pretraživanja kako bi se izvukle dodatne komunikacije koje će najvjerojatnije biti od najveće obavještajne vrijednosti i koje su povezane sa zakonskim funkcijama agencije. Te se komunikacije potom mogu odabrati za pregled za jednu ili više operativnih svrha navedenih u nalogu ako su ispunjeni uvjeti nužnosti i proporcionalnosti. Samo oni dijelovi komunikacija koji nisu filtrirani mogu se odabrati za pregled koji obavljaju ovlaštene osobe." (Kodeks dobre prakse za presretanje komunikacija, točka 6.6., vidjeti bilješku 278.)

([388]) Vidjeti članak 152. stavak 1. točke (a) i (b) IPA-e iz 2016. prema kojima se pregled obiju vrsta podataka (presretnuti sadržaj i sekundarni podaci) mora provoditi samo za određenu svrhu i biti nužan i proporcionalan u svim okolnostima.

([389]) Ta vrsta naloga nije potrebna kad su podaci koji se odnose na pojedince koji se nalaze na Britanskim otocima „sekundarni podaci" (vidjeti članak 152. stavak 1. točku (c) IPA-e iz 2016.).

([390]) Članci 152. i 193. IPA-e iz 2016.

([391]) Članci 155. i 196. IPA-e iz 2016.

(230) Ocjena koju provodi analitičar u vezi s odabirom materijala podliježe *ex post* nadzoru IPC-a koji ocjenjuje usklađenost s posebnim zaštitnim mjerama iz IPA-e iz 2016. za fazu pregleda ([392]) (vidjeti i uvodnu izjavu 229.). IPC mora preispitivati (među ostalim u okviru revizije, inspekcije i istrage) način na koji tijela javne vlasti izvršavaju ovlasti utvrđene u IPA-i iz 2016. ([393]) U Kodeksu dobre prakse za presretanje i Kodeksu dobre prakse za ometanje opreme u tom se pogledu pojašnjava da agencija mora voditi evidenciju radi naknadnih provjera i revizija, a u njoj se mora navesti zašto je pristup ovlaštenih osoba materijalu nužan i proporcionalan te primjenjive operativne svrhe ([394]). Na primjer, u Godišnjem izvješću za 2018. Ureda povjerenika za istražne ovlasti (IPCO) ([395]) zaključeno je da obrazloženja koja su analitičari naveli za pregled određenog masovno prikupljenog materijala zadovoljavaju traženi standard proporcionalnosti jer su naveli dostatne pojedinosti o razlozima svojih „pretraživanja" u odnosu na svrhu koju treba ostvariti ([396]). U svojem izvješću za 2019. IPCO je, u odnosu na masovne ovlasti, jasno izrazio namjeru da nastavi s inspekcijama masovnih presretanja, uključujući detaljan pregled selektora i kriterija pretraživanja ([397]). Ujedno će pri razmatranju zahtjeva za izdavanje naloga nastaviti pažljivo kontrolirati u svakom pojedinačnom slučaju izbor mjera nadzora (ciljane u odnosu na masovne) u okviru postupka dvostruke zaštite i pri provedbi inspekcija ([398]). To daljnje praćenje propisno će se uzeti u obzir u kontekstu praćenja Komisije povezanoga s ovom Odlukom iz uvodnih izjava od 281. do 284.

3.3.1.1.4.2. Masovno pribavljanje podataka o komunikacijama

(231) U poglavlju 2. dijela 6. IPA-e iz 2016. uređuju se nalozi za masovno prikupljanje kojima se adresat ovlašćuje da od telekomunikacijskog operatera zahtijeva da otkrije ili pribavi podatke o komunikacijama kojima raspolaže. Tim nalozima tijelo koje podnosi zahtjev ovlašćuje se i da odabere podatke za daljnju fazu pregleda. Jednako kao i u slučaju ciljanog zadržavanja i pribavljanja podataka o komunikacijama (vidjeti uvodnu izjavu 199.), masovno pribavljanje podataka o komunikacijama obično se ne odnosi na osobne podatke ispitanika iz EU-a koji se u skladu s ovom Odlukom prenose u Ujedinjenu Kraljevinu. Obveza otkrivanja podataka o komunikacijama u skladu s poglavljem 2. dijela 6. IPA-e iz 2016. obuhvaća podatke koje su prikupili telekomunikacijski operateri u Ujedinjenoj Kraljevini izravno od korisnika telekomunikacijske usluge ([399]). Ta vrsta obrade „u izravnom kontaktu s klijentom" obično ne uključuje prijenos na temelju ove Odluke, tj. prijenos od voditelja obrade/izvršitelja obrade u EU-u voditelju obrade/izvršitelju obrade u Ujedinjenoj Kraljevini.

(232) Međutim, radi potpunosti, u nastavku su opisani uvjeti i zaštitne mjere kojima se uređuje pribavljanje masovnih podataka o komunikacijama.

([392]) Članci 152. i 193. IPA-e iz 2016.

([393]) Članak 229. IPA-e iz 2016.

([394]) Kodeks dobre prakse za presretanje komunikacija, točka 6.74., vidjeti bilješku 278. i Kodeks dobre prakse za ometanje opreme, točka 6.78., vidjeti bilješku 348.

([395]) IPCO je uspostavljen na temelju članka 238. IPA-e iz 2016. kako bi se IPC-u osiguralo potrebno osoblje, prostor, oprema te druga sredstva i usluge potrebni za obavljanje njegovih funkcija (vidjeti uvodnu izjavu 251.).

([396]) U godišnjem izvješću IPCO-a za 2018. navodi se da su obrazloženja koja su zabilježili analitičari GCHQ-a „zadovoljavala potreban standard i da su analitičari dovoljno detaljno obrazložili proporcionalnost svojih zahtjeva za velike količine podataka". Godišnje izvješće povjerenika za istražne ovlasti za 2018., točka 6.22., vidjeti bilješku 464.

([397]) Godišnje izvješće povjerenika za istražne ovlasti za 2019., točka 7.6., vidjeti bilješku 463.

([398]) Godišnje izvješće povjerenika za istražne ovlasti za 2019., točka 10.22., vidjeti bilješku 463.

([399]) To proizlazi iz definicije podataka o komunikacijama iz članka 261. stavka 5. IPA-e iz 2016., prema kojoj podatke o komunikacijama čuva ili prikuplja telekomunikacijski operater te se ti podaci odnose na korisnika telekomunikacijske usluge i povezani su s pružanjem te usluge ili su sadržani u komunikaciji, čine njezin dio, priloženi su joj ili su logički povezani s njom (vidjeti i Kodeks dobre prakse za masovno pribavljanje podataka o komunikacijama dostupan na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, točke od 2.15. do 2.22.). Osim toga, definicija telekomunikacijskog operatera utvrđena u članku 261. stavku 10. IPA-e iz 2016. zahtijeva da je telekomunikacijski operater osoba koja nudi ili pruža telekomunikacijsku uslugu osobama u Ujedinjenoj Kraljevini ili koja kontrolira ili pruža telekomunikacijski sustav koji se (u cijelosti ili djelomično) nalazi u Ujedinjenoj Kraljevini ili se njime upravlja iz te zemlje. Te definicije pojašnjavaju da se obveze na temelju IPA-e iz 2016. ne mogu nametnuti telekomunikacijskim operatorima čija se oprema ne nalazi u Ujedinjenoj Kraljevini ili se njome ne upravlja iz te zemlje ili koji ne nude niti pružaju usluge osobama u Ujedinjenoj Kraljevini (vidjeti i Kodeks dobre prakse za masovno pribavljanje podataka o komunikacijama, točka 2.2.). Ako pretplatnici u EU-u (bez obzira na to nalaze li se u EU-u ili u Ujedinjenoj Kraljevini) koriste usluge u Ujedinjenoj Kraljevini, sve komunikacije povezane s pružanjem te usluge izravno prikuplja pružatelj usluga u Ujedinjenoj Kraljevini te se one ne prenose iz EU-a.

(233) IPA-om iz 2016. zamjenjuje se zakonodavstvo o pribavljanju masovnih podataka o komunikacijama koje je predmet presude Suda Europske unije u predmetu *Privacy International*. Zakonodavstvo o kojem je riječ u tom predmetu stavljeno je izvan snage, a novim se sustavom predviđaju posebni uvjeti i zaštitne mjere u okviru kojih se takva mjera može odobriti.

(234) Konkretnije, za razliku od prethodnog sustava na temelju kojeg je ministar imao pune diskrecijske ovlasti za odobravanje mjere ([400]) IPA-om iz 2016. zahtijeva se da ministar izdaje nalog samo ako je mjera nužna i proporcionalna. To u praksi znači da bi trebala postojati veza između pristupa podacima i cilja koji se želi postići ([401]). Točnije, ministar će morati ocijeniti postoji li veza između zatražene mjere i jedne ili više „operativnih svrha" navedenih u nalogu (vidjeti uvodnu izjavu 219.) u pogledu ocjene proporcionalnosti; u odgovarajućem kodeksu dobre prakse navodi se da „ministar mora uzeti u obzir je li se ono što se nastoji postići nalogom moglo razumno ostvariti drugim manje nametljivim sredstvima (članak 2. stavak 2. točka (a) Zakona). Na primjer, dobivanje potrebnih informacija s pomoću manje nametljivih ovlasti kao što je ciljano pribavljanje podataka o komunikacijama" ([402]).

(235) Ministar će takvu ocjenu provesti na temelju informacija koje su voditelji obavještajnih službi ([403]) dužni dostaviti u svojem zahtjevu, kao što su razlozi zbog kojih se mjera smatra nužnom na temelju jedne od zakonskih osnova i razlozi zbog kojih se ono što se nastoji postići nije moglo razumno ostvariti drugim manje nametljivim sredstvima ([404]). Nadalje, operativnim svrhama ograničava se opseg za koji se podaci prikupljeni na temelju naloga mogu odabrati za pregled ([405]). Kako je navedeno u relevantnom kodeksu dobre prakse, u operativnim svrhama mora biti naveden jasan zahtjev te one moraju sadržavati dovoljno pojedinosti kako bi se ministar uvjerio da se pribavljeni podaci mogu odabrati za pregled samo za određene razloge ([406]). Ministar će zapravo prije odobravanja naloga morati osigurati da postoje posebni postupci kojima se osigurava da je za pregled odabran samo onaj materijal koji se smatra potrebnim za pregled za operativnu i zakonski propisanu svrhu i da su ti postupci proporcionalni i nužni u svim okolnostima. Taj posebni zahtjev, koji se odražava u člancima 158. i 172. ([407]) IPA-e iz 2016., u pogledu prethodne procjene nužnosti i proporcionalnosti kriterija koji se upotrebljavaju u svrhe odabira još je jedna važna novost sustava uvedenog IPA-om iz 2016. u usporedbi s prethodnim sustavom.

