

EIROPAS CILVĒKTIESĪBU TIESA

LIELĀ PALĀTA

**LIETA ““BIG BROTHER WATCH” UN CITI**

**pret APVIENOTO KARALISTI”**

*(Pieteikumi Nr. 58170/13, 62322/14 un 24960/15)*

SPRIEDUMS

8. pants • Privātā dzīve • Slepenas uzraudzības režīma, tostarp masveida sakaru pārtveršanas un izlūkdatu apmaiņas, atbilstība konvencijai • Nepieciešamība izstrādāt judikatūru, ņemot vērā būtiskās atšķirības starp mērķētu pārtveršanu un masveida pārtveršanu • Pielāgots tests masveida pārtveršanas režīmu pārbaudei, veicot visaptverošu novērtēšanu • Koncentrēšanās uz ““no gala līdz galam” drošības pasākumiem”, lai ņemtu vērā aizvien lielāko iejaukšanos tiesībās uz privātās dzīves neaizskaramību dažādos masveida pārtveršanas procesa posmos • Būtiskas nepilnības masveida pārtveršanas režīmā, kam par pamatu ir atsevišķas atļaujas neesība, selektoru kategoriju neiekļaušana pieprasījumā ordera saņemšanai un sākotnējās iekšējās atļaujas nesaņemšana attiecībā uz selektoriem, kas saistīti ar personu • Pietiekama paredzamība un drošības pasākumi režīmā, lai saņemtu no ārvalstu izlūkdienestiem izlūkdatus • Režīms sakaru datu iegūšanai no sakaru pakalpojumu sniedzējiem, kas “neatbilst likumam”

10. pants • Vārda brīvība • Nepietiekama konfidenciālu žurnālistikas materiālu aizsardzība elektroniskās uzraudzības sistēmu ietvaros

STRASBŪRA

2021. gada 25. maijs

*Spriedums ir galīgs, bet tajā var tikt veikti redakcionāli labojumi.*

EIROPAS PADOME



Lietā ““Big Brother Watch” un citi pret Apvienoto Karalisti”

Eiropas Cilvēktiesību tiesa, sanākusi kā Lielā palāta šādā sastāvā:

 Roberts Spano [*Robert Spano*], *priekšsēdētājs,*

 Jons Fridriks Kjelbro [*Jon Fridrik Kjølbro*],

 Angelika Nusbergere [*Angelika Nußberger*],

 Pauls Lemenss [*Paul Lemmens*],

 Jonko Grozevs [*Yonko Grozev*],

 Vincents A. De Gaetano [*Vincent A. De Gaetano*],

 Paulo Pinto de Albukerke [*Paulo Pinto de Albuquerque*],

 Fariss Vehabovičs [*Faris Vehabović*],

 Jūlija Antoanella Motoka [*Iulia Antoanella Motoc*],

 Karlo Ranconi [*Carlo Ranzoni*],

 Mārtiņš Mits,

 Gabriele Kucsko-Štadlmeijere [*Gabriele Kucsko-Stadlmayer*],

 Marko Bošņaks [*Marko Bošnjak*],

 Tims Eike [*Tim Eicke*],

 Darians Pavli [*Darian Pavli*],

 Ēriks Venerstrēms [*Erik Wennerström*],

 Sādeta Juksela [*Saadet Yüksel*], *tiesneši,*

un Sorens Prebensens [*Søren Prebensen*], *Lielās palātas sekretāra palīgs*,

pēc apspriešanās slēgtās tiesas sēdēs 2019. gada 11. jūlijā, 2019. gada 4. un 6. septembrī un 2021. gada 17. februārī

pasludina šo spriedumu, kas pieņemts pēdējā no minētajiem datumiem.

1. TIESVEDĪBA

1. Lieta ierosināta, ņemot vērā trīs pieteikumus (Nr. 58170/13, 62322/14 un 24960/15) pret Lielbritānijas un Ziemeļīrijas Apvienoto Karalisti, ko saskaņā ar Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas (turpmāk tekstā – “Konvencija”) 34. pantu attiecīgi 2013. gada 4. septembrī, 2014. gada 11. septembrī un 2015. gada 20. maijā Tiesai iesniedza pielikumā minētās sabiedrības, labdarības organizācijas, organizācijas un personas (turpmāk tekstā – “pieteikuma iesniedzēji”).

2. Pieteikuma iesniedzējus pārstāvēja D. Kerijs [*D. Carey*] no “Deighton Pierce Glynn Solicitors”, R. Kērlinga [*R. Curling*] no “Leigh Day and Co. Solicitors” un E. Nortone [*E. Norton*] no “Liberty”. Apvienotās Karalistes valdību (turpmāk tekstā – “Valdība”) pārstāvēja tās pārstāvis Č. Vikremasinghs [*C. Wickremasinghe*] no Ārlietu un sadraudzības lietu biroja.

3. Pieteikuma iesniedzēji sūdzējās par Apvienotās Karalistes Valdības izmantoto elektroniskās uzraudzības programmu darbības jomu un apmēru.

4. Valdībai tika paziņots par pieteikumiem 2014. gada 7. janvārī, 2015. gada 5. janvārī un 2015. gada 24. novembrī. Pirmajā lietā atļauja iejaukties tika piešķirta “Human Rights Watch”, “Access Now”, “Dutch Against Plasterk”, “Center For Democracy & Technology”, Eiropas Nacionālo cilvēktiesību institūciju tīklam un Līdztiesības un cilvēktiesību komisijai, Helsinku Cilvēktiesību fondam, Starptautiskajai Juristu komisijai, “Open Society Justice Initiative”, Anglijas un Velsas Juridiskajai biedrībai un “Project Moore”. Otrajā lietā atļauja iejaukties tika piešķirta “Center For Democracy & Technology”, Helsinku Cilvēktiesību fondam, Starptautiskajai Juristu komisijai, Nacionālajai Žurnālistu biedrībai un Plašsaziņas līdzekļu juristu asociācijai. Trešajā lietā atļauja iejaukties tika piešķirta “Article 19”, Elektroniskās privātuma informācijas centram un Līdztiesības un cilvēktiesību komisijai.

5. 2017. gada 4. jūlijā Pirmās nodaļas palāta nolēma apvienot pieteikumus un rīkot mutisku paskaidrojumu uzklausīšanu. Šī uzklausīšana notika atklāti Cilvēktiesību ēkā, Strasbūrā, 2017. gada 7. novembrī. 2018. gada 13. septembrī šīs nodaļas palāta, ko veidoja tiesneši Lins‑Aleksandrs Sikiljans [*Linos-Alexandre Sicilianos*], Kristīna Pardalosa [*Kristina Pardalos*], Alešs Pejhals [*Aleš Pejchal*], Ksenija Turkoviča [*Ksenija Turković*], Armens Harutjunjans [*Armen Harutyunyan*], Paulīne Koskelo [*Pauliine Koskelo*] un Tims Eike un nodaļas sekretārs Abels Kamposs [*Abel Campos*], pasludināja spriedumu. Palāta vienbalsīgi atzina par nepieņemamām pieteikuma iesniedzēju sūdzības trešajā no apvienotajām lietām par 6. un 10. pantu, ciktāl pieteikuma iesniedzēji atsaucās uz savu statusu kā NVO, un par 14. pantu un atzina par pieņemamām pārējās šo pieteikuma iesniedzēju sūdzības. Tā ar balsu vairākumu atzina par pieņemamām pieteikuma iesniedzēju sūdzības pirmajā un otrajā no apvienotajām lietām. Palāta ar balsu vairākumu arī nolēma, ka ir noticis Konvencijas 8. un 10. panta pārkāpums gan attiecībā uz 8. panta 4. punktā noteikto režīmu, gan uz II nodaļā noteikto režīmu, un nosprieda, ka nav noticis Konvencijas 8. panta pārkāpums saistībā ar izlūkdatu apmaiņas režīmu. Spriedumam tika pievienots tiesneses Koskelo daļēji piekrītošais un daļēji atšķirīgais viedoklis, kam pievienojās tiesnese Turkoviča, kā arī tiesnešu Pardalosas un Eikes kopīgais daļēji atšķirīgais un daļēji piekrītošais viedoklis.

6. Attiecīgi 2018. gada 12. decembrī un 2018. gada 11. decembrī pieteikuma iesniedzēji pirmajā un trešajā no apvienotajām lietām lūdza nodot lietu izskatīšanai Lielajā palātā saskaņā ar Konvencijas 43. pantu. 2019. gada 4. februārī Lielās palātas tiesnešu kolēģija apmierināja šo lūgumu.

7. Lielās palātas sastāvs tika noteikts saskaņā ar Konvencijas 26. panta 4. un 5. punktu un Tiesas reglamenta 24. pantu.

8. Pieteikuma iesniedzēji un Valdība iesniedza apsvērumus (59. panta 1. punkts) par lietas pieņemamību un būtību.

9. Lielās palātas priekšsēdētājs rakstveida procesā saskaņā ar Konvencijas 36. panta 2. punktu un Tiesas reglamenta 44. panta 3. punktu piešķīra atļauju iejaukties Francijas, Norvēģijas un Nīderlandes valdībai, kā arī Apvienoto Nāciju Īpašajam ziņotājam vārda brīvības jautājumos.

10. Uzklausīšana notika atklāti Cilvēktiesību ēkā, Strasbūrā, 2019. gada 10. jūlijā.

Tiesas sēdē piedalījās:

|  |  |  |
| --- | --- | --- |
| a) *Valdības pārstāvji* |  |  |
| Č. Vikremasinghs, |  | *pārstāvis*, |
| Dž. Īdijs [*J. Eadie*] Q. C. un |  |  |
| Dž. Mitfords [*J. Mitford*], |  | *padomnieks*, |
| R. Jārdlijs [*R. Yardley*], |  |  |
| L. Morgana [*L. Morgan*], |  |  |
| H. Mobijs [*H. Mawby*], |  |  |
| T. Raterfords [*T. Rutherford*] un |  |  |
| Dž. Kījs-Braits [*J. Keay-Bright*], |  | *konsultanti*; |

|  |  |  |
| --- | --- | --- |
| b) pieteikuma iesniedzēju pārstāvji |  |  |
| B. Džafijs [*B. Jaffey*], Q. C., |  |  |
| H. Mauntfīlda [H. Mountfield], Q. C., |  |  |
| K. Makartijs [*C. McCarthy*], |  |  |
| R. Mehta [*R. Mehta*], |  |  |
| G. Saratija [*G. Sarathy*] un |  |  |
| D. Hītons [*D. Heaton*], |  | *padomnieks*, |
| D. Kerijs [*D. Carey*] un |  |  |
| R. Kērlinga, |  | *konsultanti.* |

11. Tiesa uzklausīja Īdija, Džafija un Mauntfīldas uzrunas un viņu atbildes uz jautājumiem.

1. FAKTU IZKLĀSTS

I. PRIEKŠVĒSTURE

12. Visi trīs pieteikumi tika iesniegti pēc tam, kad Edvards Snoudens [*Edward Snowden*] bija atklājis informāciju par Amerikas Savienoto Valstu un Apvienotās Karalistes izlūkdienestu izmantotajām elektroniskās uzraudzības programmām.

13. Visi pielikumā norādītie pieteikuma iesniedzēji uzskatīja, ka viņu darbībai raksturīgo iezīmju dēļ viņu elektroniskās saziņas saturu, iespējams, bija pārtvēruši Apvienotās Karalistes izlūkdienesti, ieguvuši Apvienotās Karalistes izlūkdienesti pēc tam, kad tās bija pārtvērušas citu valstu valdības, un/vai ieguvušas Apvienotās Karalistes iestādes no sakaru pakalpojumu sniedzējiem (turpmāk tekstā – “SPS”).

II. ATTIECĪGĀS INTERNETA SLEPENĀS UZRAUDZĪBAS SISTĒMAS

14. Interneta sakari galvenokārt tiek pārraidīti pa SPS izmantotajiem starptautiskajiem zemūdens optiskās šķiedras kabeļiem. Katram kabelim var būt vairāki “nesēji”, un globālajā internetā ir aptuveni 100 000 šādu nesēju. Atsevišķi sakari internetā ir iedalīti “paketēs” (datu vienībās), ko iespējams pārraidīt atsevišķi starp dažādiem nesējiem. Šīs paketes tiek nosūtītas, izmantojot visātrāko un vienlaicīgi vislētāko risinājumu. Līdz ar to dažas vai visas jebkuru konkrēto sakaru paketes, ko viena persona nosūta otrai personai neatkarīgi no tā, vai tā atrodas Apvienotajā Karalistē vai ārpus tās, iespējams maršrutēt caur vienu vai vairākām citām valstīm, ja tas iesaistīto SPS ieskatā ir optimālais risinājums.

A. Apvienotā Karaliste

1. Masveida pārtveršana

15. Edvarda Snoudena 2013. gadā atklātā informācija liecināja, ka Valdības komunikāciju galvenā pārvalde (turpmāk tekstā – “*GCHQ*”, viens no Apvienotās Karalistes izlūkdienestiem) īstenoja operāciju ar nosaukumu “TEMPORA”, ļaujot piekļūt milzīga apjoma datiem, kuri iegūti no nesējiem, un tos uzglabāt. Apvienotās Karalistes iestādes ne apstiprināja, ne noliedza operācijas “TEMPORA” esību.

16. Tomēr saskaņā ar Parlamenta Izlūkošanas un drošības komitejas 2015. gada marta ziņojumu (turpmāk tekstā – “*ISC* ziņojums”, skat. turpmāk 142.–149. punktu) *GCHQ* izmantoja divas vērienīgas apstrādes sistēmas masveida sakaru pārtveršanai.

17. Pirmā no abām *ISC* ziņojumā minētajām apstrādes sistēmām attiecās uz ļoti nelielu nesēju daļu. Sakariem plūstot starp attiecīgajiem nesējiem, sistēma veica informācijas plūsmas salīdzināšanu ar “vienkāršiem selektoriem”, proti, konkrētiem identifikatoriem (piemēram, e-pasta adresēm), kas saistīti ar kādu zināmu adresātu. Sakari, kas atbilda šiem vienkāršajiem selektoriem, tika apkopoti, savukārt sakari, kas tiem neatbilda, automātiski tika atmesti. Pēc tam analītiķi veica apkopoto sakaru “šķirošanas procesu”, lai noteiktu saziņas aktu saturu ar vislielāko izlūkošanas vērtību, kas līdz ar to ir jāatver un jāizlasa. Analītiķi no visas šā procesa ietvaros apkopotās informācijas praktiski atvēra un izlasīja tikai ļoti nelielu informācijas daļu. Saskaņā ar *ISC* ziņojumu *GCHQ* nevarēja izlasīt visu saziņas aktu saturu.

18. Otrā apstrādes sistēma attiecās uz vēl mazāku nesēju skaitu (pakārtoti tiem nesējiem, kuriem tika piekļūts iepriekšējā punktā aprakstītā procesa ietvaros), kuri bija apzināti izraudzīti kā tādi, kas, visticamāk, varētu pārraidīt izlūkošanas ziņā vērtīgu saziņas aktu saturu. Šī otrā sistēma ietvēra divus posmus: pirmkārt, sākotnēju tādu “apstrādes noteikumu” kopuma piemērošanu, kas bija izstrādāts, lai atmestu materiālu ar, visticamāk, vismazāko izlūkošanas vērtību, un, otrkārt, sarežģītu vaicājumu piemērošanu atlasītajam materiālam, lai iegūtu materiālu ar, visticamāk, vislielāko izlūkošanas vērtību. Balstoties uz šiem meklējumiem, tika iegūts konkrēts indekss, un analītiķi varēja pārbaudīt vienīgi informāciju ar šādu indeksu. Viss saziņas aktu saturs, kam nebija šāda indeksa, bija jāatmet.

19. Tiesiskais regulējums par masveida pārtveršanu, kas bija spēkā attiecīgajā brīdī, ir detalizēti izklāstīts turpmāk iedaļā “Piemērojamie valsts tiesību akti”. Īsi sakot, 2000. gada Likuma par izmeklēšanas pilnvaru regulējumu [*Regulation of Investigatory Powers Act 2000*] (turpmāk tekstā – “*RIPA*”, skat. turpmāk 72. punktu) 8. panta 4. punkts ļāva valsts sekretāram izdot orderus “ārējo sakaru pārtveršanai”, un saskaņā ar *RIPA* 16. pantu (skat. turpmāk 84.–92. punktu) pārtverto materiālu nevarēja atlasīt, lai to lasītu, aplūkotu vai klausītos, “ņemot vērā faktoru, kas attiecināms uz personu, par kuru zināms, ka tā attiecīgajā brīdī atrodas Britu salās”.

2. Izlūkdatu apmaiņa

20. Sakaru pārtveršanas prakses kodeksa [*Interception of Communications Code of Practice*] (turpmāk tekstā – “*IC* kodekss”, skat. turpmāk 116. punktu) 12. nodaļā bija izklāstīti apstākļi, kādos Apvienotās Karalistes izlūkdienesti varēja pieprasīt izlūkdatus no ārvalsts izlūkdienestiem, kā arī šāda pieprasījuma iesniegšanas kārtība. 12. nodaļa *IC* kodeksam tika pievienota pēc tam, kad Izmeklēšanas pilnvaru tiesa (turpmāk tekstā – “*IPT*”) bija uzdevusi izlūkdienestiem izpaust savus izlūkdatu apmaiņas pasākumus tiesvedībā, ko pieteikuma iesniedzēji bija ierosinājuši apvienotajās lietās (““Liberty” tiesvedība”, skat. turpmāk 28.–60. punktu).