(236) IPA-om iz 2016. uvedena je i obveza da ministar osigura, prije nego što izda nalog za masovno pribavljanje podataka o komunikacijama, da postoje posebna ograničenja u pogledu sigurnosti, zadržavanja i otkrivanja prikupljenih osobnih podataka ([408]). U slučaju otkrivanja stranim tijelima zaštitne mjere opisane u uvodnoj izjavi 227. za masovno presretanje i masovno ometanje opreme primjenjuju se i u ovom kontekstu ([409]). Dodatna ograničenja uspostavljena su u zakonodavstvu o trajanju ([410]), produljenju ([411]) i izmjeni masovnih naloga ([412]).

(237) Važno je napomenuti da, kao i za ostale masovne ovlasti, prije izdavanja naloga ministar mora dobiti odobrenje pravosudnog povjerenika ([413]). To je ključna značajka sustava uspostavljenog IPA-om iz 2016.

([400]) U članku 94. stavku 1. Zakona o telekomunikacijama iz 1984. predviđeno je da ministar može izdati „opće smjernice koje ministar smatra potrebnima ili primjerenima u interesu nacionalne sigurnosti […]" (vidjeti bilješku 451.).

([401]) Vidjeti predmet *Privacy International*, točku 78.

([402]) Vidjeti Kodeks dobre prakse za masovno pribavljanje podataka o komunikacijama, točku 4.11. (vidjeti bilješku 399414.).

([403]) Nalog za masovno pribavljanje mogu zatražiti samo voditelji obavještajnih službi, a to su: i. glavni direktor Sigurnosne službe; ii. šef Tajne obavještajne službe; iii. direktor GCHQ-a (vidjeti članke 158. i 263. IPA-e iz 2016.).

([404]) Kodeks dobre prakse za masovno pribavljanje podataka o komunikacijama, točka 4.5. (vidjeti bilješku 399.).

([405]) Prema članku 161. IPA-e iz 2016., operativne svrhe navedene u nalogu moraju na popisu koji vode voditelji obavještajnih službi („popis operativnih svrha") biti utvrđene kao svrhe koje oni smatraju operativnim svrhama za koje se podaci o komunikacijama dobiveni na temelju naloga za masovno pribavljanje mogu odabrati za pregled.

([406]) Kodeks dobre prakse za masovno pribavljanje podataka o komunikacijama, točka 6.6. (vidjeti bilješku 399.).

([407]) Člankom 172. IPA-e iz 2016. zahtijeva se uspostavljanje posebnih zaštitnih mjera za fazu filtriranja i odabira za pregled masovno pribavljene komunikacije. Osim toga, pregled koji se namjerno provodi protivno tim zaštitnim mjerama ujedno je kazneno djelo (vidjeti članak 173. IPA-e iz 2016.).

([408]) Članak 171. IPA-e iz 2016.

([409]) Članak 171. stavak 9. IPA-e iz 2016.

([410]) Članak 162. IPA-e iz 2016.

([411]) Članak 163. IPA-e iz 2016.

([412]) Članci od 164. do 166. IPA-e iz 2016.

([413]) Članak 159. IPA-e iz 2016.

(238) IPC provodi *ex post* nadzor nad postupkom ispitivanja masovno pribavljenog materijala (podataka o komunikacijama) (vidjeti uvodnu izjavu 254. u nastavku). U tom pogledu IPA-om iz 2016. uveden je zahtjev da obavještajni analitičar koji provodi pregled mora prije odabira podataka za pregled zabilježiti zašto je predloženi pregled nužan i proporcionalan za određenu operativnu svrhu ([414]). U godišnjem izvješću IPCO-a za 2019. utvrđeno je u pogledu aktivnosti GCHQ-a i službe MI5, da je „ključna uloga masovnih podataka o komunikacijama za niz aktivnosti koje je proveo GCHQ bila dobro obrazložena u predmetima koje smo pregledali. Uzeli smo u obzir prirodu traženih podataka i navedene zahtjeve obavještajnih službi te smo bili zadovoljni time što je dokumentacija pokazala da je njihov pristup nužan i proporcionalan ([415]). Obrazloženja koje je naveo MI5 su bila prikladna te su zadovoljila načela nužnosti i proporcionalnosti" ([416]).

3.3.1.1.4.3. Zadržavanje i pregled masovnih skupova osobnih podataka

(239) Nalozi za prikupljanje masovnih skupova osobnih podataka (*bulk personal dataset*, BPD) ([417]) ovlašćuju obavještajne agencije za zadržavanje i pregled skupova podataka koji sadržavaju osobne podatke koji se odnose na više pojedinaca. U skladu s objašnjenjima tijela Ujedinjene Kraljevine analiza tih skupova podataka može biti „jedini način da obavještajna zajednica Ujedinjene Kraljevine provede istrage i identificira teroriste na temelju vrlo ograničenih početnih obavještajnih informacija ili ako oni namjerno prikrivaju svoje komunikacije" ([418]). Postoje dvije vrste naloga: „nalozi za razred BPD-a" ([419]) koji se odnose na određenu kategoriju skupova podataka, tj. skupove podataka sličnog sadržaja i predložene uporabe u pogledu kojih se postavljaju slična pitanja, primjerice o razini zadiranja u privatnost i osjetljivosti te proporcionalnosti upotrebe podataka, te tako omogućuju ministru da razmotri nužnost i proporcionalnost pribavljanja podataka iz relevantnog razreda odjednom. Na primjer, u nalogu za razred BPD-a mogu se obuhvatiti skupovi podataka o putovanjima koji se odnose na slične rute ([420]). Za razliku od toga, „nalog za određeni BPD" ([421]) odnosi se na jedan konkretan skup podataka, kao što je skup novih ili neuobičajenih vrsta informacija koje nisu obuhvaćene postojećim nalogom za razred BPD-a, ili na skup podataka koji se odnosi na određene vrste osobnih podataka ([422]) i stoga su potrebne dodatne zaštitne mjere ([423]). Odredbama IPA-e iz 2016. koje se odnose na BPD-ove omogućuje se ispitivanje i zadržavanje takvih skupova podataka samo ako je to nužno i proporcionalno ([424]) i u skladu s općim obvezama koje se odnose na privatnost ([425]).

(240) Ovlast za izdavanje naloga za BPD podložna je postupku „dvostruke zaštite", što znači da procjenu nužnosti i proporcionalnosti mjere prvo provodi ministar, a zatim pravosudni povjerenik ([426]). Od ministra se zahtijeva da uzme u obzir prirodu i opseg tražene vrste naloga, kategoriju predmetnih podataka i broj masovnih skupova osobnih podataka koji će vjerojatno biti obuhvaćeni određenom vrstom naloga ([427]). Osim toga, kako je utvrđeno u Kodeksu dobre prakse za zadržavanje i korištenje masovnih skupova osobnih podataka u obavještajnim službama, potrebno je voditi detaljnu evidenciju koja je podložna reviziji IPC-a ([428]). Zadržavanje i pregled BPD-a izvan granica IPA-e iz 2016. kazneno je djelo ([429]).

([414]) Godišnje izvješće IPCO za 2019., točka 8.6., vidjeti bilješku 463.
([415]) Godišnje izvješće IPCO za 2019., točka 10.4., vidjeti bilješku 463.
([416]) Godišnje izvješće IPCO za 2019., točka 8.37., vidjeti bilješku 463.
([417]) Članak 200. IPA-e iz 2016.
([418]) Okvir za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, odjeljak H: Nacionalna sigurnost, str. 34., vidjeti bilješku 29.
([419]) Članak 204. IPA-e iz 2016.
([420]) Kodeks dobre prakse za zadržavanje i korištenje masovnih skupova osobnih podataka u obavještajnim službama, točka 4.7., dostupan na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf.
([421]) Članak 205. IPA-e iz 2016.
([422]) Kao što su, na primjer, osjetljivi osobni podaci, vidjeti članak 202. IPA-e iz 2016. i Kodeks dobre prakse za zadržavanje i korištenje masovnih skupova osobnih podataka u obavještajnim službama, točke 4.21. i 4.12., vidjeti bilješku 469.
([423]) Ministar mora pojedinačno razmotriti svaki zahtjev za izdavanje naloga za određeni BPD, tj. u odnosu na jedan određeni skup podataka. Od obavještajne službe člankom 205. IPA-e zahtijeva se da u svojem zahtjevu za izdavanje naloga za određeni BPD navede detaljno objašnjenje vrste i opsega predmetnog materijala te popis „operativnih svrha" za koje relevantna obavještajna služba želi pregledati BPD (ako obavještajna služba traži izdavanje naloga za zadržavanje i pregled, a ne samo zadržavanje podataka). Za razliku od toga, pri izdavanju naloga za razred BPD-a ministar odjednom razmatra cijelu kategoriju skupova podataka.
([424]) Članci 204. i 205. IPA-e iz 2016.
([425]) Članak 2. IPA-e iz 2016.
([426]) Članci 204. i 205. IPA-e iz 2016.
([427]) Kodeks dobre prakse za zadržavanje i korištenje masovnih skupova osobnih podataka u obavještajnim službama, točka 5.2., vidjeti bilješku 420.
([428]) Kodeks dobre prakse za zadržavanje i korištenje masovnih skupova osobnih podataka u obavještajnim službama, točke od 8.1. do 8.15., vidjeti bilješku 420.
([429]) Okvir za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, odjeljak H: Nacionalna sigurnost, str. 34., vidjeti bilješku 29.

3.3.2. *Daljnja uporaba prikupljenih informacija*

(241) Osobni podaci koji se obrađuju na temelju dijela 4. DPA-a iz 2018. ne smiju se obrađivati na način koji nije u skladu sa svrhom za koju su prikupljeni ([430]). DPA-om iz 2018. predviđa se da voditelj obrade može obrađivati podatke u drugu svrhu koja se razlikuje od one za koju su podaci prikupljeni ako je u skladu s izvornom svrhom i pod uvjetom da je voditelj obrade zakonski ovlašten obrađivati podatke te da je obrada nužna i proporcionalna ([431]). Nadalje, Zakonom o sigurnosnim službama iz 1989. i Zakonom o obavještajnim službama iz 1994. utvrđeno je da su voditelji obavještajnih agencija dužni osigurati da se nikakvi podaci ne prikupljaju ili otkrivaju osim u mjeri u kojoj je to potrebno za pravilno obavljanje funkcija agencije ili za druge ograničene i posebne svrhe navedene u relevantnim odredbama ([432]).