3. Sakaru datu iegūšana no SPS

21. *RIPA* II nodaļa un Sakaru datu ieguves prakses kodekss [*Acquisition of Communications Data Code of Practice*] noteica kārtību, kādā konkrētas valsts iestādes varēja pieprasīt sakaru datus no SPS (skat. turpmāk 117.–121. punktu).

B. Amerikas Savienotās Valstis

22. Nacionālās drošības aģentūra (turpmāk tekstā – “*NSA*”) atzina divu operāciju, proti, “PRISM” un “Upstream”, esību.

1. “PRISM”

23. “PRISM” bija programma, ar kuras palīdzību Amerikas Savienoto Valstu valdība ieguva izlūkošanas materiālu (piemēram, saziņas aktu saturu) no interneta pakalpojumu sniedzējiem (turpmāk tekstā – “IPS”). Piekļuve programmas “PRISM” ietvaros bija konkrēta un mērķēta (pretēji plašai datu iegūšanai). Amerikas Savienoto Valstu pārvalde norādīja, ka programmu regulēja Ārvalstu izlūkošanas uzraudzības likums [*Foreign Intelligence Surveillance Act*] (turpmāk tekstā – “*FISA*”) un ka pieteikumi par piekļuvi materiālam programmas “PRISM” ietvaros bija jāapstiprina Ārvalstu izlūkošanas uzraudzības tiesai (turpmāk tekstā – “*FISC*”).

24. Edvarda Snoudena nopludinātie *NSA* dokumenti liecināja, ka *GCHQ* bija piekļuve programmai “PRISM” kopš 2010. gada jūlija un tā šo programmu izmantoja, lai sagatavotu izlūkošanas ziņojumus. *GCHQ* atzina, ka tā no Amerikas Savienotajām Valstīm saņēma informāciju, kas bija iegūta, izmantojot programmu “PRISM”.

2. “Upstream”

25. Saskaņā ar nopludinātajiem dokumentiem programma “Upstream” ļāva apkopot saturu un sakaru datus no Amerikas Savienoto Valstu SPS piederošajiem optiskās šķiedras kabeļiem un infrastruktūras. Šī programma nodrošināja plašu piekļuvi globālajiem datiem, jo īpaši par personām, kuras nav ASV pilsoņi. Šos datus pēc tam varēja apkopot, uzglabāt un meklēt, izmantojot atslēgvārdus (skat. detalizētu informāciju turpmāk 261.–264. punktā).

III. VALSTS TIESVEDĪBA PIRMAJĀ UN OTRAJĀ NO APVIENOTAJĀM LIETĀM

26. 2013. gada 3. jūlijā pieteikuma iesniedzēji pirmajā no apvienotajām lietām (pieteikums Nr. 58170/13) iesniedza Valdībai pirmstiesas brīdinājuma vēstuli, kurā tie izklāstīja savas sūdzības un lūdza atzīt, ka 1994. gada Izlūkdienestu likuma [*Intelligence Services Act 1994*] (turpmāk tekstā – “*ISA*”, skat. turpmāk 108. un 110. punktu) 1. un 3. pants, 1989. gada Drošības dienestu likuma [*Security Services Act 1989*] (turpmāk tekstā – “*SSA*”, skat. turpmāk 106. punktu) 1. pants un *RIPA* 8. pants (skat. turpmāk 66. punktu) neatbilst Konvencijai. Valdība savā 2013. gada 26. jūlija atbildē apgalvoja, ka *RIPA* 65. panta 2. punkta mērķis bija izslēgt Augstās tiesas kompetenci saistībā ar sūdzībām par cilvēktiesībām, kas iesniegtas pret izlūkdienestiem, taču pieteikuma iesniedzēji varēja iesniegt savas sūdzības *IPT*. Tā norādīja, ka *IPT* ir īpaša tiesa, kas izveidota saskaņā ar *RIPA*, lai uzklausītu pilsoņu apgalvojumus par iespējamu pretlikumīgu iejaukšanos viņu saziņā tādas rīcības dēļ, uz kuru attiecas šis likums, un ka tai bija ekskluzīva kompetence izskatīt jebkuru sūdzību par personas sakaru pārtveršanu un, ja pārtveršana ir notikusi, pārbaudīt šīs pārtveršanas pilnvaras (skat. turpmāk 122.–133. punktu). Tomēr šie pieteikuma iesniedzēji nebija šādi rīkojušies.

27. Pieteikuma iesniedzēji otrajā no apvienotajām lietām (pieteikums Nr. 62322/14) neierosināja valsts tiesvedību, jo tie neuzskatīja, ka tiem ir pieejams efektīvs tiesiskās aizsardzības līdzeklis saistībā ar to sūdzībām, ko tie bija iesnieguši saskaņā ar Konvenciju.

IV. VALSTS TIESVEDĪBA TREŠAJĀ NO APVIENOTAJĀM LIETĀM

28. Katra no desmit cilvēktiesību aizsardzības organizācijām, kuras bija pieteikuma iesniedzēji trešajā no apvienotajām lietām (pieteikums Nr. 24960/15), laika posmā no 2013. gada jūnija līdz 2013. gada decembrim iesniedza sūdzību *IPT* (turpmāk tekstā – ““Liberty” tiesvedība”). Tās apgalvoja, ka izlūkdienesti, iekšlietu sekretārs un ārlietu sekretārs bija rīkojušies pretēji Konvencijas 8., 10. un 14. pantam: i) piekļūstot pārtvertajam saziņas aktu saturam un sakaru datiem vai kā citādi tos saņemot no Amerikas Savienoto Valstu valdības, izmantojot programmas “PRISM” un “Upstream” (turpmāk tekstā – “jautājums par “PRISM””), un ii) pārtverot, pārbaudot un saglabājot to pieteikuma iesniedzēju saziņas aktu saturu un sakaru datus, izmantojot programmu “TEMPORA” (turpmāk tekstā – “jautājums par 8. panta 4. punktu”).

29. 2014. gada 14. februārī *IPT* uzdeva apvienot šīs desmit lietas. Pēc tam tā izraudzījās tiesas padomnieku (skat. turpmāk 132. punktu), kura uzdevums bija palīdzēt *IPT* jebkādā tās norādītā veidā, tostarp pārstāvot to jautājumos, kuros ne visas puses iespējams pārstāvēt (piemēram, valsts drošības apsvērumu dēļ).

30. Valdība atbildē uz pieteikuma iesniedzēju apgalvojumiem ieņēma “ne apstiprināšanas, ne noliegšanas” nostāju, proti, tā atteicās apstiprināt vai noliegt, ka pieteikuma iesniedzēju saziņas aktu saturs patiesībā tika pārtverts. Tāpēc tika noteikts, ka *IPT* izlems juridiskos jautājumus, pamatojoties uz pieņēmumiem, proti, ka *NSA* bija ieguvusi pieteikuma iesniedzēju saziņas aktu saturu un sakaru datus, izmantojot programmu “PRISM” vai “Upstream”, un tos nodevusi *GCHQ*, kur tie tika saglabāti, uzglabāti un analizēti un ar tiem apmainījās, un ka *GCHQ* bija pārtvērusi pieteikumu iesniedzēju sakaru datus, izmantojot programmu “TEMPORA”, un tos saglabājusi, uzglabājusi un analizējusi un ar tiem apmainījusies. Bija jāizvērtē, vai, pamatojoties uz šiem pieņēmumiem, datu pārtveršana, saglabāšana, uzglabāšana un apmaiņa atbilda Konvencijas 8. un 10. pantam, tos aplūkojot atsevišķi un kopā ar Konvencijas 14. pantu.

A. Paskaidrojumu uzklausīšana

31. *IPT* divu Augstās tiesas tiesnešu, iecirkņa tiesneša un divu vecāko tiesas advokātu sastāvā rīkoja atklātu paskaidrojumu uzklausīšanu, kas norisinājās 2014. gada 14.–18. jūlijā. Valdība lūdza rīkot papildu slēgtu paskaidrojumu uzklausīšanu, lai *IPT* varētu izvērtēt *GCHQ* nepubliskotos – atklātajā paskaidrojumu uzklausīšanā kā “zem ūdenslīnijas” raksturotos – iekšējos pasākumus pārtvertā materiāla apstrādei. Pieteikuma iesniedzēji pret to iebilda, apgalvojot, ka slēgtas paskaidrojumu uzklausīšanas rīkošana nav pamatota un ka šo pasākumu neizpaušana viņiem nav taisnīga.

32. Lūgums rīkot slēgtu paskaidrojumu uzklausīšanu tika apmierināts saskaņā ar *IPT* Reglamenta 9. pantu (skat. turpmāk 129. punktu). 2014. gada 10. septembrī notika slēgta paskaidrojumu uzklausīšana, kurā *IPT* “tika atbalstīta, pilnvērtīgi, uztveroši un neitrāli piedaloties .. tiesas padomniekam”, kura uzdevumi bija: i) apzināt dokumentus, to daļas vai galvenos punktus, kas pienācīgi būtu jāizpauž; ii) sniegt argumentus, atbalstot šādu izpaušanu, kas bija prasītāju un atklāta tiesiskuma interesēs, un iii) nodrošināt, ka *IPT* tiek izvirzīti visi atbilstošie argumenti (no prasītāju skatpunkta) par faktiem un tiesību aktiem.

33. Slēgtajā paskaidrojumu uzklausīšanā *IPT* izvērtēja iekšējos (“zem ūdenslīnijas” esošos) pasākumus, kas regulē izlūkdienestu rīcību un praksi. 2014. gada 9. oktobrī tā paziņoja pieteikuma iesniedzējiem, ka tās ieskatā zināmu slēgtu materiālu varētu izpaust. Tā paskaidroja, ka tā bija aicinājusi Valdību izpaust materiālu un Valdība tam bija piekritusi. Šis materiāls pieteikuma iesniedzējiem attiecīgi tika sniegts paziņojuma veidā (turpmāk tekstā – “9. oktobra paziņojums”), un lietas dalībnieki tika aicināti izvirzīt *IPT* argumentus par izpausto materiālu.

34. Pieteikuma iesniedzēji vēlējās iegūt informāciju par paziņojuma kontekstu un avotu, taču *IPT* atteicās sniegt papildu informāciju. Pieteikuma iesniedzēji izvirzīja rakstveida argumentus par šo paziņojumu.

35. Atbildētāji pēc tam grozīja un izvērsa izpausto materiālu.

36. Pēc galīgo paziņojumu sniegšanas 2014. gada 12. novembrī 9. oktobra paziņojumā bija norādīts:

“ASV valdība ir publiski atzinusi, ka sistēma “Prism” un programma “Upstream” .. ļauj iegūt saziņu saturu ar, no vai par konkrētiem selektoriem, kas saistīti ar personām, kuras nav ASV pilsoņi un attiecībā par kurām ir pamats uzskatīt, ka tās atrodas ārpus Amerikas Savienotajām Valstīm, lai iegūtu ārvalsts izlūkdatus. Ciktāl ASV valdība ļauj izlūkdienestiem pieprasīt materiālu, kas iegūts, izmantojot sistēmu “Prism” (un/vai .. atbilstoši programmai “Upstream”), šādus pieprasījumus var iesniegt vienīgi attiecībā uz neanalizētiem pārtvertiem sakariem (un saistītajiem sakaru datiem), kas iegūti šādā veidā.

1. Šādu pieprasījumu attiecībā uz neanalizētiem pārtvertiem sakariem (un saistītajiem sakaru datiem), izņemot saskaņā ar kādu starptautisku savstarpējās tiesiskās palīdzības līgumu, izlūkdienesti var iesniegt ārpus Apvienotās Karalistes esošas valsts vai teritorijas valdībai vienīgi tad, ja:

a) valsts sekretārs saskaņā ar [*RIPA*] jau ir izdevis attiecīgo orderi par pārtveršanu, attiecīgo sakaru iegūšanai ir nepieciešama ārvalsts valdības palīdzība, jo tos nav iespējams iegūt saskaņā ar attiecīgo *RIPA* noteikto orderi par pārtveršanu, šo sakaru iegūšana izlūkdienestu ieskatā ir nepieciešama un samērīga vai

b) pieprasījuma iesniegšana par attiecīgajiem sakariem, ja nav saņemts attiecīgais *RIPA* noteiktais orderis par pārtveršanu, nav uzskatāma par apzinātu *RIPA* apiešanu vai citādi nav pretrunā ar principiem, kas noteikti spriedumā lietā ““Padfield” pret lauksaimniecības, zivsaimniecības un pārtikas ministru” [1968] AC 997 [par to, ka publisko tiesību subjektam ir jāīsteno sava rīcības brīvība, lai sekmētu (nevis apietu) politiku un tā tiesiskā regulējuma mērķus, ar kuriem šī rīcības brīvība tika noteikta] (piemēram, tādēļ, ka sakaru iegūšana saskaņā ar *RIPA* noteikumiem par pārtveršanu tehniski nav iespējama), un šo sakaru iegūšana izlūkdienestu ieskatā ir nepieciešama un samērīga. Šajos apstākļos valsts sekretāram personīgi jāizvērtē jautājums par šāda pieprasījuma iesniegšanu un jāpieņem attiecīgais lēmums. Šāds pieprasījums būtu iesniedzams vienīgi izņēmuma gadījumā, kas šā paziņojuma sagatavošanas dienā nav noticis.

(..)

2. Ja izlūkdienesti saņem pārtvertu sakaru saturu vai sakaru datus no kādas ārpus Apvienotās Karalistes esošas valsts vai teritorijas valdības neatkarīgi no tā, vai tas tiek vai netiek pieprasīts, saturs ir vai nav analizēts vai arī sakaru dati ir vai nav saistīti ar sakaru saturu, uz sakaru saturu un datiem saskaņā ar iekšējiem “pasākumiem” ir piemērojami tādi paši iekšējie noteikumi un drošības pasākumi kā tad, ja izlūkdienesti tos iegūst tieši, tos pārtverot saskaņā ar *RIPA*.

3. Izlūkdienesti, kuri saņem neanalizētu pārtvertu materiālu un saistītos sakaru datus, veicot pārtveršanu saskaņā ar 8. panta 4. punktā noteikto orderi, īsteno iekšējus “pasākumus”, attiecībā uz ko ir jāizveido ieraksts, kurā jāpaskaidro, kādēļ nepieciešams piekļūt neanalizētajam pārtvertajam materiālam, pirms tam var piekļūt kāda pilnvarota persona saskaņā ar *RIPA* 16. pantu.

4. Iekšējie “pasākumi”, ko īsteno izlūkdienesti, kuri saņem neanalizētu pārtvertu materiālu un saistītos sakaru datus, veicot pārtveršanu saskaņā ar 8. panta 4. punktā noteikto orderi, paredz (vai atkarībā no attiecīgās sistēmas uzliek par pienākumu noteikt) maksimālos saglabāšanas periodus dažādām šādu datu kategorijām, kas norāda uz attiecīgo datu raksturīgajām iezīmēm un iejaukšanās pakāpi. Šādi paredzēti (vai noteikti) laika periodi parasti nepārsniedz 2 gadus un konkrētos gadījumos ir ievērojami īsāki (izlūkošanas ziņojumus, kas balstīti uz šiem datiem, uzskata par atsevišķu kategoriju un saglabā ilgāk). Datus var saglabāt ilgāk par piemērojamo maksimālo saglabāšanas periodu, ja iepriekš no attiecīgā izlūkdienesta vecākās amatpersonas ir saņemta atļauja, pamatojoties uz to, ka konkrēto datu turpmāka saglabāšana ir tikusi atzīta par nepieciešamu un samērīgu (ja pēc tam tiek atzīts, ka šo datu turpmāka saglabāšana vairs neatbilst nepieciešamības un samērīguma pārbaudēm, tie tiek dzēsti). Ciktāl tas iespējams, visu saglabāšanas periodu pamatā ir automātiskas dzēšanas process, kas tiek uzsākts, tiklīdz ir apritējis attiecīgajiem datiem piemērojamais maksimālais saglabāšanas periods. Maksimālos saglabāšanas periodus pārrauga un saskaņo komisārs. Konkrēti attiecībā uz saistītajiem sakaru datiem sers Entonijs Mejs [*Anthony May*] sniedza ieteikumu tiem izlūkdienestiem, kuri saņem neanalizētu pārtvertu materiālu un saistītos sakaru datus, veicot pārtveršanu saskaņā ar 8. panta 4. punktā noteikto orderi, un pagaidu komisārs (sers Pols Kenedijs [*Paul Kennedy*]) nesen ir paudis apmierinātību ar šā ieteikuma īstenošanu.

5. Izlūkdienestu iekšējie “pasākumi” saskaņā ar [1989. gada Drošības dienestu likumu], [1994. gada Izlūkdienestu likumu] un *RIPA* 15.–16. pantu tiek periodiski pārskatīti, lai nodrošinātu to aktualitāti un efektivitāti. Turklāt izlūkdienesti turpmāk šādas periodiskās pārskatīšanas laikā apņemas izvērtēt, vai vairākus šos iekšējos pasākumus varētu droši un lietderīgi nodot atklātībā (piemēram, iekļaujot attiecīgajā, likumā noteiktajā prakses kodeksā).”

B. *IPT* pirmais 2014. gada 5. decembrī pasludinātais spriedums

37. *IPT* pasludināja savu pirmo spriedumu 2014. gada 5. decembrī. Spriedums attiecās uz tobrīd ieviestajiem pasākumiem sakaru pārtveršanai un ārvalsts izlūkdienestu pārtverto sakaru saņemšanai.

1. Jautājums par “PRISM”

38. *IPT* atzina, ka jautājums par “PRISM” skar Konvencijas 8. pantu, lai gan “zemākā līmenī” nekā režīms, kas tika aplūkots spriedumā lietā Nr. 54934/00 “Vēbere [*Weber*] un Sarāvija [*Saravia*] pret Vāciju” (lēmums), ECT 2006-XI. Saskaņā ar šo spriedumu iestādēm, kuras bija iesaistītas no ārvalsts izlūkdienestiem saņemtā saziņu satura apstrādē, bija jāizpilda 8. panta prasības, jo īpaši saistībā ar tā uzglabāšanu, apmaiņu, saglabāšanu un iznīcināšanu. *IPT* ieskatā, pamatojoties uz 2009. gada 10. marta sprieduma lietā Nr. 4378/02 “Bikovs [*Bykov*] pret Krieviju” [*GC*] 76. un 78. punktu un 1984. gada 2. augusta spriedumu lietā “Malouns [*Malone*] pret Apvienoto Karalisti”, A sērija Nr. 82, lai iejaukšanos uzskatītu par “atbilstošu likumam”, izpildvarai nevar būt neierobežota rīcības brīvība; drīzāk noteikumu būtībai ir jābūt skaidrai, savukārt to darbības jomai, ciktāl tas iespējams, ir jābūt publiski pieejamai. Tomēr tā uzskatīja par pašsaprotamu, ka valsts drošības jomā daudz mazāka apjoma informācijai ir jābūt publiski pieejamai un ka ir jāsamazina 8. pantā noteiktā paredzamības pakāpe, jo citādi tiktu apdraudēts valsts drošības pasākumu mērķis (citēts 1987. gada 26. marta sprieduma lietā “Leanders [*Leander*] pret Zviedriju” 51. punkts, A sērija Nr. 116).

39. *IPT* turpināja:

“41. Mēs uzskatām, ka ir nepieciešama pietiekama noteikumu vai pasākumu norādīšana, ciktāl tie netiek izpausti (..). Mēs esam pārliecināti, ka izlūkdatu apmaiņas jomā nav paredzams, ka noteikumiem ir jābūt ietvertiem tiesību aktā (kā spriedumā lietā “Vēbere”) vai pat kodeksā (kā to paredzēja Tiesas secinājumi 2008. gada 1. jūlija spriedumā lietā Nr. 58243/00 ““Liberty” pret [Apvienoto Karalisti”]). Mūsu spriedumā pietiek ar to, ka:

i) atbilstoši noteikumi vai pasākumi ir ieviesti, tie ir publiski zināmi un ir apstiprināta to esība, turklāt ir pienācīgi norādīts to saturs, lai par tiem sniegtu adekvātu norādi (kā spriedumā lietā “Malouns” ..);

ii) tie ir pakļauti pienācīgai kontrolei.”

40. *IPT* piebilda, ka informācijas apmaiņas pasākumi ir paredzēti tiesiskajā regulējumā, kas ietverts 1989. gada Drošības dienestu likumā (skat. turpmāk 105.–106. punktu) un 1994. gada Izlūkdienestu likumā (skat. turpmāk 107.–110. punktu). Tā arī atsaucās uz liecību, ko iepriekšminētajā “Liberty” tiesvedībā sniedza Iekšlietu ministrijas Drošības un terorisma apkarošanas biroja ģenerāldirektors Čārlzs Farrs [*Charles Farr*], kurš paskaidroja, ka minētajos likumos ietvertais tiesiskais regulējums ir balstīts uz detalizētiem iekšējiem norādījumiem, tostarp pasākumiem, kuru mērķis ir nodrošināt, ka dienesti saņem vienīgi atbilstošai funkciju izpildei nepieciešamo informāciju. Viņš arī norādīja, ka personāls ir pabeidzis obligātās mācības par tiesisko un politikas regulējumu, kurā tas darbojās, kā arī ir saņēmis skaidrus norādījumus par to, ka ir stingri jāievēro tiesību akti un iekšējie norādījumi. Visbeidzot viņš apgalvoja, ka detalizēta informācija par pasākumiem ir konfidenciāla, jo to nevar droši publiskot, neapdraudot valsts drošības intereses.

41. *IPT* atzina, ka, tā kā pasākumi nebija publiskoti, pat ne kopsavilkuma veidā, tie nebija pieejami. Tomēr *IPT* ieskatā bija svarīgi, ka pasākumus kontrolēja un izmeklēja Parlamenta Izlūkošanas un drošības komiteja (turpmāk tekstā – “*ISC*”) un neatkarīgs komisārs sakaru pārtveršanas jautājumos (turpmāk tekstā – “*IC* komisārs”). Turklāt tā arī pati varēja nodrošināt šādu kontroli, piekļūstot visai slepenajai informācijai, un pārtraukt slēgto paskaidrojumu uzklausīšanu, lai izvērtētu, vai Farra minētie pasākumi ir ieviesti un spēj nodrošināt individuālu aizsardzību pret patvaļīgu iejaukšanos.

42. Izvērtējot “zem ūdenslīnijas” esošos pasākumus, *IPT* guva pārliecību, ka 9. oktobra paziņojumā (ar turpmākiem grozījumiem, skat. iepriekš 33. un 36. punktu) sniegts skaidrs un precīzs pārskats par slēgtajā paskaidrojumu uzklausīšanā sniegto pierādījumu daļu un ka pārējie slēgtajā paskaidrojumu uzklausīšanā sniegtie pierādījumi ir pārāk sensitīvi, lai tos izpaustu, neapdraudot valsts drošību, vai “ne apstiprināšanas, ne noliegšanas” principam. Tā arī guva pārliecību, ka priekšnoteikumi informācijas pieprasīšanai no Amerikas Savienoto Valstu valdības bija skaidri, proti, bija nepieciešams 8. panta 1. punktā vai 8. panta 4. punktā minētais orderis, kura darbības jomā ietilpa ierosinātā mērķa saziņu saturs, vienlaicīgi ņemot vērā arī 16. panta 3. punkta grozījumus (skat. turpmāk 86. punktu), ja bija zināms, ka persona atradās Britu salās. Līdz ar to uz jebkuru pieprasījumu saskaņā ar “PRISM” vai “Upstream” attiecībā uz pārtverto informāciju vai sakaru datiem attiecās *RIPA* noteiktais režīms, ja vien tas neatbilda galēja izņēmuma scenārijam, kas izklāstīts pēc pirmās paskaidrojumu uzklausīšanas publiskotā materiāla 1. punkta b) apakšpunktā. Taču 1. punkta b) apakšpunktā minētais pieprasījums netika iesniegts.

43. Tomēr *IPT* par “satraucošu” atzina šādu jautājumu:

“Lai gan uz jebkuru pārtvertās informācijas vai sakaru datu pieprasījumu vai saņemšanu saskaņā ar “Prism” un/vai “Upstream” attiecas tie paši drošības pasākumi kā gadījumā, kad pārtverto informāciju vai sakaru datus iegūst tieši atbildētāji, ja tika iesniegts 1. punkta b) apakšpunktā noteiktais pieprasījums, kaut arī tas jāiesniedz valsts sekretāram un ar jebkuru šādi iegūtu materiālu jārīkojas saskaņā ar *RIPA*, pastāv iespēja, ka 16. pantā minētie aizsardzības pasākumi nav piemērojami. Kā minēts iepriekš, 1. punkta b) apakšpunktā minētais pieprasījums netika iesniegts, tādēļ šajā ziņā nav radušās nekādas problēmas. Tomēr mēs esam pārliecināti, ka bija jāievieš procedūra, kas paredz, ka jebkuram šādam pieprasījumam, ja tāds iesniegts un nosūtīts izskatīšanai valsts sekretāram, jāattiecas uz 16. panta 3. punkta jautājumu.”

44. Tomēr, ņemot vērā šo iebildumu, *IPT* secināja:

“i) Izvērtējot “zem ūdenslīmeņa” esošos pasākumus, kā tie raksturoti šajā spriedumā, mēs esam guvuši pārliecību, ka bija ieviesti adekvāti pasākumi, lai nodrošinātu atbilstību tiesiskajam regulējumam un Konvencijas 8. un 10. pantam, ciktāl tas attiecas uz pārtvertās informācijas saņemšanu, izmantojot “Prism” un/vai “Upstream”.

ii) Protams, ar to vien nepietiek, jo šiem pasākumiem ir jābūt pietiekami pieejamiem sabiedrībai. Mēs esam guvuši pārliecību, ka tie ir pietiekami skaidri norādīti tiesiskajā regulējumā, uz kuru mēs esam atsaukušies, un *ISC* un komisāra iepriekš citētajos apgalvojumos un ka tos kopš šā brīža, proti, pēc abām slēgtajām paskaidrojumu uzklausīšanas reizēm, atbildētāji ir publiski izpauduši un tie ir norādīti šajā spriedumā.

iii) Šie pasākumi tiek kontrolēti.

iv) Atbildētājiem piešķirtās rīcības brīvības apjoms, lai saņemtu un izmantotu pārtverto materiālu un sakaru datus, un (saskaņā ar 8. panta 4. punkta jautājumiem, kā norādīts turpmāk) tās īstenošanas veids attiecīgi (un atbilstoši tam, kā norādīts lietā “Bikovs”, skat. iepriekš 37. punktu) ir pieejams un pietiekami skaidrs, lai nodrošinātu personai adekvātu aizsardzību pret patvaļīgu iejaukšanos.”

45. Visbeidzot *IPT* pievērsās argumentam, ko bija izvirzījusi vienīgi organizācija “Amnesty International”, proti, ka Apvienotajai Karalistei saskaņā ar Konvencijas 8. pantu bija pozitīvs pienākums novērst vai nepieļaut, ka Amerikas Savienotās Valstis pārtver sakarus, kā arī pienākums neatbalstīt šādu pārtveršanu, saņemot tās produktu. Tomēr *IPT*, citējot 2012. gada 31. jūlija sprieduma lietā Nr. 40020/03 “M. un citi pret Itāliju un Bulgāriju” 127. punktu, piebilda, ka “ar Konvenciju izveidotās institūcijas atkārtoti ir norādījušas, ka Konvencijā nav noteiktas tiesības, kas paredzētu Augstajai Līgumslēdzējai pusei īstenot diplomātisku aizsardzību vai atbalstīt pieteikuma iesniedzēja sūdzības, kas iesniegtas saskaņā ar starptautiskajām tiesībām, vai kā citādi iejaukties kādas citas valsts iestāžu darbā pieteikuma iesniedzēja vārdā”. Tādēļ *IPT* noraidīja šo argumentu.

2. 8. panta 4. punkta jautājums

46. *IPT* formulēja četrus jautājums, kas bija jāizlemj, lai noteiktu, vai 8. panta 4. punktā minētais režīms (kas paredzēja tiesisko regulējumu ārējo sakaru masveida pārtveršanai) atbilst Konvencijai:

“1) Vai grūtības noteikt atšķirību starp ārējiem un iekšējiem sakariem .. ir pamats tam, ka 8. panta 4. punktā noteiktais režīms neatbilst likumam un līdz ar to ir pretrunā ar Konvencijas 8. panta 2. punktu?

2) Vai *RIPA* 16. pantā noteiktais drošības pasākums ir pietiekams, ciktāl tas nepieciešams, lai Konvencijas 8. panta pārkāpums būtu attaisnojams ar likumu?

3) Vai režīms neatkarīgi no tā, vai tiek vai netiek ņemts vērā 16. pants, pietiekami atbilst spriedumā lietā “Vēbere” izklāstītajām prasībām, ciktāl tas nepieciešams, lai nodrošinātu atbilstību likumam?

4) Vai 16. panta 2. punkts ir netieši diskriminējošs, tādējādi pārkāpjot Konvencijas 14. pantu, un, ja tā, vai tas ir attaisnojams?”

47. Attiecībā uz pirmo jautājumu pieteikuma iesniedzēji apgalvoja, ka pēc “radikālajām izmaiņām kopš 2000. gada” pamatā visi sakari tagad ir ārēji un ka līdz ar to 8. panta 4. punktā noteiktais iekšējo un ārējo sakaru iedalījums vairs nav “piemērots nolūkam”. Lai gan *IPT* atzina, ka tehnoloģiskās izmaiņas ir bijušas vērienīgas un ka pārtveršanas posmā nav iespējams nošķirt ārējos un iekšējos sakarus, tā nosprieda, ka šīs atšķirības jēdziena “ārējie sakari” precīzas definīcijas kontekstā *per se* nav pamats tam, lai 8. panta 4. punktā noteiktais režīms būtu pretrunā ar Konvencijas 8. panta 2. punktu. Šajā ziņā tā uzskatīja, ka grūtības atšķirt “iekšējos” sakarus no “ārējiem” sakariem ir pastāvējušas jau kopš *RIPA* pieņemšanas un ka tehnoloģisko izmaiņu dēļ nav būtiski palielinājies to sakaru apjoms vai īpatsvars, ko pārtveršanas brīdī varētu vai nevarētu uzskatīt par ārējiem vai iekšējiem. Tās vissliktākajā gadījumā “ir paātrinājušas procesu, kādā aizvien vairāk lietu pasaulē faktiski kļūst ārējas, nevis iekšējas”. *IPT* norādīja, ka jebkurā gadījumā šādai atšķirībai ir bijusi nozīme vienīgi pārtveršanas posmā. Tā apgalvoja, ka “visgrūtāko darbu” jau ir paveicis *RIPA* 16. pants, kas liedzis atlasīt pārtverto materiālu, lai to lasītu, aplūkotu vai klausītos, “ņemot vērā faktoru, kas attiecināms uz personu, par kuru zināms, ka tā attiecīgajā brīdī atrodas Britu salās” (skat. turpmāk 84.–92. punktu). Turklāt visus sakarus, kas pārtverti saskaņā ar 8. panta 4. punktā minēto orderi, var izvērtēt pārbaudes veikšanai, vienīgi atsaucoties uz šo pantu.

48. Attiecībā uz otro jautājumu *IPT* uzskatīja, ka 16. pantā noteiktie drošības pasākumi, kas piemēroti vienīgi pārtvertajam materiālam, nevis saistītajiem sakaru datiem, ir bijuši pietiekami. Lai gan tā secināja, ka spriedumā lietā “Vēbere” noteiktie kritēriji attiekušies arī uz sakaru datiem, tā uzskatīja, ka bijuši nodrošināti adekvāti aizsardzības un drošības pasākumi, atsaucoties uz *RIPA* 15. pantu (skat. turpmāk 77.–82. punktu). Turklāt, ciktāl 16. pants sakaru saturam ir paredzējis lielāku aizsardzību nekā sakaru datiem, šī atšķirība ir bijusi pamatota un samērīga, jo sakaru dati bijuši nepieciešami, lai identificētu personas, kuru pārtvertā materiāla aizsardzību paredz 16. pants (proti, personas, par kurām zināms, ka tās atrodas Britu salās).

49. Pievēršoties trešajam jautājumam, *IPT* secināja, ka 8. panta 4. punktā noteiktais režīms pietiekami atbildis spriedumā lietā “Vēbere” izklāstītajiem kritērijiem (proti, iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 95. punktā minētajiem kritērijiem, skat. arī turpmāk 274. un 335. punktu) un jebkurā gadījumā bijis “atbilstošs likumam”. Attiecībā uz pirmo un otro prasību tā uzskatīja, ka atsaukšanās uz “valsts drošību” bija pietiekami skaidra (citējot “Esbesters [*Esbester*] pret Apvienoto Karalisti” (lēmums), Nr. 18601/91, 1993. gada 2. aprīlis, un “Kenedijs [*Kennedy*] pret Apvienoto Karalisti”, Nr. 26839/05, 2010. gada 18. maijs); mērķtiecīgas kontroles neesība pārtveršanas posmā bija pieņemama un neizbēgama, kā tas norādīts spriedumā lietā “Vēbere”; šajā kontekstā *IC* kodeksa 5.2. punkta noteikumi, tos aplūkojot kopā ar 2.4., 2.5., 5.3., 5.4., 5.5. un 5.6. punktu (skat. turpmāk 96. punktu), bija atbilstoši; netika pieprasīts norādīt pieteikumā ordera saņemšanai vai pašā orderī meklēšanas vārdus, jo tas būtu lieki apdraudējis un ierobežojis ordera darbību un jebkurā gadījumā bijis praktiski neiespējami, kā arī nebija nevienas prasības, kas noteiktu, ka šādam orderim ir jābūt apstiprinātam tiesā.