(242) Osim toga, u članku 109. DPA-a iz 2018. utvrđeni su posebni zahtjevi za međunarodne prijenose osobnih podataka koje obavještajne službe prenose trećim zemljama ili međunarodnim organizacijama. U skladu s tom odredbom ne dopušta se prijenos osobnih podataka zemlji ili području izvan Ujedinjene Kraljevine ili međunarodnoj organizaciji, osim ako je prijenos nužan i proporcionalan za svrhu zakonom propisanih funkcija voditelja obrade ili druge svrhe predviđene u članku 2. stavku 2. točki (a) Zakona o sigurnosnim službama iz 1989. ili članku 2. stavku 2. točki (a) i članku 4. stavku 2. točki (a) Zakona o obavještajnim službama iz 1994. ([433]) Važno je napomenuti da se ti zahtjevi primjenjuju i u slučajevima u kojima se poziva na izuzeće radi nacionalne sigurnosti u skladu s člankom 110. DPA-a iz 2018. jer se u članku 110. DPA-a iz 2018. ne navodi da je članak 109. DPA-a iz 2018. jedna od odredbi koje se mogu izuzeti od primjene ako se u svrhu zaštite nacionalne sigurnosti zahtijeva izuzeće od određenih odredbi.

(243) Štoviše, kako je ICO istaknuo u svojim smjernicama za obradu podatka koju provode obavještajne službe, uz zaštitne mjere predviđene dijelom 4. DPA-a iz 2018., i obavještajna agencija, kad dijeli podatke s obavještajnim tijelom treće zemlje, podliježe zaštitnim mjerama predviđenima drugim zakonodavnim mjerama koje se primjenjuju na ta tijela kako bi se osiguralo da se osobni podaci pribavljaju, dijele te da se s njima postupa na odgovoran i zakonit način ([434]). Primjerice, IPA-om iz 2016. utvrđuju se dodatne zaštitne mjere u pogledu prijenosa trećoj zemlji materijala prikupljenih ciljanim presretanjem ([435]), ciljanim ometanjem opreme ([436]), masovnim presretanjem ([437]), masovnim pribavljanjem podataka o komunikacijama ([438]) i masovnim ometanjem opreme ([439]) (tzv. „otkrivanja stranim tijelima"). Konkretno, tijelo koje izdaje nalog mora osigurati da postoje dogovori kojima se osigurava da treća zemlja koja prima podatke ograničava broj osoba kojima se otkriva materijal, opseg otkrivanja i broj primjeraka bilo kojeg materijala na minimum nužan za odobrene svrhe navedene u IPA-i iz 2016. ([440])

3.3.3. *Nadzor*

(244) Pristup vlade za potrebe nacionalne sigurnosti nadzire niz različitih tijela. Povjerenik za informiranje nadzire obradu osobnih podataka u smislu DPA-a iz 2018. (za više informacija o neovisnosti, imenovanju, ulozi i ovlastima povjerenika vidjeti uvodne izjave od 85. do 98.), dok neovisni i sudski nadzor nad primjenom istražnih ovlasti na

([430]) Članak 87. stavak 1. DPA-a iz 2018.

([431]) Članak 87. stavak 3. DPA-a iz 2018. Iako se voditelji obrade mogu izuzeti od tog načela u skladu s člankom 110. DPA-a iz 2018. u mjeri u kojoj je takvo izuzeće potrebno za zaštitu nacionalne sigurnosti, takvo izuzeće mora se procijeniti za svaki slučaj pojedinačno i može se primijeniti samo ako bi primjena određene odredbe imala negativne posljedice za nacionalnu sigurnost (vidjeti uvodnu izjavu 132.). Potvrde o nacionalnoj sigurnosti za obavještajne službe Ujedinjene Kraljevine (dostupne na: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/)) ne obuhvaćaju članak 87. stavak 3. DPA-a iz 2018. Osim toga, budući da svaka obrada u drugu svrhu mora biti dopuštena zakonom, obavještajne službe moraju imati jasnu pravnu osnovu za daljnju obradu.

([432]) Za dodatne informacije o tim svrhama vidjeti bilješku 312.

([433]) Vidjeti bilješku 312.

([434]) Smjernice ICO-a za obradu koju provode obavještajne službe (vidjeti bilješku 161.).

([435]) Članak 54. IPA-e iz 2016.

([436]) Članak 130. IPA-e iz 2016.

([437]) Članak 151. IPA-e iz 2016.

([438]) Članak 171. stavak 9. IPA-e iz 2016.

([439]) Članak 192. IPA-e iz 2016.

([440]) Ti dogovori moraju uključivati mjere kojima se osigurava da se svaki primjerak tog materijala čuva na siguran način sve dok se zadržava. Materijal dobiven na temelju naloga i svaki primjerak bilo kojeg dijela tog materijala mora se uništiti čim više nema relevantnih razloga za njegovo zadržavanje (vidjeti članak 150. stavke 2. i 5. te članak 151. stavak 2. IPA-e iz 2016.). Treba istaknuti da je utvrđeno da su slične zaštitne mjere, predviđene prethodnim pravnim okvirom (RIPA iz 2000)., u skladu sa zahtjevima Europskog suda za ljudska prava za razmjenu materijala dobivenog masovnim presretanjem s trećim zemljama ili međunarodnim organizacijama (Sud za ljudska prava (Veliko vijeće), *Big Brother Watch i drugi protiv United Kingdom*, (vidjeti prethodnu bilješku 279.), točke 362. i 399).

temelju IPA-e iz 2016. osigurava IPC. IPC nadzire način na koji tijela za kazneni progon i tijela nacionalne sigurnosti primjenjuju istražne ovlasti iz IPA-e iz 2016. Politički nadzor osigurava Odbor Parlamenta za obavještajne službe.

3.3.3.1. Nadzor na temelju dijela 4. DPA-a

(245) Obradu osobnih podataka koju obavljaju obavještajne službe na temelju dijela 4. DPA-a iz 2018. nadzire Povjerenik za informiranje ([441]).

(246) Opće funkcije povjerenika za informiranje u pogledu obrade osobnih podataka koju obavljaju obavještajne službe na temelju dijela 4. DPA-a iz 2018. utvrđene su u Prilogu 13. DPA-u iz 2018. Te zadaće obuhvaćaju, ali nisu ograničene na, praćenje i provedbu dijela 4. DPA-a iz 2018., promicanje javne svijesti, savjetovanje Parlamenta, vlade i drugih institucija o zakonodavnim i upravnim mjerama, informiranje voditelja obrade i izvršitelja obrade o njihovim obvezama, davanje informacija ispitanicima o ostvarivanju njihovih prava, provođenje istraga itd.

(247) Povjerenik je, kao i za dio 3. DPA-a iz 2018., ovlašten obavijestiti voditelje obrade o navodnom kršenju pravila te izdavati upozorenja o tome da će se obradom vjerojatno prekršiti pravila i izdavati opomene u slučaju potvrde kršenja pravila. Može izdavati i zahtjeve za izvršenje i rješenja o kazni zbog kršenja određene odredbe zakona ([442]). Međutim, za razliku od situacije s drugim dijelovima DPA-a iz 2018., povjerenik ne može izdavati zahtjev za provjeru nacionalnom sigurnosnom tijelu ([443]).

(248) Nadalje, u članku 110. DPA-a iz 2018. predviđa se iznimka od primjene određenih ovlasti povjerenika kad je to potrebno radi zaštite nacionalne sigurnosti. To uključuje ovlast povjerenika da izdaje zahtjeve i rješenja (bilo koje vrste) na temelju DPA-a (zahtjevi za dostavu informacija, provjeru i izvršenje te rješenja o kazni), ovlast provođenja inspekcija u skladu s međunarodnim obvezama, ovlasti ulaska i inspekcije te pravila o kaznenim djelima ([444]). Kako je objašnjeno u uvodnoj izjavi 126., te se iznimke primjenjuju samo ako je to nužno i proporcionalno te na pojedinačnoj osnovi.

(249) ICO i obavještajne službe Ujedinjene Kraljevine potpisale su Memorandum o razumijevanju ([445]) kojim se uspostavlja okvir za suradnju u brojnim pitanjima, uključujući obavijesti o povredi podataka i postupanje s pritužbama ispitanika. Konkretno, njime se predviđa da će ICO nakon zaprimanja pritužbe provjeriti je li primjena izuzeća radi nacionalne sigurnosti odgovarajuća. Odgovore na upite ICO-a u kontekstu ispitivanja pojedinačnih pritužbi predmetna obavještajna agencija mora dati u roku od 20 radnih dana, koristeći odgovarajuće sigurne kanale ako odgovori uključuju klasificirane podatke. Od travnja 2018. do danas ICO je zaprimio 21 pritužbu koju su podnijeli pojedinci u pogledu rada obavještajnih službi. Svaka je pritužba provjerena te je ispitanik obaviješten o ishodu provjere ([446]).

([441]) Članak 116. DPA-a iz 2018.

([442]) U skladu s točkom 2. Priloga 13. DPA-u iz 2018. voditelju obrade ili izvršitelju obrade mogu se izdati zahtjevi za izvršenje i rješenja o kazni u vezi s kršenjima dijela 4. poglavlja 2. DPA-a iz 2018. (načela obrade), odredbe iz dijela 4. DPA-a iz 2018. o davanju prava ispitaniku, zahtjeva za obavještavanje povjerenika o povredama osobnih podataka na temelju članka 108. DPA-a iz 2018. i načelâ za prijenos osobnih podataka trećim zemljama, državama koje nisu potpisnice Konvencije i međunarodnim organizacijama iz članka 109. DPA-a iz 2018. (za dodatne pojedinosti o zahtjevu za izvršenje i rješenju o kazni vidjeti uvodnu izjavu 92.).

([443]) U skladu s člankom 147. stavkom 6. DPA-a iz 2018. povjerenik za informiranje ne smije izdati zahtjev za provjeru tijelu iz članka 23. stavka 3. Zakona o slobodi informiranja iz 2000. To uključuje Sigurnosnu službu (MI5), Tajnu obavještajnu službu (MI6) i Vladin komunikacijski stožer.

([444]) Mogu se izuzeti sljedeće odredbe: članak 108. (obavješćivanje povjerenika o povredi osobnih podataka), članak 119. (inspekcija u skladu s međunarodnim obvezama); članci od 142. do 154. i Prilog 15. (zahtjevi i rješenja te ovlasti povjerenika za ulazak i inspekciju); članci od 170. do 173. (kažnjiva djela povezana s osobnim podacima). Osim toga, u pogledu obrade koju obavljaju obavještajne službe u Prilogu 13. (ostale opće funkcije povjerenika), točki 1. podtočkama (a) i (g) i točki 2.

([445]) Memorandum o razumijevanju između Ureda povjerenika za informiranje i obavještajne zajednice Ujedinjene Kraljevine, vidjeti bilješku 165.

([446]) U sedam od tih slučajeva ICO je savjetovao podnositelju pritužbe da se u vezi sa svojim prigovorom obrati voditelju obrade podataka (to je slučaj kad je pojedinac iznio prigovor ICO-u, a trebao se prvo obratiti voditelju obrade podataka), u jednom od tih slučajeva ICO je dao općenite savjete voditelju obrade podataka (to se primjenjuje kad se čini da voditelj obrade nije svojim postupcima prekršio zakonodavstvo, ali se poboljšanjem prakse moglo izbjeći podnošenje prigovora ICO-u), a u preostalih 13 slučajeva nije bilo potrebno da voditelj obrade podataka poduzme ikakve mjere (to se primjenjuje ako pojedinac iznese prigovore koji su obuhvaćeni Zakonom o zaštiti podataka iz 2018. jer se odnose na obradu osobnih podataka, ali na temelju dostavljenih informacija čini se da voditelj obrade nije prekršio zakonodavstvo).

3.3.3.2. Nadzor primjene istražnih ovlasti na temelju IPA-e iz 2016.

(250) U skladu s dijelom 8. IPA-e iz 2016. nadzor nad primjenom istražnih ovlasti vrši povjerenik za istražne ovlasti (IPC). IPC-u pomažu drugi pravosudni povjerenici koji se zajednički nazivaju pravosudni povjerenici ([447]). IPA-om iz 2016. utvrđena su jamstva koja štite neovisnost pravosudnih povjerenika. Pravosudni povjerenici moraju imati ili su prethodno morali imati visoki položaj u pravosuđu (tj. moraju biti ili su prethodno morali biti članovi najviših sudova) ([448]) i, kao sve pravosudno osoblje, neovisni su od Vlade ([449]). U skladu s člankom 227. IPA-e iz 2016. predsjednik Vlade je taj koji imenuje IPC-a i onoliko pravosudnih povjerenika koliko smatra potrebnim. Svi povjerenici, bilo da su oni sadašnje ili bivše pravosudno osoblje, mogu biti imenovani samo na temelju zajedničke preporuke triju predsjednika sudova za Englesku i Wales, Škotsku i Sjevernu Irsku i lorda kancelara ([450]) Ministar je dužan osigurati osoblje, prostore, opremu i druga sredstva i usluge IPC-u ([451]). Mandat povjerenika traje tri godine, a povjerenik može biti ponovno imenovan ([452]). Kako bi se dodatno zajamčila njihova neovisnost, pravosudni povjerenici mogu biti razriješeni dužnosti isključivo uz primjenu strogih uvjeta kojima se utvrđuje visok prag, odnosno može ih razriješiti predsjednik Vlade u posebnim okolnostima taksativno navedenima u članku 228. stavku 5. IPA-e iz 2016. (poput stečaja ili kazne zatvora) ili ako su oba doma Parlamenta donijela odluku o razrješenju dužnosti ([453]).

(251) Ured povjerenika za istražne ovlasti (IPCO) podupire IPC-a i pravosudne povjerenike u izvršavanju njihovih funkcija. Osoblje IPCO-a obuhvaća skupinu inspektora, interne pravne i tehničke stručnjake te savjetodavnu skupinu za tehnologiju koji daju stručne savjete. Na isti način kao i za pojedinačne pravosudne povjerenike, neovisnost IPCO-a je zaštićena. IPCO je „neovisno tijelo" Ministarstva unutarnjih poslova, tj. dobiva financijska sredstva od Ministarstva unutarnjih poslova, ali izvršava svoje funkcije neovisno ([454]).

(252) Glavne funkcije pravosudnih povjerenika navedene su u članku 229. IPA-e iz 2016. ([455]) Konkretno, pravosudni povjerenici imaju opsežnu ovlast prethodnog odobrenja, koja je dio zaštitnih mjera uvedenih u pravni okvir Ujedinjene Kraljevine IPA-om iz 2016. Naloge povezane s ciljanim presretanjem, ometanjem opreme, masovnim skupovima osobnih podataka, masovnim pribavljanjem podataka o komunikacijama i zahtjevima za zadržavanje podataka o komunikacijama moraju odobriti pravosudni povjerenici ([456]). IPC uvijek mora izdati prethodno odobrenje za pribavljanje podataka o komunikacijama za potrebe kaznenog progona ([457]). Ako povjerenik odbije odobriti nalog, ministar može podnijeti žalbu povjereniku za istražne ovlasti, čija je odluka konačna.

([447]) U skladu s člankom 227. stavcima 7. i 8. IPA-e iz 2016. povjerenik za istražne ovlasti je pravosudni povjerenik te se povjerenik za istražne ovlasti i ostali pravosudni povjerenici zajednički nazivaju pravosudnim povjerenicima. Trenutačno postoji 15 pravosudnih povjerenika.

([448]) U skladu s člankom 60. stavkom 2. dijela 3. Zakona o ustavnoj reformi iz 2005. „visoki položaj u pravosuđu" znači dužnost suca bilo kojeg od sljedećih sudova: i. Vrhovni sud; ii. Žalbeni sud u Engleskoj i Walesu; iii. Visoki sud u Engleskoj i Walesu; iv. Vrhovni građanski sud (*Court of Session*); v. Žalbeni sud u Sjevernoj Irskoj; vi. Visoki sud u Sjevernoj Irskoj; ili dužnost pravnog lorda.

([449]) Neovisnost pravosuđa temelji se na običaju te je općenito priznata od Zakona o nasljeđivanju prijestolja iz 1701.

([450]) Članak 227. stavak 3. IPA-e iz 2016. Pravosudne povjerenike mora preporučiti i povjerenik za istražne ovlasti, članak 227. stavak 4. točka (e) IPA-e iz 2016.

([451]) Članak 238. IPA-e iz 2016.

([452]) Članak 227. stavak 2. IPA-e iz 2016.

([453]) Postupak razrješenja dužnosti jednak je onome za druge suce u Ujedinjenoj Kraljevini (vidjeti, na primjer, članak 11. stavak 3. Zakona o visokim sudovima iz 1981. i članak 33. Zakona o ustavnoj reformi iz 2005. kojima se isto utvrđuje da je odluka o razrješenju podložna odobrenju obaju domova Parlamenta). Do danas nijedan pravosudni povjerenik nije razriješen dužnosti.

([454]) Neovisno tijelo je organizacija ili agencija koju financira Vlada, ali može djelovati neovisno (za definiciju i više informacija o neovisnom tijelu vidjeti Priručnik Vladina ureda o klasifikaciji javnih tijela, dostupan na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf, i prvo izvješće sa sjednice 2014.–2015. Posebnog odbora za javnu upravu Zastupničkog doma, dostupno na: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf).

([455]) U skladu s člankom 229. IPA-e iz 2016. pravosudni povjerenik ima opsežne nadzorne ovlasti koje obuhvaćaju i nadzor nad zadržavanjem i otkrivanjem podataka koje su prikupile obavještajne agencije.

([456]) Odluke o odobrenju odluke ministra za izdavanje naloga donose sami pravosudni povjerenici. Ako povjerenik odbije odobriti nalog, ministar može podnijeti žalbu povjereniku za istražne ovlasti, čija je odluka konačna.

([457]) Odobrenje IPC-a uvijek se zahtijeva kad se podaci o komunikacijama prikupljaju za potrebe kaznenog progona (članak 60.A IPA-e iz 2016.). Ako su podaci o komunikacijama pribavljeni za potrebe nacionalne sigurnosti, odobrenje može izdati IPC ili viši imenovani službenik relevantnog tijela javne vlasti (vidjeti članke 61. i 61.A IPA-e iz 2016. i uvodnu izjavu 203.).

(253) Posebni izvjestitelj UN-a za pravo na privatnost vrlo je pozitivno ocijenio institut pravosudnih povjerenika uspostavljen IPA-om iz 2016. s obzirom na to da „sve osjetljivije zahtjeve za provođenje nadzora ili one kojima se zadire u privatnost treba odobriti ministar u Vladi i Ured povjerenika za istražne ovlasti". Posebno je istaknuo da je „taj element sudskog preispitivanja [preko funkcije IPC-a], koji podupire tim iskusnih inspektora i stručnjaka za tehnologiju, jedna od najznačajnijih novih zaštitnih mjera uvedenih IPA-om", koji je zamijenio prethodno rascjepkani sustav nadzornih tijela i kojim se nadopunjava uloga Odbora Parlamenta za obavještajne poslove i sigurnost te Suda za istražne ovlasti ([458]).

(254) Osim toga, IPC ima ovlasti provoditi *ex post* nadzor, među ostalim u okviru revizije, inspekcije i istrage, nad primjenom istražnih ovlasti na temelju IPA-e iz 2016. ([459]) i neke druge ovlasti i funkcije predviđene relevantnim zakonodavstvom ([460]). Rezultati takvog *ex post* nadzora navedeni su u izvješću koje IPC mora sastaviti svake godine i iznijeti predsjedniku Vlade ([461]) te koje se mora objaviti i predstaviti Parlamentu ([462]). Izvješće sadržava relevantne statističke podatke i informacije o primjeni istražnih ovlasti obavještajnih agencija i tijela kaznenog progona te o uvođenju zaštitnih mjera u odnosu na informacije koje podliježu obvezi čuvanja povjerljivosti, povjerljivi novinarski materijal i izvore novinarskih informacija, kao i informacije o poduzetim mjerama i korištenim operativnim svrhama u kontekstu masovnih naloga. Naposljetku, u godišnjem izvješću IPCO-a navodi se područje u kojem su dane preporuke tijelima javne vlasti te što su ona poduzela po pitanju tih preporuka ([463]).

(255) U skladu s člankom 231. IPA-e iz 2016., ako IPC sazna da su tijela javne vlasti pri primjeni istražnih ovlasti počinila relevantnu pogrešku, o tome mora obavijestiti predmetnu osobu ako smatra da je pogreška ozbiljna i da je u javnom interesu da osoba bude obaviještena ([464]). Konkretno, u članku 231. IPA-e iz 2016. navodi se da pri obavještavanju osobe o pogrešci IPC mora navesti informacije o svim njezinim pravima da se obrati Sudu za istražne ovlasti te navesti pojedinosti koje povjerenik smatra potrebnima za ostvarivanje tih prava te ako postoji javni interes za otkrivanje tih pojedinosti ([465]).

([458]) Izjava povodom završetka posjeta posebnog izvjestitelja za pravo na privatnost Ujedinjenoj Kraljevini Velike Britanije i Sjeverne Irske (vidjeti bilješku 281.).

([459]) Članak 229. IPA-e iz 2016. Istražne ovlasti i ovlasti u pogledu informacija pravosudnog povjerenika navedene su u članku 235. IPA-e iz 2016.