50. Izvērtējot sprieduma lietā “Vēbere” minēto trešo, ceturto, piekto un sesto kritēriju, *IPT* ņēma vērā *RIPA* 15. un 16. pantā, *IC* kodeksā un “zem ūdenslīnijas” esošajos pasākumos paredzētos drošības pasākumus. Tā neuzskatīja par nepieciešamu publicēt visu drošības pasākumu precīzu informāciju vai to ietvert tiesību aktā vai prakses kodeksā. Jo īpaši valsts drošības jomā iespējams ņemt vērā neizpaužamus administratīvus pasākumus, kurus izpildvara pēc būtības varējusi grozīt neatkarīgi no parlamenta, ja izpaustā informācija liecinājusi par rīcības brīvības apmēru un īstenošanas veidu. Gluži kā šajā lietā, tas tā jo īpaši bijis tad, kad *IC* kodekss attiecies uz pasākumiem un bijusi ieviesta kontroles sistēma (proti, *IC* komisārs, pati *IPT* un *ISC*), kas nodrošinājusi, ka šie pasākumi tiek pārskatīti. *IPT* guva pārliecību, ka, spriežot pēc slēgtajā paskaidrojumu uzklausīšanā sniegtās informācijas, nebija izveidota liela sakaru datubāze un bija ieviesti atbilstoši pasākumi attiecībā uz datu saglabāšanas ilgumu un iznīcināšanu. Attiecībā uz “PRISM” jautājumu *IPT* uzskatīja, ka 8. panta 4. punktā paredzētie pasākumi bija pietiekami norādīti tiesību aktā, *IC* kodeksā, *IC* komisāra ziņojumos un tagad arī tās pasludinātajā spriedumā.

51. Attiecībā uz ceturto un pēdējo jautājumu *IPT* nekonstatēja, ka patiesībā pieļauta netieša diskriminācija nacionālās piederības dēļ, kas izriet no dažādajiem režīmiem, kas piemērojami personām, kuras atrodas Britu salās, un personām, kuras atrodas ārpus tām, jo tā uzskatīja, ka jebkura netieša diskriminācija bija pietiekami pamatota, jo ir grūtāk izmeklēt terorisma un noziedzīgus draudus no ārvalstīm. Tā kā ārējo sakaru piekļuves mērķis ir galvenokārt iegūt informāciju par ārvalstīs esošajām personām, atsakoties no iekšējo un ārējo sakaru nošķiršanas, rastos nepieciešamība praktiski jebkurā gadījumā iegūt apliecinājumu saskaņā ar *RIPA* 16. panta 3. punktu (kas īpašā kārtā ļāva piekļūt materiālam par Britu salās esošajām personām, kurš pārtverts saskaņā ar 8. panta 4. punktā minēto orderi, skat. turpmāk 86. punktu), kas radikāli apdraudētu 8. panta 4. punktā paredzētā režīma efektivitāti.

52. Visbeidzot pieteikuma iesniedzēji apgalvoja, ka Konvencijas 10. pantā garantētā aizsardzība uz NVO, kas darbojas izmeklēšanas jomā, attiekusies tāpat kā uz žurnālistiem. “Amnesty International” sākotnēji *IPT* izteica apgalvojumu, ka, visticamāk, nav adekvātu pasākumu attiecībā uz materiālu, ko aizsargā advokāta un klienta saziņas konfidencialitāte un kas bija sūdzība, kura pēc tam tika “novirzīta” izskatīšanai lietā “Belhažs [*Belhadj*]” (skat. turpmāk 99.–101. punktu), kurā “Amnesty International” iestājās kā papildu prasītājs. Līdz 2014. gada 17. novembrim (pēc pirmās un otrās atklātās paskaidrojumu uzklausīšanas) nebija izvirzīts neviens līdzīgs arguments par NVO konfidencialitāti. Tā kā *IPT* uzskatīja, ka šo argumentu varēja izvirzīt jebkurā laikā, tās spriedumā tas bijis izvirzīts “par vēlu”, lai to iekļautu tiesvedībā.

53. Attiecībā uz pārējām saskaņā ar 10. pantu iesniegtajām sūdzībām *IPT* piebilda, ka nav atsevišķu argumentu papildus tam, kas izriet no 8. panta. Lai gan *IPT* ņēma vērā 2010. gada 14. septembra spriedumu lietā Nr. 38224/03 ““Sanoma Uitgevers B.V.” pret Nīderlandi” [*GC*], tā uzsvēra, ka pieteikuma iesniedzēju lieta nav attiekusies uz žurnālistu vai nevalstisko organizāciju mērķētu uzraudzību. Jebkurā gadījumā tā uzskatīja, ka nemērķētas pārraudzības kontekstā, pamatojoties uz 8. panta 4. punktā noteikto orderi, būtu “acīmredzami neiespējami” paredzēt iepriekšēju tiesas atļauju pirms ordera, kas attiecas vienīgi uz to, kas varētu skart 10. pantu. Lai gan *IPT* atzina, ka varētu rasties problēmas, ja satura pārbaudes gaitā rastos daži ar žurnālistikas konfidencialitāti saistīti jautājumi, *IC* kodekss paredz papildu drošības pasākumus saistībā ar šāda materiāla apstrādi.

54. Pēc sprieduma publicēšanas lietas dalībnieki tika aicināti izvirzīt argumentus par to, vai paziņojumu iesniegšanas *IPT* tiesiskais režīms saistībā ar “PRISM” jautājumu atbilda 8. un 10. pantam, kā arī par to sakaru iespējamās pārtveršanas samērīgumu un likumību. *IPT* neuzskatīja par nepieciešamu izvirzīt papildu argumentus par 8. panta 4. punkta samērīgumu kopumā.

C. *IPT* otrais 2015. gada 6. februārī pasludinātais spriedums

55. *IPT* savā otrajā 2015. gada 6. februārī pasludinātajā spriedumā izvērtēja, vai pirms tās 2014. gada decembra sprieduma pasludināšanas ar “PRISM” vai “Upstream” pasākumiem ir pārkāpts Konvencijas 8. un/vai 10. pants.

56. Tā piekrita, ka, tikai atsaucoties uz 9. oktobra paziņojumu ar attiecīgajiem grozījumiem (skat. iepriekš 33. un 36. punktu), tā guvusi pārliecību, ka režīms bijis “atbilstošs likumam”. *IPT* ieskatā, ja nebūtu iesniegti attiecīgie paziņojumi, nebūtu sniegti atbilstoši norādījumi, kā to nosaka 8. un 10. pants. Tādēļ tā paziņoja, ka pirms paziņojumu iesniegšanas:

“23. (..) [R]ežīms, kas reglamentē kārtību, kādā Apvienotās Karalistes iestādes pieprasa, saņem, uzglabā un pārraida Apvienotajā Karalistē esošu personu privātos sakarus, ko ASV iestādes ieguvušas, izmantojot “Prism” un/vai .. “Upstream”, bija pretrunā ar *ECHR* 8. un 10. pantu, taču tagad tas šiem pantiem atbilst.”

D. *IPT* trešais 2015. gada 22. jūnijā pasludinātais spriedums, kas grozīts ar tās 2015. gada 1. jūlija vēstuli

57. Trešajā *IPT* spriedumā, kas publicēts 2015. gada 22. jūnijā, *IPT* izvērtēja, vai Apvienotās Karalistes iestādes pieteikuma iesniedzēju saziņu saturu, kas iegūts, izmantojot “PRISM” vai “Upstream”, bija pieprasījušas, saņēmušas, uzglabājušas vai pārsūtījušas, pārkāpjot Konvencijas 8. un/vai 10. pantu, un vai Apvienotās Karalistes iestādes bija pārtvērušas, aplūkojušas, uzglabājušas vai pārsūtījušas pieteikuma iesniedzēju saziņu saturu tādā apmērā, kas uzskatāms par pretlikumīgu rīcību vai 8. un/vai 10. panta pārkāpumu.

58. *IPT* nepieņēma lēmumu par labu astoņiem no desmit pieteikuma iesniedzējiem. Atbilstoši tās ierastajai praksei, kad tā nespriež par labu prasītājam, tā neapstiprināja, ka pieteikuma iesniedzēju saziņu saturs ticis pārtverts. Tomēr *IPT* pieņēma lēmumus saistībā ar diviem pieteikuma iesniedzējiem. Vienas organizācijas nosaukums spriedumā bija norādīts kļūdaini, taču *IPT* šo kļūdu laboja ar 2015. gada 1. jūlija vēstuli.

59. Attiecībā uz “Amnesty International” *IPT* konstatēja, ka e-pasta saziņu satura pārtveršana un piekļuve tam bijusi likumīga un samērīga un notikusi saskaņā ar *RIPA* 8. panta 4. punktu, taču nebija ticis ņemts vērā *GCHQ* iekšējās politikas nostādnēs noteiktais pieļaujamais saglabāšanas periods, tādēļ materiāls ticis saglabāts ilgāk par pieļaujamo saglabāšanas periodu. Taču *IPT* guva pārliecību, ka piekļuve materiālam nebija notikusi pēc attiecīgā saglabāšanas perioda beigām un ka pārkāpums kvalificējams kā tehnisks pārkāpums. Tomēr tas bija uzskatāms par 8. panta pārkāpumu, tādēļ *GCHQ* bija uzdots iznīcināt visu saziņu saturu, ko tā saglabājusi ilgāk par attiecīgo periodu, un septiņu dienu laikā iesniegt dokumentu drukātās versijas *IC* komisāram to saglabāšanai uz pieciem gadiem, ja turpmākās tiesvedības gaitā rastos nepieciešamība tās izmantot. Tāpat *GCHQ* bija uzdots četrpadsmit dienu laikā iesniegt konfidenciālu ziņojumu, kurā apstiprināta dokumentu iznīcināšana. Par to netika piešķirta nekāda kompensācija.

60. Attiecībā uz “Legal Resources Centre” *IPT* konstatēja, ka saziņu saturs no e-pasta adreses, kas saistīts ar pieteikuma iesniedzēju, bija pārtverts un atlasīts pārbaudei saskaņā ar 8. panta 4. punktā noteikto orderi. Lai gan tā guva pārliecību, ka pārtveršana bija likumīga un samērīga un ka saziņu satura atlase pārbaudei bija samērīga, *IPT* konstatēja, ka nebija ievērota iekšējā atlases procedūra. Līdz ar to noticis 8. pantā garantēto “Legal Resources Centre” tiesību pārkāpums. Tomēr *IPT* guva pārliecību, ka materiāls netika izmantots un ka netika saglabāti nekādi ieraksti, tādēļ pieteikuma iesniedzējam nebija radīts materiāls kaitējums, zaudējumi vai negatīva ietekme. Tādējādi tās lēmums bija taisnīgs, un netika piešķirta nekāda kompensācija.

1. PIEMĒROJAMAIS TIESISKAIS REGULĒJUMS UN PRAKSE

I. PIEMĒROJAMIE VALSTS TIESĪBU AKTI

A. Sakaru pārtveršana

1. Orderi. Vispārīga informācija

61. 2000. gada *RIPA* 1. panta 1. punkts (ko tagad aizstājis 2016. gada Izmeklēšanas pilnvaru likums [*Investigatory Powers Act 2016*]) noteica, ka publiska pasta pakalpojuma vai publiskas telekomunikāciju sistēmas ceļā pārraidītu sakaru pārtveršana ir pretlikumīga, ja vien tā nav notikusi saskaņā ar 5. pantā noteikto orderi (turpmāk tekstā – “pārtveršanas orderis”).

62. Saskaņā ar 5. panta 2. punktu valsts sekretārs(-e) varēja atļaut izdot pārtveršanas orderi, ja tas viņa vai viņas ieskatā bija nepieciešams 5. panta 3. punktā minēto iemeslu dēļ, proti, valsts drošības interesēs, smagu noziegumu novēršanai vai atklāšanai vai arī Apvienotās Karalistes ekonomiskās labklājības aizsardzībai (ciktāl šīs intereses sasaucas ar valsts drošības interesēm, skat. *IC* kodeksa 3.5. un 6.11. punktu turpmāk 96. punktā), un ja ar orderi atļautā rīcība bija samērīga ar šīs rīcības mērķi. Izvērtējot nepieciešamību un samērīgumu, bija jāņem vērā, vai uz ordera pamata iegūstamo informāciju pamatoti varēja iegūt ar citiem līdzekļiem.

63. *RIPA* 81. panta 2. punkta b) apakšpunktā jēdziens “smags noziegums” bija definēts kā noziegums, kas atbilst vienam no šiem kritērijiem:

“a) nodarījums vai viens no nodarījumiem, kas ir vai būtu izdarīts ar attiecīgo rīcību, ir nodarījums, par kuru personai, kas sasniegusi divdesmit viena gada vecumu un kam nav iepriekšējas sodāmības, pamatoti varētu piespriest brīvības atņemšanu uz trim gadiem vai ilgāk;

b) rīcība izpaužas kā vardarbība, kā rezultātā tiek gūts būtisks finansiāls labums, vai arī rīcība ir attiecināma uz lielu skaitu personu, kas rīkojušās kopēja mērķa sasniegšanai.”

64. 81. panta 5. punktā bija noteikts:

“Šā likuma izpratnē nozieguma atklāšana ietver:

a) nozieguma izdarītāja, mērķa, nozieguma izdarīšanas līdzekļu un apstākļu noskaidrošanu kopumā un

b) tās personas aizturēšanu, kura izdarījusi noziegumu,

un attiecīgi ir jāinterpretē visas norādes uz nozieguma novēršanu vai atklāšanu šajā likumā (..).”

65. 6. pantā bija noteikts, ka attiecībā uz izlūkdienestiem pārtveršanas orderi varēja pieprasīt vienīgi *MI5* ģenerāldirektors, *MI6* vadītājs un *GCHQ* direktors.

66. Tas arī paredzēja divu veidu pārtveršanas orderus, uz kuriem attiecās 5. un 6. pants, proti, specifisku orderi, kā noteikts 8. panta 1. punktā, un nespecifisku orderi, kā noteikts 8. panta 4. punktā.

67. Saskaņā ar *RIPA* 9. pantu orderis, kas izdots valsts drošības interesēs vai Apvienotās Karalistes ekonomiskās labklājības aizsardzībai, zaudēja spēku pēc sešu mēnešu apritēšanas, savukārt orderis, kas izdots smaga nozieguma atklāšanai, zaudēja spēku pēc trīs mēnešu apritēšanas. Jebkurā brīdī pirms minēto periodu beigām valsts sekretārs(-e) varēja atjaunot orderi (attiecīgi uz sešiem un trim mēnešiem), ja viņa vai viņas ieskatā orderis joprojām nepieciešams 5. panta 3. punktā minēto iemeslu dēļ. Valsts sekretāram(-ei) bija jāatceļ pārtveršanas orderis, ja viņš vai viņa bija guvis(-usi) pārliecību, ka orderis 5. panta 3. punktā minēto iemeslu dēļ vairs nav nepieciešams.

68. Saskaņā ar 5. panta 6. punktu ar orderi atļautā rīcība ietvēra tādu sakaru pārtveršanu, kas orderī nav norādīti, ja nepieciešams veikt to, kas orderī skaidri atļauts vai noteikts, kā arī saistīto sakaru datu iegūšanu.

69. 21. panta 4. punktā jēdziens “sakaru dati” bija definēts kā:

“a) jebkuri datplūsmas dati, kas iekļauti kādā saziņu saturā vai tam pievienoti (neatkarīgi no tā, vai tos ietvēris vai pievienojis sūtītājs vai kāda cita persona) jebkura tāda pasta pakalpojuma vai tādas telekomunikāciju sistēmas nolūkiem, ar kuru starpniecību dati tiek vai varētu tikt pārraidīti;

b) jebkura informācija, kas neietver nekādu saziņas saturu (izņemot informāciju, uz kuru neattiecas a) apakšpunkts) un kas raksturo veidu, kādā persona izmanto:

i) jebkuru pasta vai telekomunikāciju pakalpojumu vai

ii) jebkuru telekomunikāciju sistēmas daļu saistībā ar jebkura telekomunikāciju pakalpojuma sniegšanu kādai personai vai tā izmantošanu;

c) jebkura informācija, uz kuru neattiecas a) vai b) apakšpunkts un ko persona, kura sniedz pasta vai telekomunikāciju pakalpojumu, saglabā vai iegūst saistībā ar personām, kurām tā sniedz šo pakalpojumu.”

70. 2015. gada marta Sakaru datu iegūšanas un izpaušanas prakses kodeksā [*The March 2015 Acquisition and Disclosure of Communications Data Code of Practice*] šīs trīs kategorijas ir norādītas kā “datplūsmas dati”, “informācija par pakalpojuma izmantošanu” un “informācija par abonentu”. *RIPA* 21. panta 6. punktā jēdziens “datplūsmas dati” ir definēts kā dati, ar kuriem identificē personu, iekārtu, vietu vai adresi, uz kuru vai no kuras saziņas saturs pārraidīts, kā arī informācija par datora datni vai programmu, kam piekļūts vai kas palaista saziņas satura nosūtīšanas vai saņemšanas gaitā.

71. Saskaņā ar *RIPA* 20. pantu “saistītie sakaru dati” attiecībā uz sakariem, kas pārtverti, tos pārraidot ar pasta pakalpojuma vai telekomunikāciju sistēmas starpniecību, nozīmē “tik lielu sakaru datu apjomu, kas iegūts pārtveršanas gaitā vai saistībā ar pārtveršanu”, un tie ir saistīti “ar attiecīgo saziņu saturu vai tā sūtītāju vai saņēmēju, vai arī paredzamo saņēmēju.”

2. Orderi. 8. panta 4. punkts

a) Atļauja

72. Saziņu satura “masveida pārtveršana” notika saskaņā ar 8. panta 4. punktā noteikto orderi. Saskaņā ar *RIPA* 8. panta 4. un 5. punktu valsts sekretārs varēja izdot orderi, lai “pārtvertu ārējos sakarus brīdī, kad tie tiek pārraidīti ar telekomunikāciju sistēmas starpniecību”.