([460]) To uključuje mjere nadzora na temelju RIPA-e iz 2000., izvršavanje funkcija na temelju dijela 3. Zakona o policiji iz 1997. (izdavanje odobrenja za postupanja povezana s imovinom) i izvršavanje funkcija ministra na temelju članaka od 5. do 7. Zakona o obavještajnim službama iz 1994. (nalozi za ometanje bežične telegrafije, ulazak i zadiranje u vlasnička prava (članak 229. IPA-e iz 2016.)).

([461]) Članak 230. IPA-e iz 2016. IPC ujedno može na vlastitu inicijativu izvijestiti predsjednika Vlade o svim pitanjima povezanima sa svojom funkcijom. IPC mora izvještavati predsjednika Vlade i na njegov zahtjev, a predsjednik Vlade može naložiti IPC-u preispitivanje bilo kojih funkcija obavještajnih službi.

([462]) Neki dijelovi mogu biti isključeni ako bi njihovo objavljivanje bilo u suprotnosti s nacionalnom sigurnošću.

([463]) Na primjer, u godišnjem izvješću IPCO-a za 2019. (točka 6.38.) navodi se da se je službi MI5 preporučeno da izmijeni politiku zadržavanja masovnih skupova osobnih podataka (BPD) s obzirom na to da je služba trebala zauzeti pristup razmatranja proporcionalnosti zadržavanja za sva polja masovnih skupova osobnih skupova podataka i za svaki pojedini masovni skup osobnih podataka koje posjeduje. Krajem 2018. IPCO nije bio uvjeren da se ta preporuka primjenjuje te je u izvješću za 2019. objašnjeno je da MI5 sad uvodi novi postupak za ispunjavanje tog zahtjeva. U godišnjem izvješću za 2019. (točka 8.22.) navodi se i da je GHCQ dobio niz preporuka za vođenje evidencije o proporcionalnosti svojih zahtjeva u pogledu masovnih podataka. U izvješću je potvrđeno da su na tom području krajem 2018. postignuta poboljšanja. Godišnje izvješće Ureda povjerenika za istražne ovlasti za 2019., dostupno na: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Osim toga, svaka inspekcija tijela javne vlasti koju provodi IPCO zaključuje se izvješćem koje se dostavlja tijelu i uključuje sve preporuke koje proizlaze iz te inspekcije. IPCO zatim započinje svaku sljedeću inspekciju pregledom svih prethodnih preporuka od posljednjeg puta i u novom izvješću o inspekciji uzima se u obzir jesu li poduzete određene mjere na temelju prethodnih preporuka ili bi li ih trebalo ponoviti.

([464]) Pogreška se smatra „ozbiljnom" ako povjerenik smatra da su predmetnoj osobi znatno ugrožena prava ili da joj je nanesena znatna šteta (članak 231. stavak 2. IPA-e iz 2016.). U 2018. prijavljene su 22 pogreške, od kojih se osam smatralo ozbiljnima i o njima su obaviještene predmetne osobe. Vidjeti Godišnje izvješće Ureda povjerenika za istražne ovlasti za 2018., Prilog C (vidjeti https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). U 2019. ozbiljnima se smatralo 14 pogrešaka. Vidjeti Godišnje izvješće Ureda povjerenika za istražne ovlasti za 2019., Prilog C, vidjeti bilješku 463.

([465]) U članku 231. IPA-e iz 2016. navodi se da pri obavještavanju osobe o pogrešci IPC mora navesti pojedinosti koje smatra potrebnima za ostvarivanje njezinih prava, posebno uzimajući u obzir u kojoj bi mjeri otkrivanje pojedinosti bilo u suprotnosti s javnim interesom ili štetno za sprečavanje ili otkrivanje teških kaznenih djela, gospodarsku dobrobit Ujedinjene Kraljevine ili daljnje obavljanje funkcija bilo koje od obavještajnih službi.

3.3.3.3. Parlamentarni nadzor obavještajnih službi

(256) Zakonska osnova za parlamentarni nadzor Odbora za obavještajne poslove i sigurnost (ISC) je Zakon o pravosuđu i sigurnosti iz 2013. (JSA iz 2013.) ([466]). Tim se zakonom osniva ISC kao odbor Parlamenta Ujedinjene Kraljevine. Od 2013. ISC je dobio veće ovlasti, uključujući nadzor operativnih aktivnosti sigurnosnih službi. U skladu s člankom 2. JSA-e iz 2013. ISC ima zadaću nadzirati rashode, upravljanje, politiku i operacije nacionalnih sigurnosnih agencija. U JSA-i iz 2013. propisano je da ISC može provoditi istrage o operativnim pitanjima ako se ona ne odnose na operacije koje su u tijeku ([467]). U Memorandumu o razumijevanju koji su sklopili predsjednik Vlade i ISC ([468]) detaljno se navode elementi koje treba uzeti u obzir pri utvrđivanju je li određena aktivnost dio operacije koja je u tijeku ([469]). Predsjednik Vlade može od ISC-a zatražiti i da istraži operacije koje su u tijeku te ISC može pregledavati informacije koje mu agencije dobrovoljno dostave.

(257) U skladu s Prilogom 1. JSA-i iz 2013. ISC može od voditelja bilo koje od triju obavještajnih službi zatražiti da otkrije bilo koju informaciju. Agencija mora te informacije staviti na raspolaganje, osim ako ministar to ne zabrani ([470]). Prema objašnjenjima tijela Ujedinjene Kraljevine, u praksi se ISC-u uskraćuje vrlo malo informacija ([471]).

(258) ISC se sastoji od članova koji pripadaju obama domovima Parlamenta, a imenuje ih predsjednik Vlade nakon savjetovanja s čelnikom oporbe ([472]). ISC je obvezan podnositi godišnje izvješće Parlamentu o obavljanju svojih funkcija i druga izvješća koja smatra primjerenima ([473]). Nadalje, ISC ima pravo svaka tri mjeseca primati popis operativnih svrha koji se koristi za pregled masovno prikupljenog materijala ([474]). Primjerke dokumenata o istragama, inspekcijama ili revizijama povjerenika za istražne ovlasti ISC-u dostavlja predsjednik Vlade ako je tema izvješća relevantna za zakonske nadležnosti Odbora ([475]). Naposljetku, Odbor može zatražiti od IPC-a da provede istragu, a povjerenik mora obavijestiti ISC o odluci o tome hoće li provesti takvu istragu ([476]).

(259) ISC je dostavio mišljenje i o nacrtu IPA-e iz 2016., što je dovelo do niza izmjena koje su sad odražene u IPA-i iz 2016. ([477]) Konkretno, ISC je preporučio jačanje zaštite privatnosti uvođenjem niza mjera za zaštitu privatnosti koje

([466]) Kako su objasnila tijela Ujedinjene Kraljevine, JSA-om je proširena nadležnost ISC-a kako bi se uključila funkcija nadzora obavještajne zajednice povrh triju glavnih agencija te omogućio naknadni nadzor operativnih aktivnosti agencija u pitanjima od velikog nacionalnog interesa.

([467]) Članak 2. JSA-a iz 2013.

([468]) Memorandum o razumijevanju između predsjednika Vlade i ISC-a, dostupan na: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.

([469]) Memorandum o razumijevanju između predsjednika Vlade i ISC-a, točka 14., vidjeti bilješku 468.

([470]) Ministar može zabraniti otkrivanje informacija samo na temelju dvaju razloga: informacije su osjetljive i ne smiju se otkriti ISC-u u interesu nacionalne sigurnosti; ili su informacije takve prirode da bi ministar, ako bi se od njega zatražilo da dostavi te informacije posebnom resornom odboru Zastupničkog doma, smatrao (zbog razloga koji nisu ograničeni na nacionalnu sigurnost) da nije primjereno da to učini. (točka 4. podtočka 2. Priloga 1. JSA-i iz 2013.).

([471]) Okvir za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, odjeljak H: Nacionalna sigurnost, str. 43., vidjeti bilješku 31.

([472]) Članak 1. JSA-a iz 2013. Ministri ne mogu biti imenovani za članove ISC-a. Članovi zadržavaju svoje mjesto u ISC-u dok traje mandat Parlamenta za vrijeme kojeg su imenovani. Može ih se razriješiti dužnosti odlukom doma koji ih je imenovao ili ako prestanu biti zastupnici u Parlamentu ili postanu ministri. Član može i podnijeti ostavku.

([473]) Izvješća i izjave Odbora dostupni su na: https://isc.independent.gov.uk/publications/. ISC je 2015. objavio izvješće pod nazivom *Privacy and Security: A modern and transparent legal framework* (Privatnost i sigurnost: moderan i transparentan pravni okvir) (vidjeti: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), u kojem je razmatrao pravni okvir za tehnike nadzora koje koriste obavještajne agencije i izdao niz preporuka koje su potom uzete u obzir i uključene u nacrt Prijedloga zakona o istražnim ovlastima koji je kasnije postao zakon – IPA iz 2016. Odgovor Vlade na to izvješće o privatnosti i sigurnosti dostupan je na: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

([474]) Članci 142., 161. i 183. IPA-e iz 2016.

([475]) Članak 234. IPA-e iz 2016.

([476]) Članak 236. IPA-e iz 2016.

([477]) Odbor Parlamenta za obavještajne poslove i sigurnost, Izvješće o nacrtu Prijedloga zakona o istražnim ovlastima, dostupno na: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

se primjenjuju za cijeli niz istražnih ovlasti ([478]). Predložio je i izmjene predloženih tehničkih sposobnosti za ometanje opreme, BPD-a i podataka o komunikacijama te je zatražio druge posebne izmjene radi jačanja ograničenja i zaštitnih mjera za primjenu istražnih ovlasti ([479]).

3.3.4. *Sudska zaštita*

(260) U području pristupa vlade za potrebe nacionalne sigurnosti ispitanici moraju imati mogućnost pokretanja sudskog postupka pred neovisnim i nepristranim sudom radi pristupa svojim osobnim podacima ili ispravka ili brisanja tih podataka ([480]). Takvo sudsko tijelo mora prvenstveno imati ovlast za donošenje obvezujućih odluka o obavještajnim službama ([481]). U Ujedinjenoj Kraljevini, kako je objašnjeno u uvodnim izjavama od 261. do 271., različiti oblici sudske zaštite pružaju ispitanicima mogućnost da zatraže i koriste takve pravne lijekove.

3.3.4.1. Mehanizmi sudske zaštite dostupni na temelju dijela 4. DPA-a

(261) U skladu s člankom 165. DPA-a iz 2018. ispitanik može podnijeti pritužbu povjereniku za informiranje ako smatra da u vezi s osobnim podacima koji se odnose na njega postoji kršenje dijela 4. DPA-a iz 2018. Povjerenik za informiranje ovlašten je ocijeniti usklađenost voditelja obrade i izvršitelja obrade s DPA-om iz 2018. te zahtijevati od njih da poduzmu potrebne mjere. Nadalje, na temelju dijela 4. DPA-a iz 2018. pojedinci imaju pravo obratiti se Visokom sudu (ili Vrhovnom građanskom sudu u Škotskoj (*Court of Session*)) da izda nalog kojim se od voditelja obrade zahtijeva da poštuje prava na pristup podacima ([482]), podnošenje prigovora na obradu ([483]) te ispravak ili brisanje podataka ([484]).

(262) Pojedinci imaju pravo i na naknadu pretrpljene štete zbog kršenja zahtjeva iz dijela 4. DPA-a iz 2018. koju isplaćuje voditelj obrade ili izvršitelj obrade ([485]). Šteta obuhvaća i financijski gubitak i štetu koja ne uključuje financijski gubitak, kao što je pretrpljena duševna bol ([486]).

3.3.4.2. Mehanizmi sudske zaštite dostupni na temelju IPA-e iz 2016.

(263) Pojedinci mogu dobiti sudsku zaštitu u slučaju kršenja IPA-e iz 2016. pred Sudom za istražne ovlasti (*Investigatory Powers Tribunal*).

(264) Sud za istražne ovlasti uspostavljen je RIPA-om iz 2000. i neovisan je od izvršne vlasti ([487]). U skladu s člankom 65. RIPA-e iz 2000. članove tog suda imenuje Njezino Veličanstvo na razdoblje od pet godina. Njezino Veličanstvo može razriješiti dužnosti člana tog suda na molbu ([488]) obaju domova Parlamenta ([489]).

([478]) Te opće obveze u pogledu privatnosti sad su navedene u članku 2. stavku 2. IPA-e iz 2016., kojim se predviđa da tijelo javne vlasti koje djeluje na temelju IPA-e iz 2016. mora voditi računa o tome je li se ono što se nastoji postići nalogom, odobrenjem ili zahtjevom razumno moglo postići drugim, manje nametljivim sredstvima, je li razina zaštite koja se primjenjuje za svako prikupljanje informacija na temelju naloga, odobrenja ili zahtjeva veća zbog osobite osjetljivosti tih informacija, javnog interesa povezanog s integritetom i sigurnošću telekomunikacijskih sustava i poštanskih usluga te svih drugih aspekata javnog interesa koji se odnose na zaštitu privatnosti.

([479]) Na primjer, na zahtjev ISC-a broj dana koliko „hitni" nalog može biti na snazi prije nego što ga pravosudni povjerenik mora odobriti smanjen je s pet radnih dana na tri radna dana, a ISC je ovlašten uputiti predmete na istragu povjereniku za istražne ovlasti.

([480]) Predmet *Schrems II*, točka 194.

([481]) Predmet *Schrems II*, točka 197.

([482]) Članak 94. stavak 11. DPA-a iz 2018.

([483]) Članak 99. stavak 4. DPA-a iz 2018.

([484]) Članak 100. stavak 1. DPA-a iz 2018.

([485]) Člankom 169. DPA-a iz 2018. dopušta se da „osoba koja trpi štetu zbog kršenja zahtjeva iz zakonodavstva o zaštiti podataka" podnese zahtjev za naknadu štete. Prema informacijama koje su dostavila tijela Ujedinjene Kraljevine, zahtjev za naknadu štete ili pritužba protiv obavještajnih službi u praksi se najčešće podnosi Sudu za istražne ovlasti, koji ima široku nadležnost, može dodijeliti naknadu/odštetu i podnošenje takvog zahtjeva ne uključuje nikakve troškove.

([486]) Članak 169. stavak 5. DPA-a iz 2018.

([487]) Prema Prilogu 3. RIPA-i iz 2000. članovi Suda moraju imati utvrđeno pravosudno iskustvo i mogu biti ponovno imenovani.

([488]) „Molba" (*address*) je prijedlog upućen Parlamentu čija je svrha obavijestiti vladara o mišljenju Parlamenta o određenom pitanju.

([489]) Točka 1. podtočka 5. Priloga 3. RIPA-i iz 2000.

(265) U skladu s člankom 65. RIPA-e iz 2000. Sud je pravosudno tijelo nadležno za sve pritužbe osobe oštećene postupkom provedenim na temelju IPA-e iz 2016., RIPA-e iz 2000. ili bilo kojim postupkom obavještajnih službi ([490]).

(266) Za pokretanje postupka pred Sudom za istražne ovlasti („zahtjev u pogledu procesne legitimacije"), u skladu s člankom 65. RIPA-e iz 2000. pojedinac mora biti uvjeren ([491]) da se postupak obavještajne službe odnosio na njega, bilo koju njegovu imovinu, bilo koju komunikaciju koju je poslao ili koja mu je poslana ili koja mu je bila namijenjena ili na njegovo korištenje bilo koje poštanske usluge, telekomunikacijske usluge ili telekomunikacijskog sustava ([492]). Osim toga, podnositelj pritužbe mora biti uvjeren da je postupak proveden u „okolnostima koje se mogu osporavati" ([493]) ili „da su ga provele obavještajne službe ili je izvršen u njihovo ime" ([494]). Budući da se posebno taj standard „uvjerenja" prilično široko tumači ([495]), pokretanje postupka pred tim sudom podliježe niskim zahtjevima u pogledu procesne legitimacije.

(267) Ako Sud za istražne ovlasti razmatra pritužbu koja mu je podnesena, dužnost mu je istražiti jesu li osobe protiv kojih se iznosi bilo kakva tvrdnja u pritužbi bile u nekoj vrsti odnosa s podnositeljem pritužbe, kao i provesti istragu o tijelu koje je navodno počinilo kršenje te o tome je li navodni postupak počinjen ([496]). Sud u svakom postupku koji vodi mora primijeniti ista načela za donošenje odluka u tim postupcima koje bi primjenjivao opći sud u slučaju zahtjeva za sudsko preispitivanje ([497]). Osim toga, adresati naloga ili zahtjeva na temelju IPA-e iz 2016. i svi drugi subjekti koji imaju poslovni nastan u Ujedinjenoj Kraljevini, koji su zaposleni u policiji ili povjerenik za policijske istrage i preispitivanje imaju dužnost otkriti ili dostaviti Sudu sve dokumente i informacije koje Sud može zahtijevati kako bi mogao izvršavati svoju nadležnost ([498]).

(268) Sud za istražne ovlasti mora obavijestiti podnositelja pritužbe o tome je li donesena odluka u njegovu korist ili nije ([499]). Na temelju članka 67. stavaka 6. i 7. RIPA-e iz 2000. Sud ima ovlast izdavati privremene odluke i dodjeljivati naknadu štete ili druge naloge koji smatra primjerenima. To može uključivati odluku kojom se ukida ili poništava bilo koji nalog ili odobrenje i odluku kojom se zahtijeva uništenje bilo koje evidencije informacija

([490]) Članak 65. stavak 5. RIPA-e iz 2000.

([491]) O standardu provjere „uvjerenja" vidjeti predmet *Human Rights Watch protiv Secretary of State* [2016] UKIPTrib15_165-CH, točku 41. U tom je predmetu Sud za istražne ovlasti, pozivajući se na sudsku praksu Europskog suda za ljudska prava, odgovarajućom provjerom navedenog uvjerenja smatrao utvrđivanje postoji li bilo kakva osnova za uvjerenje da je određeni postupak obuhvaćen člankom 68. stavkom 5. RIPA-e iz 2000. provela neka obavještajna služba ili da je proveden u njezino ime, primjerice da pojedinac može tvrditi da je žrtva kršenja do kojeg dolazi zbog samog postojanja tajnih mjera ili zakonodavstva kojim se omogućuju tajne mjere samo ako može dokazati da je zbog svoje osobne situacije mogao biti izložen opasnosti od toga da bude podvrgnut takvim mjerama.

([492]) Članak 65. stavak 4. točka (a) RIPA-e iz 2000.

([493]) Takve okolnosti odnose se na postupke tijela javne vlasti s ovlaštenjem (npr. nalog, odobrenje/zahtjev za pribavljanje komunikacija itd.) ili ako su okolnosti takve (bez obzira na to postoji li takvo ovlaštenje) da ne bi bilo primjereno da se postupak provodi bez ovlaštenja ili da se prethodno barem ne razmotri bi li trebalo zatražiti takvo ovlaštenje. Smatra se da su se postupci koje je odobrio pravosudni povjerenik dogodili u okolnostima koje se mogu osporavati (članak 65. stavak 7.ZA RIPA-e iz 2000.), dok se za druge postupke koji se provode uz dozvolu osobe koja obavlja sudačku dužnost smatra da se nisu dogodili u okolnostima koje se mogu osporavati (članak 65. stavci 7. i 8. RIPA-e iz 2000.).

([494]) Prema informacijama koje su dostavila tijela Ujedinjene Kraljevine, nizak prag za podnošenje pritužbe dovodi do toga da nije neuobičajeno da se u istrazi Suda utvrdi da podnositelj pritužbe doista nije nikad bio predmet istrage tijela javne vlasti. U posljednjem statističkom izvješću Suda za istražne ovlasti navodi se da je Sud 2016. zaprimio 209 pritužbi, od čega se 52 % njih smatralo neutemeljenima ili zlonamjernima, a 25 % njih zaključeno je „bez odluke". Tijela Ujedinjene Kraljevine objasnila su da to znači da se u odnosu na podnositelja pritužbe ne upotrebljavaju tajne aktivnosti/ovlasti ili da su korištene tajne tehnike, ali je Sud utvrdio da je aktivnost zakonita. Osim toga, 11 % pritužbi odbačeno je zbog nenadležnosti Suda ili su povučene ili proglašene nevažećima, 5 % ih je odbačeno zbog isteka roka, a u 7 % pritužbi odlučeno je u korist podnositelja pritužbe. Statističko izvješće Suda za istražne ovlasti za 2016. dostupno je na: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([495]) Vidjeti predmet *Human Rights Watch protiv Secretary of State* [2016] UKIPTrib15_165-CH. U tom je predmetu Sud za istražne ovlasti, pozivajući se na sudsku praksu Europskog suda za ljudska prava, odgovarajućom provjerom uvjerenja smatrao utvrđivanje postoji li bilo kakva osnova za uvjerenje da je određeni postupak obuhvaćen člankom 68. stavkom 5. RIPA-e iz 2000. provela neka obavještajna služba ili da je proveden u njezino ime, uključujući činjenicu da pojedinac može tvrditi da je žrtva kršenja do kojeg dolazi zbog samog postojanja tajnih mjera ili zakonodavstva kojim se omogućuju tajne mjere samo ako može dokazati da je zbog svoje osobne situacije mogao biti izložen opasnosti od toga da bude podvrgnut takvim mjerama (vidjeti predmet *Human Rights Watch protiv Secretary of State*, točku 41.).