73. 8. panta 4. punktā noteiktā ordera izdošanas brīdī valsts sekretāram(-ei) bija jāizdod arī apliecinājums, kurā raksturots pārtvertais materiāls, ko viņš vai viņa uzskata par nepieciešamu pārbaudīt, un norādīts, ka, viņaprāt vai viņasprāt, materiāla pārbaude ir nepieciešama 5. panta 3. punktā minēto iemeslu dēļ (proti, valsts interesēs, smaga nozieguma novēršanai vai atklāšanai vai arī Apvienotās Karalistes ekonomiskās labklājības aizsardzībai, ciktāl šīs intereses atbilst valsts drošības interesēm; skat. *IC* kodeksa 3.5. un 6.11. punktu turpmāk 96. punktā).

b) “Ārējie” sakari

74. 20. pantā jēdziens “ārējie sakari” definēts kā “ārpus Britu salām nosūtīts vai saņemts saziņu saturs”.

75. “Liberty” tiesvedībā Drošības un terorisma apkarošanas biroja (turpmāk tekstā – “*OSCT*”) ģenerāldirektors Čārlzs Farrs norādīja, ka e-pasta sarakste starp divām Apvienotajā Karalistē esošām personām uzskatāma par “iekšējiem sakariem”, pat ja e-pasta pakalpojums darbojas uz servera Amerikas Savienotajās Valstīs, tomēr šo saziņu saturu var pārtvert kā ārējo sakaru pārtveršanas ordera “līdzproduktu”. Taču tad, kad Apvienotajā Karalistē esoša persona “sazinās” ar ārvalstīs esošu meklētājprogrammu, runa ir par ārējiem sakariem, gluži kā Apvienotajā Karalistē esoša persona, kura publicē publisku ziņojumu (piemēram, kā “Twitter” sīkziņu vai “Facebook” statusa atjauninājumu), ja vien visi šā ziņojuma saņēmēji neatrodas Britu salās.

76. Sniedzot liecību *ISC* 2014. gada oktobrī, valsts sekretārs ārlietās un sadraudzības lietās uzskatīja, ka:

“Attiecībā uz e-pasta ziņojumu, ja sūtītājs vai saņēmējs vai abi atrodas ārvalstīs, runa būtu par ārējiem sakariem.

Attiecībā uz interneta pārlūkošanu, ja persona lasa rakstu “Washington Post” tīmekļa vietnē, tas nozīmē, ka tā ir “sazinājusies” ar ārvalstīs esošu tīmekļa serveri, tādēļ runa ir par ārējiem sakariem.

Attiecībā uz sociālajiem tīkliem, ja persona kaut ko publicē “Facebook”, runa būtu par ārējiem sakariem, jo tīmekļa serveris atrodas ārvalstīs.

Attiecībā uz informācijas saglabāšanu mākoņkrātuvē (piemēram, “Dropbox” augšupielādētām datnēm) runa būtu par ārējiem sakariem, jo šī informācija ir nosūtīta uz ārvalstīs esošu tīmekļa serveri.”

3. RIPA paredzētie specifiskie drošības pasākumi

a) 15. pants

77. Saskaņā ar 15. panta 1. punktu valsts sekretāram(-ei) saistībā ar pārtveršanas orderiem bija pienākums nodrošināt, ka spēkā ir tādi pasākumi, kādus viņš vai viņa uzskatījis par nepieciešamiem 2. un 3. punktā noteikto prasību izpildei saistībā ar pārtverto materiālu un jebkuriem saistītajiem sakaru datiem, un ka attiecībā uz orderiem, saistībā ar kuriem izdoti 8. panta 4. punktā noteiktie apliecinājumi, ir izpildītas arī 16. pantā noteiktās prasības.

78. 15. panta 2. punkts noteica:

“Šajā punktā noteiktās prasības saistībā ar pārtverto materiālu un jebkuriem saistītajiem sakaru datiem uzskatāmas par izpildītām, ja:

a) to personu skaits, kurām jebkurš materiāls vai dati tiek izpausti vai kā citādi padarīti pieejami;

b) apmērs, kādā jebkurš materiāls vai dati tiek izpausti vai kā citādi padarīti pieejami;

c) apmērs, kādā jebkurš materiāls vai dati tiek kopēti, un

d) izgatavoto kopiju skaits

tiek ierobežoti līdz minimumam, kas nepieciešams atļautajiem nolūkiem.”

79. 15. panta 3. punkts noteica:

“Šajā punktā noteiktās prasības saistībā ar pārtverto materiālu un jebkuriem saistītajiem sakaru datiem uzskatāmas par izpildītām, ja katra izgatavotā materiāla vai datu kopija (ja tā nav iznīcināta agrāk) tiek iznīcināta, tiklīdz vairs nav pamata to saglabāt kā tādu, kas nepieciešama kādam no atļautajiem nolūkiem.”

80. Saskaņā ar 15. panta 4. punktu kaut kas ir nepieciešams atļautajiem nolūkiem vienīgi tad, ja tas joprojām ir vai, visticamāk, kļūs nepieciešams, kā norādīts likuma 5. panta 3. punktā (proti, valsts drošības interesēs, smaga nozieguma novēršanai vai atklāšanai vai arī Apvienotās Karalistes ekonomiskās labklājības aizsardzībai (ciktāl šīs intereses atbilst valsts drošības interesēm; skat. *IC* kodeksa 3.5. un 6.11. punktu turpmāk 96. punktā), vai lai īstenotu jebkura starptautiskā savstarpējā palīdzības līguma noteikumus); vai tas ir nepieciešams, lai sekmētu jebkuras valsts sekretāra pārtveršanas funkcijas izpildi; tas ir nepieciešams, lai sekmētu jebkuras *IC* komisāra vai *IPT* funkcijas izpildi; tas ir nepieciešams, lai nodrošinātu, ka persona, kas veic kriminālvajāšanu, ir informēta par to, ko tās amata pienākums paredz, lai kriminālvajāšanā nodrošinātu godīgumu, vai arī tas ir nepieciešams, lai izpildītu jebkuru amata pienākumu, ko personai nosaka publisko reģistru tiesiskais regulējums.

81. 15. panta 5. punkts paredzēja, ka pasākumiem, kas ieviesti, lai nodrošinātu atbilstību 15. panta 2. punktam, jāietver tādi pasākumi, kurus valsts sekretārs uzskata par nepieciešamiem, lai nodrošinātu, ka jebkura izgatavotā materiāla vai datu kopija visu tās saglabāšanas laiku tiktu uzglabāta droši.

82. Saskaņā ar 15. panta 6. punktu 15. panta 1. punktā minētie pasākumi nebija nepieciešami, lai nodrošinātu 15. panta 2. un 3. punktā noteikto prasību izpildi, ciktāl tās attiecās uz jebkuru pārtverto materiālu vai saistītajiem sakaru datiem, vai arī jebkuru šā materiāla vai datu kopiju, kas nodotas jebkuras ārpus Apvienotās Karalistes esošas valsts vai teritorijas iestādes īpašumā. Tomēr šādi pasākumi bija nepieciešami, lai jebkura šāda ordera gadījumā nodrošinātu, ka pārtvertais materiāls un dati, kā arī materiāla vai datu kopijas tiek nodotas ārpus Apvienotās Karalistes esošas valsts vai teritorijas iestādes īpašumā vienīgi tad, ja ir izpildītas 15. panta 7. punktā noteiktās prasības. 15. panta 7. punkts noteica:

“Ordera gadījumā šajā punktā noteiktās prasības uzskatāmas par izpildītām, ja valsts sekretārs uzskata, ka:

a) prasības, kas atbilst 2. un 3. punktā minētajām prasībām, tiks piemērotas tādā apmērā, kādā valsts sekretārs to uzskata par vajadzīgu (ja tās tiks piemērotas) saistībā ar jebkuru pārtverto materiālu vai saistītajiem sakaru datiem, kuri nodoti vai kuru kopijas nodotas attiecīgo iestāžu īpašumā, un

b) ir spēkā ierobežojumi, kas liegtu tādā apmērā, kādā valsts sekretārs to uzskata par vajadzīgu (ja tas tiktu liegts), rīkoties Apvienotās Karalistes jebkuras tiesvedības ietvaros, tās nolūkiem vai saistībā ar to, kā rezultātā tiktu izpausta informācija, ko saskaņā ar 17. pantu Apvienotajā Karalistē nevarēja izpaust.”

83. *RIPA* 17. pantā bija noteikts, ka saistībā ar tiesvedību parasti nevar sniegt pierādījumus, izpaust informāciju vai veikt citus pasākumus, ar kuriem tiktu izpausts pārtverto sakaru saturs vai saistītie sakaru dati.

b) 16. pants

84. 16. pantā ir izklāstīti papildu drošības pasākumi saistībā ar “ārējo” sakaru pārtveršanu saskaņā ar 8. panta 4. punktā noteikto orderi. 16. panta 1. punkts noteica, ka pārtverto materiālu var lasīt, aplūkot vai klausīties vienīgi personas, kurām tas kļūst pieejams saskaņā ar orderi, ja un ciktāl tas tika apstiprināts kā materiāls, ko nepieciešams pārbaudīt, kā noteikts likuma 5. panta 3. punktā, un ja uz to attiecas 16. panta 2. punkts. 20. pantā jēdziens “pārtvertais materiāls” bija definēts kā jebkuru tādu sakaru saturs, kas pārtverts, veicot pārtveršanu, uz ko attiecas orderis.

85. 16. panta 2. punkts noteica:

“Saskaņā ar 3. un 4. punktu šis punkts attiecas uz pārtverto materiālu vienīgi tiktāl, ciktāl tas atlasīts, lai to lasītu, aplūkotu vai klausītos kā citādi, nevis atbilstoši faktoram:

a) kas attiecināms uz personu, par kuru zināms, ka tā attiecīgajā brīdī atrodas Britu salās, un

b) kura nolūks vai viens no nolūkiem ir identificēt materiālu, kas iekļauts tai nosūtītajos vai paredzētajos sakaros.”

86. Saskaņā ar 16. panta 3. punktu uz pārtverto materiālu attiecās 16. panta 2. punkts neatkarīgi no tā, ka tas tika atlasīts, atsaucoties uz kādu no šajā punktā minētajiem apstākļiem, ja valsts sekretārs saskaņā ar 8. panta 4. punktu bija apliecinājis, ka bija nepieciešams pārbaudīt materiālu, kas atlasīts atbilstoši apstākļiem, kas attiecināmi uz attiecīgo personu, kā noteikts likuma 5. panta 3. punktā, un ka materiāls attiecās vienīgi uz saziņu saturu, kurš nosūtīts apliecinājumā norādītajā periodā, kas nepārsniedz maksimālo pieļaujamo periodu.

87. 16. panta 3.A punktā noteikts šāds “pieļaujamais maksimālais periods”:

“a) seši mēneši attiecībā uz materiālu, kura pārbaude ir apliecināta saskaņā ar 8. panta 4. punktu, ja tas nepieciešams valsts drošības interesēs, un

b) trīs mēneši pārējos gadījumos.”

88. Saskaņā ar 16. panta 4. punktu uz pārtverto materiālu attiecās arī 16. panta 2. punkts, pat ja tas tika atlasīts, atsaucoties uz kādu no šajā punktā minētajiem faktoriem, ja persona, kurai bija adresēts attiecīgais orderis, pamatoti uzskatīja, ka attiecīgajos apstākļos šis punkts attiektos uz materiālu, vai arī saistībā ar materiāla atlasi bija izpildīti 16. panta 5. punktā minētie nosacījumi.

89. 16. panta 5. punkts noteica:

“Nosacījumi saistībā ar pārtvertā materiāla atlasīšanu uzskatāmi par izpildītiem, ja:

a) personai, kurai adresēts attiecīgais orderis, uzskata, ka ir notikušas tik būtiskas attiecīgās apstākļu izmaiņas, ka šo izmaiņu dēļ, izņemot 4. punkta b) apakšpunktu, uz pārtverto materiālu neattiektos 2. punkts;

b) kopš tā saņemšanas vadošā amatpersona ir devusi rakstveida atļauju lasīt, aplūkot vai klausīties materiālu un

c) atlasīšana notikusi pirms pieļaujamā perioda beigām.”

90. Saskaņā ar 16. panta 5.A punktu “pieļaujamais periods” bija:

“a) attiecībā uz materiālu, kura pārbaude apliecināta saskaņā ar 8. panta 4. punktu, periods, kas beidzas piektās darba dienas beigās pēc dienas, kurā to saskaņā ar 5. punkta a) apakšpunktu sākotnēji saņēmusi persona, kurai adresēts orderis, un

b) jebkurā citā gadījumā – periods, kas beidzas pirmās darba dienas beigās pēc dienas, kurā šī persona to materiālu sākotnēji saņēmusi.”

91. Saskaņā ar 16. panta 6. punktu “attiecīgās apstākļu izmaiņas” nozīmēja, ka vai nu attiecīgā persona bija ieceļojusi Britu salās, vai arī personas, kurai adresēts orderis, pārliecība par attiecīgās personas atrašanos ārpus Britu salām patiesībā bijusi maldīga.

92. Sniedzot liecību *ISC* 2014. gada oktobrī, valsts sekretārs ārlietās un Sadraudzības lietās paskaidroja:

“Kad analītiķis atlasa sakarus, kas pārbaudes nolūkos pārtverti atbilstoši 8. panta 4. punktā noteiktajam orderim, nav nozīmes tam, kāda veida sakarus persona izmanto un vai tās pārējie sakari tiek uzglabāti tam paredzētā pasta serverī vai mākoņkrātuvē, kas faktiski atrodas Apvienotajā Karalistē, ASV vai kur citur (un individuāls mākoņpakalpojumu lietotājs patiesībā nezinās, kur tie ir uzglabāti). Ja par viņu ir zināms, ka viņš vai viņa atrodas Britu salās, nav atļauts meklēt viņa vai viņas sakarus, izmantojot viņa vai viņas vārdu, e-pasta adresi vai kādu citu personas identifikatoru.”

4. Sakaru pārtveršanas prakses kodekss

93. *RIPA* 71. pants paredzēja, ka valsts sekretāram(-ei) ir jāpieņem prakses kodeksi saistībā ar viņa vai viņas pilnvaru īstenošanu un amata pienākumu izpildi šā likuma ietvaros. Prakses kodu projekti bija jāiesniedz izskatīšanai parlamentam, turklāt tie bija publiski dokumenti. Tie varēja stāties spēkā vienīgi saskaņā ar valsts sekretāra rīkojumu. Valsts sekretārs varēja izdot šādu rīkojumu vienīgi tad, ja šā rīkojuma projekts bija iesniegts izskatīšanai parlamentam un tas bija apstiprināts ar katras palātas lēmumu.

94. Saskaņā ar *RIPA* 72. panta 1. punktu personai, kura īsteno jebkādas pilnvaras vai pilda amata pienākumus saistībā ar sakaru pārtveršanu, bija jāievēro attiecīgie prakses kodeksa noteikumi. Saskaņā ar *RIPA* 72. panta 4. punktu prakses kodeksa noteikumus attiecīgajos apstākļos varēja ņemt vērā arī tiesas un tribunāli.

95. *IC* kodekss tika izdots saskaņā ar *RIPA* 71. pantu. Attiecīgajā brīdī spēkā esošais *IC* kodekss tika izdots 2016. gadā.

96. Ciktāl tas attiecināms uz šo tiesvedību, *IC* kodeksā bija noteikts:

“3.2. Ir noteikts ierobežots skaits to personu, kuras vai kuru vārdā var pieprasīt pārtveršanas orderi. Tās ir:

* Drošības dienesta ģenerāldirektors;
* Slepenās izlūkošanas dienesta vadītājs;
* Valdības komunikāciju galvenās pārvaldes (*GCHQ*) direktors;
* Valsts noziedzības apkarošanas aģentūras (turpmāk tekstā – “*NCA*”) ģenerāldirektors (*NCA* veic pārtveršanu tiesībsargājošo iestāžu vārdā Anglijā un Velsā);
* Skotijas policijas vecākais virsnieks;
* Metropoles policijas komisārs (Metropoles policijas Terorisma apkarošanas komanda veic pārtveršanu Terorisma apkarošanas vienību, Speciālo nodaļu un dažu policijas spēku speciālo vienību vārdā Anglijā un Velsā);
* Ziemeļīrijas policijas vecākais virsnieks;
* Apvienotās Karalistes Ieņēmumu un muitas dienesta (turpmāk tekstā – “*HMRC*”) komisāri;
* Aizsardzības izlūkošanas dienesta vadītājs;
* [juridiska] persona, kura saskaņā ar jebkuru starptautisko savstarpējās tiesiskās palīdzības līgumu ir kādas ārpus Apvienotās Karalistes esošas valsts vai teritorijas kompetentā iestāde.

3.3. Jebkuru pieteikumu kādas iepriekšminētās personas vārdā iesniedz persona, kura ieņem amatu Apvienotās Karalistes valdībā.

3.4. Visus pārtveršanas orderus izdod valsts sekretārs. Pat steidzamības kārtā valsts sekretārs personīgi apstiprina orderi, lai arī to paraksta vecākā amatpersona.

**Nepieciešamība un samērīgums**

3.5. Saņemot orderi saskaņā ar *RIPA*, vienīgi tiks nodrošināts, ka atļautā pārtveršana ir pamatota iejaukšanās personas tiesībās saskaņā ar Eiropas Cilvēktiesību konvencijas (turpmāk tekstā – “*ECHR*”) 8. pantu (tiesībās uz privātās un ģimenes dzīves neaizskaramību), ja šāda rīcība ir nepieciešama un samērīga pārtveršanai. *RIPA* to atzīst, vispirms uzliekot valsts sekretāram par pienākumu pārliecināties, ka atļauja ir nepieciešama viena vai vairāku likumā noteikto iemeslu dēļ:

* valsts drošības intereses;
* smaga nozieguma novēršana vai atklāšana;
* Apvienotās Karalistes ekonomiskās labklājības aizsardzība, ciktāl šīs intereses sasaucas ar valsts drošības interesēm.