([496]) Članak 67. stavak 3. RIPA-e iz 2000.

([497]) Članak 67. stavak 2. RIPA-e iz 2000.

([498]) Članak 68. stavci 6. i 7. RIPA-e iz 2000.

([499]) Članak 68. stavak 4. RIPA-e iz 2000.

dobivenih pri izvršavanju bilo koje ovlasti koja je dodijeljena na temelju naloga, odobrenja ili zahtjeva ili koju na neki drugi način bilo koje tijelo javne vlasti ima u vezi s bilo kojom osobom ([500]). Na temelju članka 67.A RIPA-e iz 2000. na odluku Suda može se podnijeti žalba podložno dopuštenju koje dodjeljuje Sud ili mjerodavni žalbeni sud.

(269) Naposljetku, vrijedi istaknuti da se o ulozi Suda za istražne ovlasti u nekoliko navrata raspravljalo u okviru sudskih postupaka pred Europskim sudom za ljudska prava, posebno u predmetu *Kennedy protiv the United Kingdom* ([501]), a u novije vrijeme u predmetu *Big Brother Watch i drugi protiv United Kingdom* ([502]), u kojem je Sud utvrdio da „Sud za istražne ovlasti pruža sveobuhvatni pravni lijek svima koji sumnjaju da su njihove komunikacije presele obavještajne službe" ([503]).

3.3.4.3. Ostali dostupni mehanizmi sudske zaštite

(270) Kako je objašnjeno u uvodnim izjavama od 109. do 111., sredstva sudske zaštite na temelju Zakona o ljudskim pravima iz 1998. i pred Europskim sudom za ljudska prava ([504]) dostupna su i u području nacionalne sigurnosti. Člankom 65. stavkom 2. RIPA-e iz 2000. Sudu za istražne ovlasti dodjeljuje se isključiva nadležnost za sve zahtjeve na temelju Zakona o ljudskim pravima povezane s obavještajnim agencijama ([505]). To znači, kako je istaknuo Visoki sud, da „utvrđivanje postojanja kršenja Zakona o ljudskim pravima na temelju činjenica pojedinog slučaja u načelu je nešto što razmatra i o čemu odlučuje neovisni sud koji ima pravo na pristup svim relevantnim materijalima, uključujući tajni materijal. […] U tom kontekstu treba voditi računa i o tome da sad i odluke samog Suda podliježu mogućnosti žalbe mjerodavnom žalbenom sudu (u Engleskoj i Walesu to bi bio Žalbeni sud); i da je Vrhovni sud nedavno odlučio da je Sud u načelu podložan sudskom preispitivanju: vidjeti predmet *R (Privacy International) protiv Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219" ([506]).

(271) Iz prethodno navedenog proizlazi da, kad tijela kaznenog progona ili tijela nacionalne sigurnosti Ujedinjene Kraljevine pristupaju osobnim podacima koji su obuhvaćeni područjem primjene ove Odluke, taj je pristup uređen zakonima kojima se utvrđuju uvjeti pod kojima je pristup moguć i kojima se osigurava da su pristup i daljnja uporaba podataka ograničeni na ono što je nužno i proporcionalno cilju kaznenog progona ili nacionalne sigurnosti koji se želi postići. Nadalje, takav pristup u većini slučajeva podliježe prethodnom odobrenju pravosudnog tijela, tako da je potrebno ishoditi odobrenje naloga za pribavljanje ili dostavljanje informacija, te u svakom slučaju neovisnom nadzoru. Nakon što tijela javne vlasti dobiju pristup podacima, njihova obrada, uključujući daljnju razmjenu i daljnji prijenos, podliježe posebnim mjerama za zaštitu podataka na temelju dijela 3. DPA-a iz 2018., koje odražavaju one utvrđene u Direktivi (EU) 2016/680 za obradu koju provode tijela kaznenog progona, i dijela 4. DPA-a iz 2018. za obradu koju provode obavještajne agencije. Naposljetku, ispitanici u tom području uživaju prava na učinkovitu upravnu i sudsku zaštitu, uključujući pravo na pristup svojim podacima ili ispravak ili brisanje tih podataka.

(272) S obzirom na važnost takvih uvjeta, ograničenja i zaštitnih mjera za potrebe ove Odluke, Komisija će pomno nadzirati primjenu i tumačenje pravila Ujedinjene Kraljevine kojima se postavlja okvir za pristup državnih tijela podacima. To će uključivati relevantne promjene zakonodavstva, propisa i sudske prakse, kao i aktivnosti ICO-a i

([500]) Primjer primjene tih ovlasti iznesen je u predmetu *Liberty i drugi protiv the Security Service, SIS, GCHQ*, [2015] UKIP Trib 13_77-H_2. Sud je odlučio u korist dvaju podnositelja pritužbe jer je njihova komunikacija u jednom slučaju bila zadržana izvan utvrđenih rokova, a u drugom jer postupak ispitivanja nije proveden kako je utvrđeno u internim pravilima GCHQ-a. Sud je u prvom predmetu naložio obavještajnim službama da unište komunikacije koje su zadržane dulje od propisanog roka. U drugom slučaju nalog za uništenje nije izdan jer komunikacija nije zadržana.

([501]) Predmet *Kennedy*, vidjeti bilješku 129.

([502]) Europski sud za ljudska prava, predmet *Big Brother Watch i drugi protiv United Kingdom*, (vidjeti prethodnu bilješku 268.), točke od 413. do 415.

([503]) Europski sud za ljudska prava, predmet *Big Brother Watch*, točka 425.

([504]) Kao što, na primjer, pokazuje nedavna presuda Velikog vijeća Europskog suda za ljudska prava u predmetu *Big Brother Watch i drugi protiv United Kingdom* (vidjeti prethodnu bilješku 279.), to omogućuje učinkovitu sudsku kontrolu međunarodnog suda nad time poštuju li tijela javne vlasti temeljna prava pri pristupu osobnim podacima sličnu onoj koja se primjenjuje na države članice EU-a. Osim toga, izvršenje presuda Europskog suda za ljudska prava podliježe posebnom nadzoru Vijeća Europe.

([505]) U predmetu *Belhaj i drugi* [2017] UKSC 3 utvrđivanje nezakonitosti presretanja materijala koji podliježu obvezi čuvanja povjerljivosti temeljilo se izravno na članku 8. EKLJP-a (vidjeti odluku br. 11).

([506]) Visoki sud, predmet *Liberty* [2019] EWHC 2057 (Admin), točka 170.

drugih nadzornih tijela u tom području. Pozorno će se pratiti i izvršava li Ujedinjena Kraljevina relevantne presude Europskog suda za ljudska prava, uključujući mjere utvrđene u „akcijskim planovima" i „izvješćima o poduzetim mjerama" koje se dostavljaju Odboru ministara u kontekstu nadzora nad poštovanjem presuda Suda.

4. ZAKLJUČAK

(273) Komisija smatra da Opća uredba o zaštiti podataka Ujedinjene Kraljevine i DPA iz 2018. osiguravaju razinu zaštite osobnih podataka koji se prenose iz Europske unije koja je u načelu istovjetna onoj koja se jamči Uredbom (EU) 2016/679.

(274) Nadalje, Komisija smatra da nadzorni mehanizmi i mogućnosti za sudsku zaštitu predviđeni pravom Ujedinjene Kraljevine u cjelini omogućavaju da se u praksi utvrde i kazne povrede te ispitaniku pružaju pravne lijekove za dobivanje pristupa osobnim podacima koji se odnose na njega te, konačno, za ispravak ili brisanje takvih podataka.

(275) Konačno, na temelju dostupnih informacija o pravnom poretku Ujedinjene Kraljevine Komisija smatra da će se svako zadiranje u temeljna prava pojedinaca čije osobne podatke iz Europske unije u Ujedinjenu Kraljevinu prenose tijela javne vlasti Ujedinjene Kraljevine za potrebe javnog interesa, posebno u svrhu kaznenog progona i nacionalne sigurnosti, ograničiti na ono što je nužno za ostvarivanje predmetnog legitimnog cilja te da postoji djelotvorna pravna zaštita od takvog zadiranja.

(276) Stoga bi, s obzirom na zaključke ove Odluke, trebalo odlučiti da Ujedinjena Kraljevina osigurava primjerenu razinu zaštite u smislu članka 45. Uredbe (EU) 2016/679, tumačeno s obzirom na Povelju Europske unije o temeljnim pravima.

(277) Taj se zaključak temelji na relevantnom nacionalnom sustavu Ujedinjene Kraljevine i njezinim međunarodnim obvezama, posebno poštovanju Europske konvencije o ljudskim pravima i prihvaćanju nadležnosti Europskog suda za ljudska prava. Kontinuirano poštovanje tih međunarodnih obveza stoga je osobito važan element procjene na kojoj se temelji ova Odluka.

5. UČINCI OVE ODLUKE I AKTIVNOSTI TIJELA ZA ZAŠTITU PODATAKA

(278) Države članice i njihova tijela dužni su poduzeti mjere potrebne za usklađivanje s aktima institucija Unije jer se potonji smatraju zakonitima i proizvode pravne učinke do njihova isteka, povlačenja, poništenja u postupku za poništenje ili proglašavanja nevažećima nakon zahtjeva za prethodnu odluku ili tužbenog zahtjeva za proglašenje nezakonitosti.

(279) Stoga je odluka Komisije o primjerenosti donesena u skladu s člankom 45. stavkom 3. Uredbe (EU) 2016/679 obvezujuća za sva tijela država članica kojima je upućena, uključujući njihova neovisna nadzorna tijela. Konkretnije, dok se primjenjuje ova Odluka, za prijenos podataka od voditelja obrade ili izvršitelja obrade u Europskoj uniji voditeljima obrade ili izvršiteljima obrade u Ujedinjenoj Kraljevini nisu potrebna daljnja odobrenja.

(280) Trebalo bi podsjetiti da, u skladu s člankom 58. stavkom 5. Uredbe (EU) 2016/679 i kako je objašnjeno u presudi Suda EU-a u predmetu *Schrems* ([507]), ako nacionalno tijelo za zaštitu podataka, među ostalim nakon što je zaprimilo pritužbu, ima sumnje u pogledu spojivosti odluke Komisije o primjerenosti s temeljnim pravima pojedinca na privatnost i zaštitu podataka, nacionalnim pravom mora biti predviđen pravni lijek za iznošenje tih prigovora pred nacionalnim sudom od kojeg se može tražiti da Sudu EU-a uputi zahtjev za prethodnu odluku ([508]).

([507]) Presuda u predmetu *Schrems*, točka 65.

([508]) Presuda u predmetu *Schrems*, točka 65.: „U tom je pogledu nacionalni zakonodavac dužan predvidjeti pravna sredstva koja neovisnom nadzornom tijelu omogućavaju isticanje prigovora pred nacionalnim sudovima koje smatra osnovanima, kako bi ti sudovi mogli, u slučaju da dijele sumnje tog tijela u vezi s valjanošću Komisijine odluke, uputiti zahtjev za prethodnu odluku radi ispitivanja valjanosti te odluke."

6. **PRAĆENJE, SUSPENZIJA, STAVLJANJE IZVAN SNAGE ILI IZMJENA OVE ODLUKE**

(281) U skladu s člankom 45. stavkom 4. Uredbe (EU) 2016/679 Komisija treba kontinuirano pratiti relevantne procese u Ujedinjenoj Kraljevini nakon donošenja ove Odluke kako bi procijenila je li njome i dalje osigurana u načelu istovjetna razina zaštite. Takvo je praćenje posebno važno u ovom slučaju jer će Ujedinjena Kraljevina primjenjivati i provoditi novi sustav zaštite podataka koji više ne podliježe pravu Europske unije i koji bi mogao biti podložan promjenama. U tom će se pogledu posebna pažnja posvetiti praktičnoj primjeni pravila Ujedinjene Kraljevine o prijenosu osobnih podataka u treće zemlje i učinku koji bi on mogao imati na razinu zaštite koja se osigurava za podatke koji se prenose na temelju ove Odluke, na djelotvornost izvršavanja pojedinačnih prava, uključujući sve relevantne promjene u zakonodavstvu i praksi koje se odnose na iznimke ili ograničenja takvih prava (posebno one koje se odnose na provedbu djelotvorne kontrole useljavanja), kao i poštovanje ograničenja i zaštitnih mjera u pogledu pristupa državnih tijela. Među ostalim elementima, razvoji u sudskoj praksi te nadzor ICO-a i drugih neovisnih tijela pridonijet će praćenju Komisije.

(282) Kako bi olakšala to praćenje, tijela Ujedinjene Kraljevine trebala bi odmah obavijestiti Komisiju o svim bitnim promjenama pravnog poretka Ujedinjene Kraljevine koje imaju učinak na pravni okvir koji je predmet ove Odluke, kao i o svim promjenama prakse povezane s obradom osobnih podataka koja se procjenjuje u ovoj Odluci u pogledu obrade osobnih podataka koju provode voditelji obrade i izvršitelji obrade na temelju Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, ali i ograničenja i zaštitnih mjera koje se primjenjuju na pristup tijela javne vlasti osobnim podacima. To bi trebalo uključivati promjene povezane s elementima spomenutima u uvodnoj izjavi 281.

(283) Nadalje, kako bi Komisija mogla djelotvorno obavljati svoju funkciju praćenja, države članice trebale bi je obavješćivati o svim relevantnim mjerama koje poduzimaju nacionalna tijela za zaštitu podataka, naročito u pogledu upita ili pritužbi ispitanika iz EU-a o prijenosu osobnih podataka iz Unije voditeljima obrade ili izvršiteljima obrade u Ujedinjenoj Kraljevini. Komisiju bi trebalo obavijestiti i o svakoj naznaci da mjere tijela javne vlasti Ujedinjene Kraljevine odgovornih za sprečavanje, istragu, otkrivanje ili progon kaznenih djela ili za nacionalnu sigurnost, uključujući nadzorna tijela, ne osiguravaju potrebnu razinu zaštite.

(284) Ako dostupne informacije, naročito informacije dobivene praćenjem primjene ove Odluke ili informacije koje dostavljaju tijela Ujedinjene Kraljevine ili država članica, pokazuju da razina zaštite koju pruža Ujedinjena Kraljevina možda više nije primjerena, Komisija bi o tome trebala odmah obavijestiti nadležna tijela Ujedinjene Kraljevine i zatražiti poduzimanje odgovarajućih mjera u navedenom roku, koji ne smije biti duži od tri mjeseca. To se razdoblje prema potrebi može produžiti za određeni rok, uzimajući u obzir prirodu problema i/ili mjere koje treba poduzeti. Primjerice, takav bi se postupak pokrenuo u slučajevima kad se daljnji prijenosi, među ostalim na temelju novih uredbi o primjerenosti koje donosi ministar ili međunarodnih sporazuma koje zaključuje Ujedinjena Kraljevina, više ne bi provodili pod zaštitnim mjerama koje osiguravaju kontinuitet zaštite u smislu članka 44. Uredbe (EU) 2016/679.

(285) Ako nakon isteka navedenog roka nadležna tijela Ujedinjene Kraljevine ne poduzmu te mjere ili na drugi zadovoljavajući način ne dokažu da se ova Odluka i dalje temelji na primjerenoj razini zaštite, Komisija će pokrenuti postupak iz članka 93. stavka 2. Uredbe (EU) 2016/679 radi djelomične ili potpune suspenzije ili stavljanja izvan snage ove Odluke.

(286) Alternativno, Komisija će pokrenuti taj postupak radi izmjene Odluke, ponajprije utvrđivanjem dodatnih uvjeta za prijenose podataka ili ograničavanjem područja primjene zaključka o primjerenosti samo na prijenose podataka za koje se i dalje osigurava primjerena razina zaštite.

(287) Zbog valjano utemeljenih krajnje hitnih razloga Komisija će iskoristiti mogućnost donošenja, u skladu s postupkom iz članka 93. stavka 3. Uredbe (EU) 2016/679, odmah primjenjivih provedbenih akata o suspenziji, stavljanju izvan snage ili izmjeni Odluke.

7. **TRAJANJE I PRODULJENJE OVE ODLUKE**

(288) Komisija mora uzeti u obzir da će, nakon isteka prijelaznog razdoblja predviđenog Sporazumom o povlačenju i čim privremena odredba na temelju članka 782. Sporazuma o trgovini i suradnji između EU-a i Ujedinjene Kraljevine prestane važiti, Ujedinjena Kraljevina primjenjivati i provoditi novi sustav zaštite podataka koji se razlikuje od onog koji je bio na snazi kad je za nju bilo obvezujuće pravo Unije. To može ponajprije uključivati izmjene ili promjene okvira za zaštitu podataka procijenjenog u ovoj Odluci, kao i druge relevantne promjene.

(289) Stoga je primjereno predvidjeti da se ova Odluka primjenjuje u razdoblju od četiri godine od njezina stupanja na snagu.

(290) Ako se na temelju određenih informacija koje proizlaze iz praćenja primjene ove Odluke utvrdi da su zaključci koji se odnose na primjerenost razine zaštite osigurane u Ujedinjenoj Kraljevini i dalje činjenično i pravno opravdani, Komisija bi trebala najkasnije šest mjeseci prije nego što se ova Odluka prestane primjenjivati pokrenuti postupak izmjene ove Odluke proširenjem vremenskog okvira primjene, u načelu, na dodatno razdoblje od četiri godine. Svaki takav provedbeni akt o izmjeni ove Odluke treba se donijeti u skladu s postupkom iz članka 93. stavka 2. Uredbe (EU) 2016/679.

8. **ZAVRŠNA RAZMATRANJA**

(291) Europski odbor za zaštitu podataka objavio je svoje mišljenje ([509]), koje je uzeto u obzir pri pripremi ove Odluke.

(292) Mjere predviđene ovom Odlukom u skladu su s mišljenjem Odbora osnovanog na temelju članka 93. Uredbe (EU) 2016/679,

DONIJELA JE OVU ODLUKU:

Članak 1.

1. Za potrebe članka 45. Uredbe (EU) 2016/679 Ujedinjena Kraljevina osigurava primjerenu razinu zaštite osobnih podataka koji se prenose iz Europske unije u Ujedinjenu Kraljevinu u okviru područja primjene Uredbe (EU) 2016/679.

2. Ovom Odlukom nisu obuhvaćeni osobni podaci koji se prenose radi kontrole useljavanja koju provodi Ujedinjena Kraljevina ili koji su na drugi način obuhvaćeni izuzećem od određenih prava ispitanika radi provedbe učinkovite kontrole useljavanja u skladu s točkom 4. podtočkom 1. Priloga 2. DPA-u iz 2018.

Članak 2.

Kad god nadležna nadzorna tijela u državama članicama radi zaštite pojedinaca u vezi s obradom njihovih osobnih podataka izvršavaju svoje ovlasti u skladu s člankom 58. Uredbe (EU) 2016/679 u pogledu prijenosa podataka koji su obuhvaćeni područjem primjene navedenim u članku 1., predmetna država članica o tome bez odgode obavješćuje Komisiju.

Članak 3.

1. Komisija kontinuirano prati primjenu pravnog okvira na kojem se temelji ova Odluka, uključujući uvjete pod kojima se odvijaju daljnji prijenosi, ostvaruju prava pojedinaca i tijela javne vlasti Ujedinjene Kraljevine imaju pristup podacima koji se prenose na temelju ove Odluke, kako bi ocijenila osigurava li Ujedinjena Kraljevina i dalje primjerenu razinu zaštite u smislu članka 1.

2. Države članice i Komisija međusobno se obavješćuju o slučajevima u kojima povjerenik za informiranje ili bilo koje drugo nadležno tijelo u Ujedinjenoj Kraljevini ne osigura poštovanje pravnog okvira na kojem se temelji ova Odluka.

3. Države članice i Komisija međusobno se obavješćuju o naznakama da zadiranje tijela javne vlasti Ujedinjene Kraljevine u pravo pojedinaca na zaštitu njihovih osobnih podataka prelazi ono što je nužno ili da ne postoji djelotvorna pravna zaštita od takvog zadiranja.

4. Ako ima informacije o tome da primjerena razina zaštite više nije osigurana, Komisija obavješćuje nadležna tijela Ujedinjene Kraljevine i može suspendirati, staviti izvan snage ili izmijeniti ovu Odluku.

([509]) Mišljenje 14/2021 o Nacrtu provedbene odluke Europske komisije o primjerenosti zaštite osobnih podataka u Ujedinjenoj Kraljevini u skladu s Uredbom (EU) 2016/679, dostupno na sljedećoj poveznici: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_hr.

5. Komisija može suspendirati, staviti izvan snage ili izmijeniti ovu Odluku ako zbog nesuradnje vlade Ujedinjene Kraljevine Komisija ne može utvrditi utječe li to na zaključak iz članka 1. stavka 1. ove Odluke.

Članak 4.

Ova Odluka prestaje važiti 27. lipnja 2025., osim ako se produlji u skladu s postupkom iz članka 93. stavka 2. Uredbe (EU) 2016/679.

Članak 5.

Ova je Odluka upućena državama članicama.

Sastavljeno u Bruxellesu 28. lipnja 2021.

Za Komisiju
Didier REYNDERS
Član Komisije