3.6. Šie mērķi ir izklāstīti *RIPA* 5. panta 3. punktā. Valsts sekretāram arī jāpārliecinās, ka pārtveršana ir samērīga ar šīs rīcības mērķi. Jebkurš samērīguma izvērtējums ietver līdzsvarošanu starp to, cik nopietna ir iejaukšanās operācijas subjekta (vai jebkuras citas personas, kura var tikt ietekmēta) tiesībās uz privātumu un īpašumu un cik lielā mērā šī rīcība ir nepieciešama izmeklēšanas, operatīvajā vai spējas ziņā. Orderis nebūs samērīgs, ja tas ir pārmērīgs visu lietas apstākļu kontekstā. Katrai atļautajai rīcībai jāsniedz paredzamais ieguvums izmeklēšanā vai operācijā, un tā nevar būt nesamērīga vai patvaļīga. Tikai tas vien, ka (piemēram) var tikt apdraudēta valsts drošība, nav pamats tam, lai uzskatītu visaizskarošāko rīcību par samērīgu. Iejaukšanos nevar uzskatīt par samērīgu, ja nepieciešamo informāciju iespējams iegūt ar mazāk aizskarošu līdzekļu palīdzību.

3. GALVENIE NOTEIKUMI PAR PĀRTVERŠANU ATBILSTOŠI ORDERIM

(..)

3.7. Līdz ar to jāņem vērā šādi samērīguma apstākļi:

* līdzsvars starp ierosinātās iejaukšanās apmēru, darbības jomu un sasniedzamo mērķi;
* paskaidrojums par to, kā un kāpēc pieņemtās metodes radīs vismazāko iejaukšanos subjekta un citu personu tiesībās;
* izvērtējums par to, vai attiecīgā darbība paredz atbilstošu tiesību aktu izmantošanu un saprātīgu nepieciešamā rezultāta iegūšanas veidu, ņemot vērā visas saprātīgās alternatīvas;
* pierādījumi, ciktāl tas praktiski iespējams, par citām apsvērtajām metodēm, kas tika vai netika izmantotas, taču tika atzītas par nepietiekamām, lai sasniegtu darbības mērķus, nepievienojot nepieciešamo pārtverto materiālu.

(..)

**Pārtveršanas orderu spēkā esības ilgums**

3.18. Pārtveršanas orderi, ko izdod saistībā ar smagiem noziegumiem, sākotnēji ir spēkā trīs mēnešus. Savukārt pārtveršanas orderi, ko izdod saistībā ar Apvienotās Karalistes valsts drošību / ekonomisko labklājību, sākotnēji ir spēkā sešus mēnešus. Steidzamības kārtā (jebkāda iemesla dēļ) izdoti orderi ir spēkā piecas darbdienas, sākot no to izdošanas dienas, ja vien valsts sekretārs tos neatjauno.

3.19. Pēc atjaunošanas pārtveršanas orderi, ko izdod saistībā ar smagiem noziegumiem, ir spēkā vēl trīs mēnešus. Savukārt atjaunotie pārtveršanas orderi, ko izdod saistībā ar Apvienotās Karalistes valsts drošību / ekonomisko labklājību, ir spēkā vēl sešus mēnešus. Šo laika periodu skaita no dokumenta atjaunošanas dienas.

3.20. Ja pārtveršanas orderī veiktas izmaiņas, ordera derīguma termiņš nemainās. Tomēr, ja šādas izmaiņas veiktas steidzamības kārtā, šā dokumenta termiņš beidzas pēc piecām darbdienām pēc tā izdošanas datuma, ja vien tas netiek atjaunots ierastajā kārtībā.

3.21. Ja apstākļu maiņas dēļ pārtveršanas aģentūra uzskata, ka ordera spēkā esība vairs nav nepieciešama, samērīga vai praktiski iespējama, aģentūrai ir jāiesniedz valsts sekretāram ieteikums par šā ordera tūlītēju atcelšanu.

(..)

4. ĪPAŠI NOTEIKUMI PAR PĀRTVERŠANU ATBILSTOŠI ORDERIM

**Netieša iejaukšanās**

4.1. Jāizvērtē jebkura iejaukšanās tādu personu tiesībās uz privātās dzīves neaizskaramību, uz kurām paredzētā pārtveršana neattiecas, jo īpaši tad, ja tā varētu skart ar reliģiju, medicīnu, žurnālistiku vai advokāta un klienta saziņas konfidencialitāti saistītu materiālu vai sakarus starp kādu parlamenta locekli un kādu citu personu saistībā ar vēlēšanu apgabalu, vai arī sakarus starp kādu parlamenta locekli un trauksmes cēlēju. Pieteikumā pārtveršanas ordera saņemšanai jānorāda, vai pārtveršanas gaitā zināmā mērā notiktu netieša iejaukšanās personas tiesībās uz privātās dzīves neaizskaramību. Personai, kura pieprasa pārtveršanas orderi, arī vajadzētu apsvērt pasākumus, tostarp automātisku sistēmu izmantošanu, lai novērstu netiešās iejaukšanās apmēru. Ja tas iespējams, šie pasākumi jānorāda pieteikumā. Valsts sekretārs šos apstākļus un pasākumus ņems vērā, izvērtējot pieteikumu ordera saņemšanai saskaņā ar *RIPA* 8. panta 1. punktu. Ja pārtveršanas operācijas gaitā personas, uz kurām atļauja neattiecas, pašas tiek identificētas kā izmeklēšanas mērķis, ir jāapsver atsevišķu orderu izdošana attiecībā uz šīm personām.

**Konfidenciāla informācija**

4.2. Īpaši jāizvērtē arī gadījumi, kad personām, uz kurām pārtveršana neattiecas, var būt raksturīgs augsts privātuma aizsardzības līmenis vai var tikt skarta konfidenciāla informācija. Tostarp tas ir tad, ja sakari ir saistīti ar materiālu, uz ko attiecas advokāta un klienta saziņas konfidencialitāte, ja tiek skarts konfidenciāls žurnālistikas materiāls, ja pārtveršana var ietvert sakarus starp kādu medicīnas speciālistu vai garīdznieku un personu saistībā ar šīs personas veselību vai garīgo labsajūtu vai arī sakarus starp kādu parlamenta locekli un kādu citu personu saistībā ar vēlēšanu apgabalu.

4.3. Konfidenciāls žurnālistikas materiāls ietver materiālu, kas iegūts vai izveidots žurnālistikas nolūkiem un ko kāda persona apņēmusies paturēt noslēpumā, kā arī saziņu saturu, kas izriet no informācijas, kas iegūta žurnālistikas nolūkiem un atrodas kādas personas rīcībā saskaņā ar šādu apņemšanos. Skat. arī 4.26. punktu un 4.28.–4.31. punktu, lai iegūtu vairāk informācijas par drošības pasākumiem, kas piemērojami saistībā ar konfidenciālu žurnālistikas materiālu.

(..)

**Saziņu saturs, kas ietver konfidenciālu žurnālistikas materiālu vai konfidenciālu personīgu informāciju, un saziņu saturs starp kādu parlamenta locekli un kādu citu personu saistībā ar vēlēšanu apgabalu**

4.26. Attiecībā uz pārtveršanu īpaša uzmanība ir jāpievērš arī saziņu saturam, kas ietver konfidenciālu žurnālistikas materiālu vai konfidenciālu personīgu informāciju, vai saziņu saturam starp kādu parlamenta locekli un kādu citu personu saistībā ar vēlēšanu apgabalu. Skaidrojums par konfidenciālu žurnālistikas materiālu sniegts 4.3. punktā. Konfidenciāla personīga informācija ir informācija, ko kāda persona apņēmusies paturēt noslēpumā saistībā ar kādu citu personu (dzīvu vai mirušu), kuru ar šo informāciju iespējams identificēt, kā arī materiāls, kas attiecas uz šīs personas fizisko un garīgo veselību vai reliģisko orientēšanu. Šāda informācija var ietvert gan mutvārdu, gan rakstveida sakarus. Šāda iepriekšminētā informācija tiek paturēta noslēpumā, ja kāda persona tieši vai netieši ir apņēmusies to paturēt noslēpumā vai uz to attiecas izpaušanas ierobežojums vai pienākums ievērot konfidencialitāti, kas noteikts spēkā esošajā tiesiskajā regulējumā. Piemēram, konfidenciāla personīga informācija var ietvert konsultācijas starp veselības aprūpes speciālistu un pacientu vai informāciju no pacienta slimības vēstures.

(..)

4.28. Ja paredzēts iegūt konfidenciālu personīgu informāciju, ir skaidri jādokumentē šādi iemesli un rūpīgi jāapsver šādas rīcības nepieciešamība un samērīgums. Ja konfidenciālas personīgas informācijas iegūšana ir iespējama, bet nav paredzēta, ir jāapsver jebkuri iespējamie ietekmes mazināšanas pasākumi. Ja šādu pasākumu nav, jāapsver, vai pārtveršanas aģentūrai šajā ziņā jāievieš īpaši pasākumi.

4.29. Materiāls, kas identificēts kā konfidenciāla informācija, jāsaglabā vienīgi tad, ja šāda rīcība ir nepieciešama un samērīga ar vienu vai vairākiem 15. panta 4. punktā noteiktajiem atļautajiem nolūkiem. Tas ir jāiznīcina drošā veidā, tiklīdz tas šiem nolūkiem vairs nav vajadzīga. Ja šāda informācija tiek saglabāta, ir jābūt ieviestām atbilstošām informācijas pārvaldības sistēmām, lai nodrošinātu, ka turpmāka informācijas saglabāšana ir nepieciešama un samērīga ar atļautajiem likumā noteiktajiem nolūkiem.

4.30. Ja konfidenciālā informācija tiek saglabāta vai izplatīta kādai ārējai struktūrai, jāveic atbilstoši pasākumi, lai informācija tiktu apzīmēta kā konfidenciāla. Ja radušās šaubas par konfidenciālās informācijas ierosinātās apstrādes vai izplatīšanas likumību, jāvēršas pie attiecīgās pārtveršanas aģentūras juriskonsulta, pirms materiāls tiek izplatīts.

4.31. Par jebkuru konfidenciālās informācijas saglabāšanas gadījumu jāziņo komisāram sakaru pārtveršanas jautājumos, tiklīdz tas praktiski iespējams, par to vienojoties ar komisāru. Jebkurš saglabātais materiāls komisāram jāpadara pieejams pēc viņa pieprasījuma.

4.32. Drošības pasākumi, kas noteikti 4.28.–4.31. punktā, attiecas arī uz 8. panta 4. punktā minēto materiālu (skat. 6. nodaļu), kas atlasīts pārbaudei un ir uzskatāms par konfidenciālu informāciju.

(..)

6. PĀRTVERŠANAS ORDERI (8. PANTA 4. PUNKTS)

6.1. Šī iedaļa attiecas uz ārējo sakaru pārtveršanu atbilstoši *RIPA* 8. panta 4. punktā noteiktajam orderim.

6.2. Atšķirībā no 8. panta 1. punktā minētā, 8. panta 4. punktā noteiktajā orderī nav jānosauc vai jāraksturo pārtveršanas subjekts vai jānorāda telpas, attiecībā uz kurām veicama pārtveršana. Tāpat 8. panta 4. punkts neuzliek par pienākumu ierobežot to ārējo sakaru apjomu, kas var tikt pārtverti. Piemēram, ja ir izpildītas 8. panta 4. un 5. punktā noteiktās prasības, principā var likumīgi atļaut pārtvert visus sakarus, ko pārraida pa kādu konkrētu maršrutu vai kabeli vai nosūta kāds konkrēts SPS. Minētais liecina par to, ka 8. panta 4. punktā noteiktā pārtveršana izpaužas kā spēja vākt izlūkdatus, savukārt 8. panta 1. punktā noteiktā pārtveršana galvenokārt ir izmeklēšanas līdzeklis, ko izmanto, tiklīdz ir identificēts konkrētais pārtveršanas subjekts.

6.3. Par pārtveršanas orderu izdošanu saskaņā ar *RIPA* 8. panta 4. punktu ir atbildīgs valsts sekretārs. Kad valsts sekretārs izdod šāda veida orderi, tam ir jāpievieno apliecinājums. Šis apliecinājums nodrošina, ka atlasīšanas process pārtvertajam materiālam tiek piemērots tādējādi, ka attiecīgajām personām pārbaudei ir pieejams vienīgi apliecinājumā raksturotais materiāls. Ja pārtverto materiālu nevar atlasīt, lai to lasītu, aplūkotu vai klausītos, ņemot vērā samērīgumu un apliecinājumā minētos nosacījumus, šo materiālu nav atļauts lasīt, aplūkot vai klausīties nevienai personai.

**8. panta 4. punktā noteiktā pārtveršana praksē**

6.4. Saskaņā ar 8. panta 4. punktā noteikto orderi atļauts pārtvert ārējos sakarus. Ja atbilstoši 8. panta 4. punktā noteiktajam orderim iegūts liels sakaru apjoms, pārtveršanas aģentūra parasti piemēro filtrēšanas procesu, lai automātiski atmestu sakarus, kuriem, visticamāk, nebūs izlūkošanas vērtības. Pārtveršanas aģentūras pilnvarotās personas pēc tam var piemērot meklēšanas kritērijus, lai atlasītu sakarus, kuriem, visticamāk, būs izlūkošanas vērtība, ņemot vērā valsts sekretāra izdotajā apliecinājumā minētos nosacījumus. Pirms pārtveršanas aģentūras pilnvarotā persona var piekļūt konkrētiem sakariem, attiecīgajai personai ir jāpaskaidro, kāpēc tas ir nepieciešams kādam no valsts sekretāra izdotajam orderim pievienotajā apliecinājumā norādītajiem iemesliem un kāpēc šāda rīcība konkrētajos apstākļos ir samērīga. Šis process ir pakļauts iekšējam auditam un ārējai pārraudzībai, ko veic komisārs sakaru pārtveršanas jautājumos. Ja valsts sekretārs(-e) uzskata, ka tas ir nepieciešams, viņš vai viņa var atļaut atlasīt tās personas sakarus, par kuru zināms, ka tā atrodas Britu salās. Ja šāda atļauja nav dota, pilnvarotā persona nedrīkst atlasīt šos sakarus.

**Ārējo sakaru definīcija**

6.5. Ārējie sakari ir definēti *RIPA* kā saziņu saturs, ko nosūta vai saņem ārpus Britu salām. Tas ietver ārpus Britu salām nosūtīto un saņemto saziņu saturu neatkarīgi no tā, vai pārraides brīdī tas šķērso Britu salas. Tomēr tas neietver Britu salās nosūtīto un saņemto saziņu saturu, pat ja tā pārraides gaitā tas šķērso Britu salas. Piemēram, e-pasta ziņojums, ko kāda persona Londonā nosūta kādai citai personai Birmingemā, *RIPA* 20. panta izpratnē būs iekšēji, nevis ārēji sakari neatkarīgi no tā, vai tie tiek maršrutēti caur IP adresēm ārpus Britu salām, jo sūtītājs un paredzētais saņēmējs atrodas Britu salās.

**Tādu sakaru pārtveršana atbilstoši 8. panta 4. punktā noteiktajiem orderiem, kas nav ārēji sakari**

6.6. No *RIPA* 5. panta 6. punkta a) apakšpunkta skaidri izriet, ka rīcība, kas atļauta atbilstoši 8. panta 4. punktā noteiktajam orderim, principā var ietvert tādu sakaru pārtveršanu, kas nav ārēji sakari, ciktāl tas ir nepieciešams, lai pārtvertu ārējos sakarus, uz kuriem attiecas orderis.

6.7. Veicot pārtveršanu atbilstoši 8. panta 4. punktā noteiktajam orderim, pārtveršanas aģentūrai ir jāizmanto savas zināšanas par veidu, kādā tiek maršrutēti starptautiskie sakari, kā arī regulāri jāpārbauda attiecīgie sakaru kanāli, lai apzinātu tos individuālos sakaru nesējus, kuri, visticamāk, saturēs ārējos sakarus, kas atbildīs valsts sekretāra apliecinātajiem materiāla aprakstiem saskaņā ar 8. panta 4. punktu. Tai arī jāveic pārtveršana tā, lai ierobežotu tādu sakaru apkopošanu, kas nav ārēji sakari, līdz minimumam, kas atbilst nepieciešamo ārējo sakaru pārtveršanas mērķim.

**8. panta 4. punktā noteiktā ordera piemērošana**

6.8. Pieteikumu ordera saņemšanai iesniedz valsts sekretārs. Izdodot pārtveršanas orderus, tos adresē personai, kura iesniegusi pieteikumu. Šāda ordera mērķis parasti atspoguļos vienu vai vairākas Valsts drošības padomes noteiktās (turpmāk tekstā – “*NSC*”) izlūkošanas prioritātes.

6.9. Pirms iesniegšanas katrs pieteikums tiek izskatīts aģentūrā, kas iesniedz pieteikumu. Tas ietver rūpīgu pārbaudi, ko veic vairāk nekā viena amatpersona, kas izvērtēs, vai pieteikums ir paredzēts nolūkam, uz ko attiecas *RIPA* 5. panta 3. punkts, un vai ierosinātā pārtveršana ir gan nepieciešama, gan samērīga.

6.10. Katrā pieteikumā, kura kopiju saglabā pieteikuma iesniedzējs, jānorāda šāda informācija:

* pamatinformācija par attiecīgo operāciju:
* pārtveramo sakaru raksturojums, informācija par SPS un operācijas iespējamības novērtējums, ja tas nepieciešams, un
* atļautās rīcības raksturojums, kas attiecas vienīgi uz ārējo sakaru pārtveršanu, vai tās rīcības raksturojums (tostarp attiecībā uz citu sakaru pārtveršanu, kas orderī nav konkrēti norādīti, kā to paredz *RIPA* 5. panta 6. punkta a) apakšpunkts), kas nepieciešama, lai veiktu orderī atļautos vai noteiktos pasākumus un iegūtu saistītos sakaru datus;
* apliecinājums, kas regulēs pārtvertā materiāla pārbaudi;
* paskaidrojums par to, kādēļ pārtveršana uzskatāma par nepieciešamu vienam vai vairākiem 5. panta 3. punktā noteiktajiem nolūkiem;
* izvērtējums par to, kādēļ atbilstoši orderim atļautā pārtveršana ir samērīga ar šīs rīcības mērķi;
* pamatojums, ka pieteikums ir steidzams;
* apstiprinājums, ka attiecīgās personas lasīs, aplūkos vai klausīsies vienīgi to pārtverto materiālu, kas ir apliecināts un atbilst *RIPA* 16. panta 2.–6. punktā minētajiem nosacījumiem, un
* apstiprinājums, ka viss pārtvertais materiāls tiks apstrādāts saskaņā ar drošības pasākumiem, ko paredz *RIPA* 15. un 16. pants (skat. attiecīgi 7.2. un 7.10. punktu).

**Atļauja izdot 8. panta 4. punktā noteikto orderi**

6.11. Pirms ordera izdošanas saskaņā ar 8. panta 4. punktu valsts sekretāram ir jāpārliecinās, ka orderis ir nepieciešams:

* valsts drošības interesēs;
* smaga nozieguma novēršanai vai atklāšanai vai
* Apvienotās Karalistes ekonomiskās labklājības aizsardzībai, ciktāl šīs intereses sasaucas ar valsts drošības interesēm.

6.12. Pilnvaras izdot pārtveršanas orderi, lai nodrošinātu Apvienotās Karalistes ekonomiskās labklājības aizsardzību (kā to paredz *RIPA* 5. panta 3. punkta c) apakšpunkts), var īstenot vienīgi tad, kad valsts sekretāra ieskatā attiecīgie apstākļi atbilst valsts drošības interesēm. Valsts sekretārs neizdos orderi, pamatojoties uz 5. panta 3. punkta c) apakšpunktu, ja netiek konstatēta tieša saikne starp Apvienotās Karalistes ekonomisko labklājību un valsts drošību. Līdz ar to jebkurā pieteikumā ordera izdošanai, pamatojoties uz 5. panta 3. punkta c) apakšpunktu, ir jānorāda apstākļi, kas saistīti ar valsts drošības interesēm.

6.13. Valsts sekretāram arī jāizvērtē, vai atbilstoši orderim atļautā rīcība ir samērīga ar šīs rīcības mērķi (5. panta 2. punkta b) apakšpunkts). Izvērtējot nepieciešamību un samērīgumu, valsts sekretāram ir jāņem vērā, vai nepieciešamo informāciju varētu saprātīgi iegūt ar citiem līdzekļiem (5. panta 4. punkts).

6.14. Kad valsts sekretārs(-e) izdod šāda veida orderi, tam ir jāpievieno apliecinājums, kurā valsts sekretārs(-e) apliecina, ka viņa vai viņas ieskatā pārtvertā materiāla pārbaude ir nepieciešama vienam vai vairākiem 5. panta 3. punktā noteiktajiem nolūkiem. Šā likumā noteiktā apliecinājuma mērķis ir nodrošināt, ka atlasīšanas process pārtvertajam materiālam tiek piemērots tādējādi, ka attiecīgajām personām pārbaudei ir pieejams vienīgi apliecinājumā raksturotais materiāls. Jebkuram apliecinājumam ir plaši jāatspoguļo “Izlūkdatu apkopošanas prioritātes”, ko *NSC* noteikusi kā vadlīnijas izlūkošanas aģentūrām. Piemēram, apliecinājums var paredzēt tāda materiāla pārbaudi, kas sniedz izlūkdatus par terorismu (kā noteikts 2000. gada Terorisma apkarošanas likumā [*Terrorism Act 2000*]) vai kontrolējamām narkotiskām vielām (kā noteikts 1971. gada Likumā par narkotisko vielu ļaunprātīgu izmantošanu [*Misuse of Drugs Act 1971*]). Komisāram sakaru pārtveršanas jautājumos ir jāizvērtē jebkuras izmaiņas apliecinājumā norādītā materiāla aprakstos.

6.15. Valsts sekretāram ir pienākums nodrošināt, ka ir spēkā pasākumi, kas nodrošina, ka attiecīgās personas faktiski lasa, aplūko un klausās vienīgi materiālu, par ko apliecinājumā norādīts, ka tas ir jāpārbauda 5. panta 3. punktā minētajam nolūkam, un kas atbilst 16. panta 2.–6. punktā norādītajiem nosacījumiem. Komisāram sakaru pārtveršanas jautājumos ir pienākums pārskatīt šo pasākumu atbilstību.

**Atļauja izdot 8. panta 4. punktā noteikto orderi steidzamības kārtā**

6.16. *RIPA* paredz noteikumus (7. panta 1. punkta b) apakšpunkts) gadījumos, kad pārtveršanas orderis ir nepieciešams steidzamības kārtā, bet valsts sekretārs nav pieejams, lai to parakstītu. Šādos gadījumos valsts sekretārs personīgi atļauj veikt pārtveršanu, taču orderi paraksta vecākā amatpersona pēc tam, kad amatpersonas un valsts sekretārs lietu ir apsprieduši. *RIPA* šādā veidā pieļauj orderu izdošanu vienīgi steidzamos gadījumos, kad valsts sekretārs ir personīgi un skaidri atļāvis izdot orderi (7. panta 2. punkta a) apakšpunkts), un nosaka, ka orderī jāietver attiecīgais paziņojums (7. panta 4. punkta a) apakšpunkts).

6.17. Steidzamības kārtā izdots orderis ir spēkā piecas darbdienas pēc tā izdošanas dienas, ja vien valsts sekretārs to nav atjaunojis, un tādā gadījumā tā termiņš beidzas pēc trim mēnešiem, ja tas attiecas uz smagu noziegumu, vai pēc sešiem mēnešiem, ja tas attiecas uz valsts interesēm vai ekonomisko labklājību, gluži kā pārējie 8. panta 4. punktā noteiktie orderi.

**8. panta 4. punktā noteiktā ordera formāts**

6.18. Ikviens orderis ir adresēts personai, kura iesniegusi pieteikumu. Pēc tam tā kopiju var iesniegt sakaru pakalpojumu sniedzējiem, kuri, šīs personas ieskatā, varēs palīdzēt īstenot pārtveršanu. SPS parasti nesaņem apliecinājuma kopiju. Orderī ir jānorāda šāda informācija:

* pārtveramo sakaru raksturojums;
* ordera reģistrācijas numurs un
* informācija par personām, kuras pēc tam steidzamības kārtā var modificēt apliecinājumu, kas attiecas uz orderi (ja tas atļauts saskaņā ar *RIPA* 10. panta 7. punktu).

**8. panta 4. punktā noteiktā ordera un/vai apliecinājuma modificēšana**

6.19. Pārtveršanas orderus un apliecinājumus var modificēt saskaņā ar *RIPA* 10. panta noteikumiem. Orderi var modificēt vienīgi valsts sekretārs vai steidzamības kārtā vecākā amatpersona ar valsts sekretāra skaidru atļauju. Šādos gadījumos paziņojums par šo faktu ir jāvīzē dokumentā, kas ir modificēts, un šāda modifikācija zaudē spēku piecas darbdienas pēc šā dokumenta izdošanas dienas, ja vien to nav vīzējis valsts sekretārs.

6.20. Apliecinājums jāmodificē valsts sekretāram, izņemot steidzamus gadījumus, kad to var izdarīt vecākā amatpersona, ja tā ieņem amatu, kura ietvaros tai saskaņā ar apliecinājumā ietvertajiem noteikumiem ir skaidri atļauts modificēt apliecinājumu valsts sekretāra vārdā, vai ja valsts sekretārs ir skaidri atļāvis modifikāciju un paziņojums par šo faktu ir vīzēts dokumentā, kas ir modificēts. Pēdējā no minētajiem gadījumiem modifikācija zaudē spēku piecas darbdienas pēc šā dokumenta izdošanas dienas, ja vien to nav vīzējis valsts sekretārs.

6.21. Ja valsts sekretārs to uzskata par nepieciešamu, apliecinājumu var modificēt, ļaujot atlasīt tās personas sakarus, par kuru zināms, ka tā atrodas Britu salās. Personas atrašanās vieta ir jāizvērtē, izmantojot visu pieejamo informāciju. Ja ar šīs informācijas palīdzību nav iespējams precīzi noskaidrot personas atrašanās vietu, personas atrašanās vieta ir pārdomāti jāizvērtē pēc labas ticības principa. Ja radušās pamatotas aizdomas, ka persona atrodas Apvienotajā Karalistē, tiks piemēroti šajā punktā norādītie pasākumi.

**8. panta 4. punktā noteiktā ordera atjaunošana**

6.22. Valsts sekretārs var atjaunot orderi jebkurā brīdī pirms tā termiņa beigām. Pieteikumus ordera atjaunošanai iesniedz valsts sekretāram, un tajos ietver jaunāko informāciju par iepriekš 6.10. punktā minētajiem jautājumiem. Pieteikuma iesniedzējam jo īpaši jāizvērtē pašreizējā pārtveršanas vērtība un jāpaskaidro, kādēļ tā ieskatā pārtveršana joprojām ir nepieciešama vienam vai vairākiem 5. panta 3. punktā minētajiem nolūkiem un kādēļ tas uzskata, ka pārtveršana joprojām ir samērīga.

6.23. Ja valsts sekretārs ir guvis pārliecību, ka pārtveršana joprojām atbilst *RIPA* noteiktajām prasībām, viņš orderi var atjaunot. Ja orderi izdod, pamatojoties uz kādu smagu noziegumu, atjaunotais orderis ir spēkā vēl trīs mēnešus. Ja to izdod, pamatojoties uz valsts drošību / ekonomisko labklājību, atjaunotais orderis ir spēkā sešus mēnešus. Šo laika periodu skaita no atjaunotā dokumenta parakstīšanas dienas.

6.24. Gadījumos, kad nepieciešama SPS iesaistīšanās, ordera atjaunošanas dokumenta kopiju iesniedz visām personām, kurām iesniegta oriģinālā ordera dokumenta kopija, ja šīs personas joprojām vēlas aktīvi iesaistīties. Ordera atjaunošanas dokumentā iekļauj tā ordera vai to orderu reģistrācijas numuru, ko atjauno ar šo vienoto dokumentu.

**Ordera atcelšana**

6.25. Valsts sekretāram(-ei) ir jāatceļ pārtveršanas orderis, ja jebkurā brīdī pirms tā termiņa beigām viņš vai viņa gūst pārliecību, ka orderis vairs nav nepieciešams *RIPA* 5. panta 3. punktā minētajiem nolūkiem. Līdz ar to pārtveršanas aģentūrām būs pastāvīgi jāpārskata savi orderi un jāziņo valsts sekretāram, ja tās atzīst, ka pārtveršana vairs nav nepieciešama. Praksē pienākumu valsts sekretāra vārdā atcelt orderi pilda oderi izdevušās nodaļas vecākā amatpersona.

6.26. Ordera atcelšanas dokumentu adresē personai, kurai orderi izdeva (pārtveršanas aģentūrai). Ordera atcelšanas dokumenta kopija jānosūta tiem SPS (ja tādi iesaistījušies), kuri pēdējo divpadsmit mēnešu laikā ir izpildījuši šo orderi.

**Ieraksti**

6.27. Pārraudzības režīms ļauj komisāram sakaru pārtveršanas jautājumos pārbaudīt pieteikumu ordera saņemšanai, uz kuru balstīts valsts sekretāra lēmums, un pārtveršanas aģentūrai var tikt prasīts pamatot saturu. Ikvienai pārtveršanas aģentūrai ir jāsaglabā turpmāk minētā informācija, kurai komisāram(-ei) pēc tā vai tās pieprasījuma jābūt pieejamai pārbaudei:

* visi pieteikumi, kas iesniegti, lai saņemtu 8. panta 4. punktam atbilstošos orderus, un pieteikumi šo orderu atjaunošanai;
* visi orderi un apliecinājumi, kā arī orderu atjaunošanas un grozīšanas dokumentu kopijas (ja tādi ir);
* valsts sekretāra minētie iemesli pieteikuma noraidīšanai, ja tas ticis noraidīts;
* pārtveršanas sākuma un beigu datums.

6.28. Tāpat jāreģistrē pasākumi, ar kuriem nodrošina, ka attiecīgās personas saskaņā ar *RIPA* 15. pantu faktiski lasa, aplūko un klausās vienīgi materiālu, par ko apliecinājumā norādīts, ka tas ir jāpārbauda 5. panta 3. punktā minētajam nolūkam, un kas atbilst *RIPA* 16. panta 2.–6. punktā norādītajiem nosacījumiem. Jāreģistrē arī pasākumi, ar kuriem nodrošina atbilstību 15. panta 2. punktā (pārtvertā materiāla kopēšanas un izplatīšanas samazināšana līdz minimumam) un 15. panta 3. punktā (pārtvertā materiāla iznīcināšana) minētajām prasībām. Skat. detalizētāku informāciju nodaļā “Drošības pasākumi”.

7. DROŠĪBAS PASĀKUMI

7.1. Viss materiāls, kas pārtverts saskaņā ar oderi, kurš atbilst *RIPA* 8. panta 1. vai 4. punktam, un jebkuri saistītie sakaru dati jāapstrādā saskaņā ar drošības pasākumiem, kurus valsts sekretārs(-e) apstiprinājis atbilstoši pienākumam, ko tam vai tai uzliek *RIPA*. Šie drošības pasākumi ir pieejami komisāram sakaru pārtveršanas jautājumos, un tiem jāatbilst *RIPA* 15. panta prasībām, kas norādītas turpmāk. Turklāt *RIPA* 16. pantā noteiktie drošības pasākumi attiecas uz orderiem, kas atbilst 8. panta 4. punktam. Par jebkuru šo drošības pasākumu pārkāpumu jāziņo komisāram sakaru pārtveršanas jautājumos. Pārtveršanas aģentūrām periodiski jāpārskata savi iekšējie drošības pasākumi, lai nodrošinātu, ka tie ir aktuāli un efektīvi. Šādas periodiskas pārskatīšanas laikā aģentūrām jāapsver, vai vairākus šos iekšējos pasākumus varētu droši un lietderīgi nodot atklātībā.

**15. pantā noteiktie drošības pasākumi**

7.2. *RIPA* 15. pants nosaka, ka pārtvertā materiāla izpaušana, kopēšana un saglabāšana ir ierobežota līdz minimumam atļautajiem nolūkiem. *RIPA* 15. panta 4. punkts paredz, ka kaut kas ir nepieciešams atļautajiem nolūkiem, ja pārtvertais materiāls:

* joprojām ir vai, visticamāk, kļūs nepieciešams, kā norādīts likuma 5. panta 3. punktā, proti, valsts drošības interesēs, smaga nozieguma novēršanai vai atklāšanai vai arī Apvienotās Karalistes ekonomiskās labklājības aizsardzībai apstākļos, kas valsts sekretāra ieskatā skar valsts drošību;
* ir nepieciešams, lai sekmētu valsts sekretāra funkciju izpildi saskaņā ar *RIPA* I daļas I nodaļu;
* ir nepieciešams, lai sekmētu jebkuras komisāra sakaru pārtveršanas jautājumos vai tiesas funkcijas izpildi;
* ir nepieciešams, lai nodrošinātu, ka persona, kas veic kriminālvajāšanu, ir informēta par to, ko tās amata pienākums paredz, lai kriminālvajāšanā nodrošinātu godīgumu, vai
* ir nepieciešams, lai izpildītu jebkuru amata pienākumu, ko nosaka publisko reģistru tiesību akti.

**Pārtvertā materiāla izplatīšana**

7.3. To personu skaitu, kurām pārtverto materiālu izpauž, un šādas izpaušanas apmēru ierobežo līdz minimumam, kas nepieciešams atļautajiem nolūkiem, kuri norādīti *RIPA* 15. panta 4. punktā. Šis pienākums attiecas gan uz informācijas izpaušanu papildu personām aģentūrā, gan uz izpaušanu ārpus tās. To īsteno, aizliedzot izpaust materiālu personām, kuras nav atbilstoši pārbaudītas, kā arī ievērojot “nepieciešamības zināt” principu, proti, pārtverto materiālu nedrīkst izpaust nevienai personai, ja vien šīs personas pienākumi, kuriem ir jāattiecas uz kādu no atļautajiem nolūkiem, neparedz, ka tam vai tai jāzina par pārtverto materiālu, lai veiktu šos pienākumus. Tieši tāpat var izpaust tikai tik daudz pārtvertā materiāla, cik nepieciešams saņēmējam. Piemēram, ja pietiks ar pārtvertā materiāla kopsavilkumu, nav jāizpauž vairāk par šo materiāla apjomu.

7.4. Pienākumi attiecas ne tikai uz sākotnējo pārtvērēju, bet arī uz ikvienu, kam pārtvertais materiāls vēlāk tiek atklāts. Atsevišķos gadījumos to panāks, uzliekot pēdējam no minētajiem par pienākumu pirms pārtvertā materiāla turpmākas izpaušanas saņemt dokumenta sastādītāja atļauju. Citos gadījumos sekundārajiem saņēmējiem piemēro skaidrus drošības pasākumus.

7.5. Ja pārtvertais materiāls tiek izpausts ārpus Apvienotās Karalistes esošas valsts vai teritorijas iestādēm, aģentūrai ir jāveic saprātīgi pasākumi, lai nodrošinātu, ka attiecīgās iestādes ir ieviesušas un uzturēs nepieciešamās procedūras, lai aizsargātu pārtverto materiālu, kā arī nodrošinātu, ka šis materiāls tiek izpausts, kopēts, izplatīts un saglabāts vienīgi minimālajā nepieciešamajā apjomā. Turklāt pārtverto materiālu nedrīkst tālāk izpaust trešās valsts vai teritorijas iestādēm, ja vien tas nav nepārprotami saskaņots ar izdevēju iestādi, un materiāls ir jāatdod izdevējai iestādei vai droši jāiznīcina, kad tas vairs nav nepieciešams.

**Kopēšana**

7.6. Pārtverto materiālu var kopēt tikai tiktāl, cik tas ir nepieciešams *RIPA* 15. panta 4. punktā noteiktajiem atļautajiem nolūkiem. Kopijas ietver ne tikai visa pārtvertā materiāla tiešas kopijas, bet arī izrakstus un kopsavilkumus, kas identificē sevi kā pārtveršanas produktu, kā arī jebkuru uz pārtveršanu attiecināmu ierakstu, kas ietver to personu identitāti, kurām pārtvertais materiāls nosūtīts vai kuras to nosūtījušas. Ierobežojumi tiek īstenoti, uzliekot par pienākumu rīkoties īpaši ar kopijām, izrakstiem un kopsavilkumiem, kas izveidoti, reģistrējot to izveidi, izplatīšanu un iznīcināšanu.

**Uzglabāšana**

7.7. Pārtvertais materiāls un visas tā kopijas, izraksti un kopsavilkumi ir jāapstrādā un jāuzglabā droši, lai samazinātu to zaudēšanas vai zādzības risku. Tas jāuzglabā tā, lai nebūtu pieejams personām, kurām nav nepieciešamā drošības pārbaudes līmeņa. Šis pienākums droši uzglabāt pārtverto produktu attiecas uz visām personām, kuras ir atbildīgas par tā apstrādi, tostarp SPS. Detalizēta informācija par to, ko šāda prasība praksē nozīmēs attiecībā uz SPS, tiks izklāstīta pārrunās ar valdību pirms 12. pantā minētā paziņojuma nosūtīšanas (skat. 3.13. punktu).

**Iznīcināšana**

7.8. Pārtvertais materiāls un visas tā kopijas, izraksti un kopsavilkumi, ko var identificēt kā pārtveršanas produktu, ir jāatzīmē dzēšanai un pēc iespējas ātrāk droši jāiznīcina, tiklīdz tie vairs nav nepieciešami nevienam no atļautajiem nolūkiem. Ja pārtvertais materiāls tiek saglabāts, tas atbilstošos intervālos ir jāpārskata, lai pārliecinātos, ka saskaņā ar *RIPA* 15. panta 3. punktu joprojām ir pamatots iemesls to saglabāt.

7.9. Ja pārtveršanas aģentūra veic pārtveršanu atbilstoši 8. panta 4. punktā noteiktajam orderim un saņem neanalizētu pārtverto materiālu un saistītos sakaru datus, kas pārtverti atbilstoši šim orderim, tai jānorāda (vai atkarībā no sistēmas jānosaka) maksimālie saglabāšanas periodi dažādām šādu datu kategorijām, kas norāda attiecīgo datu raksturīgās iezīmes un iejaukšanās pakāpi. Norādītajiem laika periodiem parasti nav jāilgst vairāk par diviem gadiem, un tie jāsaskaņo ar komisāru sakaru pārtveršanas jautājumos. Datus var saglabāt ilgāk par piemērojamo maksimālo saglabāšanas periodu tikai tad, ja iepriekš no attiecīgās izlūkošanas aģentūras vecākās amatpersonas ir saņemta atļauja, pamatojoties uz to, ka konkrēto datu turpmāka saglabāšana ir tikusi atzīta par nepieciešamu un samērīgu. Ja pēc tam tiek atzīts, ka šo datu turpmāka saglabāšana vairs neatbilst nepieciešamības un samērīguma pārbaudēm, tie ir jādzēš. Ciktāl tas iespējams, visu saglabāšanas periodu pamatā ir jābūt automātiskas dzēšanas procesam, kas tiek uzsākts, tiklīdz ir apritējis attiecīgajiem datiem piemērojamais maksimālais saglabāšanas periods.

**Personāla drošība**

7.10. Visām personām, kurām var būt piekļuve pārtvertajam materiālam vai kurām saistībā ar to jāaplūko jebkuri ziņojumi, ir jāveic atbilstoša drošības pārbaude. Ik gadu vadītājiem ir jāapzina jebkuras bažas, kuru dēļ var tikt pārskatīta atsevišķu personāla locekļu drošības pārbaude. Periodiski jāpārskata arī katra atsevišķa personāla locekļa drošības pārbaude. Ja vienas aģentūras darbiniekam ir jāatklāj pārtvertais materiāls kādai citai, tas ir atbildīgs par to, ka saņēmējam ir vajadzīgā atļauja.

**16. pantā noteiktie drošības pasākumi**

7.11. 16. pants paredz papildu drošības pasākumus saistībā ar pārtverto materiālu, kas savākts atbilstoši 8. panta 4. punktā noteiktajam orderim, nosakot, ka drošības pasākumiem:

* jānodrošina, ka attiecīgā persona pārtverto materiālu lasa, aplūko vai klausās vienīgi tiktāl, ciktāl tas norādīts apliecinājumā, un
* jāregulē tādu atlasīšanas faktoru izmantošana, kas attiecas uz tādu personu sakariem, par kurām zināms, ka tās attiecīgajā brīdī atrodas Britu salās.

7.12. Turklāt jebkurai atsevišķai pārtvertā materiāla atlasei jābūt samērīgai konkrētajos apstākļos (norādīti 1998. gada Cilvēktiesību likuma [*Human Rights Act 1998*] 6. panta 1. punktā).

7.13. Šis apliecinājums nodrošina, ka atlasīšanas process saskaņā ar 8. panta 4. punktā noteikto orderi pārtvertajam materiālam tiek piemērots tādējādi, ka attiecīgajām personām pārbaudei ir pieejams vienīgi apliecinājumā raksturotais materiāls (lai to lasītu, aplūkotu vai klausītos). Nevienai amatpersonai nav atļauts piekļūt datiem, kas nav norādīti apliecinājumā.

7.14. Parasti atlasei saskaņā ar *RIPA* 16. panta 1. punktu jāizmanto automatizētas sistēmas, ja tas tehniski iespējams. Izņēmuma kārtā apliecinājumā var norādīt, ka pārtvertajam materiālam drīkst piekļūt ierobežots skaits īpaši pilnvarotu personāla locekļu, to neapstrādājot vai nefiltrējot automatizētās sistēmās. Šādu piekļuvi var atļaut tikai tiktāl, ciktāl tas nepieciešams, lai noteiktu, vai materiāls ietilpst galvenajās kategorijās, kas atlasāmas atbilstoši apliecinājumā norādītajam, vai lai nodrošinātu, ka izmantotā metodoloģija ir aktuāla un efektīva. Šādai pārbaudei jābūt nepieciešamai, pamatojoties uz *RIPA* 5. panta 3. punktu. Tiklīdz šīs funkcijas ir izpildītas, visas šiem nolūkiem izgatavotās materiāla kopijas ir jāiznīcina saskaņā ar *RIPA* 15. panta 3. punktu. Šādas amatpersonu veiktās pārbaudes jāsamazina līdz minimumam; tā vietā, kad vien iespējams, jāizmanto automātiskās atlasīšanas metodes. Komisārs sakaru pārtveršanas jautājumos pārskatīs šīs pārbaudes inspekciju laikā.

7.15. Materiāls, kas savākts atbilstoši 8. panta 4. punktā noteiktajam orderim, jālasa, jāaplūko un jāklausās vienīgi pilnvarotām personām, kuras regulāri tiek apmācītas saistībā ar *RIPA* noteikumiem, jo īpaši 16. punkta darbības jomu, kā arī prasībām par nepieciešamību un samērīgumu. Šīs prasības un procedūras ir jāizklāsta iekšējos norādījumos, ko sniedz visām pilnvarotajām personām, un visu pilnvaroto personu uzmanība ir īpaši jāvērš uz likumā noteiktajiem drošības pasākumiem. Visām pilnvarotajām personām ir jāveic atbilstoša drošības pārbaude (vairāk informācijas skat. 7.10. punktā).

7.16. Pirms pilnvarotā persona var lasīt, aplūkot vai klausīties materiālu, ir jāizveido ieraksts, kurā norādīts, kāpēc ir nepieciešama piekļuve materiālam saskaņā ar 16. pantu un piemērojamo apliecinājumu un kādēļ šāda piekļuve ir samērīga. Izņemot gadījumus, kad materiāls vai automatizētās sistēmas tiek pārbaudītas, kā norādīts 7.14. punktā, ierakstā, atsaucoties uz konkrētiem apstākļiem, jānorāda materiāls, kuram persona vēlas piekļūt, un sistēmām, ciktāl tas iespējams, ir jāliedz piekļuve materiālam, ja vien šāds ieraksts ir izveidots. Ierakstā jānorāda visi apstākļi, kas varētu būt par pamatu tam, ka notiek zināma netieša iejaukšanās personas tiesībās uz privātās dzīves neaizskaramību, kā arī visi pasākumi, kas veikti, lai samazinātu šādas netiešas iejaukšanās apmēru. Visi ieraksti jāsaglabā turpmākas pārbaudes vai audita vajadzībām.

7.17. Piekļuve materiālam, kā norādīts 7.15. punktā, jāierobežo līdz noteiktam laika periodam, lai gan piekļuvi var atjaunot. Ja piekļuve tiek atjaunota, ieraksts ir jāatjaunina, norādot piekļuves atjaunošanas iemeslu. Ir jābūt ieviestām sistēmām, lai nodrošinātu, ka tad, ja atjaunošanas pieprasījums netiek iesniegts šajā laika periodā, turpmāka piekļuve netiks piešķirta. Ja materiālam vairs nav nepieciešams piekļūt, ierakstā jāpaskaidro arī attiecīgais iemesls.

7.18. Periodiski jāveic auditi, lai nodrošinātu, ka tiek ievērotas *RIPA* 16. pantā un šā kodeksa 3. nodaļā izklāstītās prasības. Šiem auditiem jāietver pārbaudes, lai nodrošinātu, ka ieraksti, kuros pieprasīta piekļuve lasāmajam, aplūkojamajam vai klausāmajam materiālam, ir pareizi apkopoti, un jo īpaši to, ka pieprasītais materiāls atbilst valsts sekretāra apliecinātajai informācijai. Par visām kļūdām vai procesuāliem trūkumiem jāziņo vadībai un jāveic korektīvie pasākumi. Par jebkuriem nopietniem trūkumiem ir jāinformē augstākā vadība, un par jebkuriem drošības pasākumu pārkāpumiem (kā minēts 7.1. punktā) jāziņo komisāram sakaru pārtveršanas jautājumos. Attiecībā uz visiem pilnvaroto personu sagatavotajiem izlūkošanas ziņojumiem ir jāveic kvalitātes kontroles audits.

7.19. Lai izpildītu *RIPA* noteiktās prasības, kas minētas iepriekš 6.3. punktā, ja atlasīšanas faktors attiecas uz personu, par kuru zināms, ka tā pašlaik atrodas Britu salās, un tā nolūks vai viens no nolūkiem ir identificēt materiālu, kas ietverts šīs personas nosūtīto vai tai paredzēto saziņu saturā, valsts sekretāram vai steidzamības kārtā vecākajai amatpersonai jāiesniedz pieteikums, paskaidrojot, kāpēc grozījums 8. panta 4. punktā minētajā apliecinājumā saistībā ar šādu personu ir nepieciešams nolūkam, uz kuru attiecas *RIPA* 5. panta 3. punkts, un ir samērīgs attiecībā uz jebkuru rīcību, kas atļauta saskaņā ar *RIPA* 8. panta 4. punktu.

7.20. Valsts sekretāram jānodrošina, ka ir spēkā attiecīgie drošības pasākumi, pirms var uzsākt pārtveršanu atbilstoši 8. panta 4. punktā noteiktajiem orderiem. Komisāram sakaru pārtveršanas jautājumos ir pienākums pārbaudīt šo drošības pasākumu atbilstību.

(..)

8. IZPAUŠANA, LAI NODROŠINĀTU GODĪGUMU KRIMINĀLPROCESĀ

(..)

**Jautājumu izslēgšana no tiesvedības**

8.3. Parasti tiesvedību nevar ietekmēt ne pārtveršanas iespēja, ne pats pārtvertais materiāls. Šo noteikumu paredz *RIPA* 17. pants, kas tiesvedībā aizliedz pierādījumus, nopratināšanu, apgalvojumu vai paziņojumu, ar ko, visticamāk, var atklāt saskaņā ar šo likumu (vai 1985. gada Likumu par sakaru pārtveršanu [*Interception of Communications Act 1985*]) izdota ordera esību (vai neesību). Ar šo noteikumu saprot to, ka pārtverto materiālu nevar izmantot ne apsūdzības, ne aizstāvības puse. Tādējādi tiek saglabāta “pušu līdzekļu vienlīdzība”, kā to nosaka *ECHR* 6. pants.

(..)

10. PĀRRAUDZĪBA

10.1. *RIPA* paredz komisāru sakaru pārtveršanas jautājumos, kura uzdevums ir neatkarīgi pārraudzīt to, kā tiek īstenotas pilnvaras ar orderi noteiktā pārtveršanas režīma ietvaros saskaņā ar *RIPA* I daļas I nodaļu.

10.2. Šis komisārs divreiz gadā veic pārbaudes katrā no deviņām pārtveršanas aģentūrām. Pārbaužu primārais mērķis ir nodrošināt, ka komisāra(-es) rīcībā ir informācija, kas viņam vai viņai ir nepieciešama, lai pildītu savas funkcijas saskaņā ar *RIPA* 57. pantu un sagatavotu ziņojumu saskaņā ar *RIPA* 58. pantu. Tas var iekļaut pārbaudi vai apsvērumus attiecībā uz:

* sakaru pārtveršanai ieviestām sistēmām;
* attiecīgiem pārtveršanas aģentūras uzturētajiem reģistriem;
* veiktās pārtveršanas likumību un
* jebkurām kļūmēm un sistēmām, kas paredzētas šādu kļūmju novēršanai.

10.3. Jebkurai personai, kura īsteno *RIPA* I daļas I nodaļā noteiktās pilnvaras, ir jāinformē komisārs par jebkuru rīcību, kas var būt pretēja *RIPA* noteikumiem, vai jebkuru neadekvātu 15. pantā noteikto drošības pasākumu neīstenošanu. Šai personai arī jāizpilda visi komisāra pieprasījumi sniegt jebkuru informāciju, kas viņam nepieciešama, lai viņš varētu veikt savas funkcijas.”

5. Čārlza Farra liecība

97. Savā liecībā, kas bija sagatavota “Liberty” tiesvedībai (skat. iepriekš 40. punktu), Čārlzs Farrs norādīja, ka līdzās informācijai, kas izklāstīta *RIPA*, 2010. gada *IC* kodeksā un 2016. gada *IC* kodeksa projektā (kas tobrīd bija publicēts apspriešanai), visa informācija par 15. un 16. pantā minētajiem drošības pasākumiem bija paturēta noslēpumā. Viņš bija personīgi pārskatījis pasākumus un guvis pārliecību, ka tos nevar droši nodot atklātībā, neapdraudot pārtveršanas metožu efektivitāti. Tomēr pasākumi bija padarīti pieejami *IC* komisāram, kuram saskaņā ar *RIPA* tie bija jāpārskata. Turklāt katrai pārtveršanas aģentūrai bija jāreģistrē attiecīgie pasākumi un par jebkuru pārkāpumu jāziņo *IC* komisāram.

6. 2015. gada Pārskats par valsts drošības stratēģiju, stratēģisko aizsardzību un drošību. Droša un turīga Apvienotā Karaliste [National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom]

98. Šajā pārskatā Valsts drošības padome (*NSC*) norādīja, ka tās prioritātes turpmākajiem pieciem gadiem ir:

“Stingri un visaptveroši apkarot terorismu gan valstī, gan ārvalstīs, cīnīties pret ekstrēmismu un izaicināt to sekmējošās kaitīgās ideoloģijas. Mēs turpināsim būt pasaules līderi kiberdrošības jomā. Mēs novērsīsim citu valstu radītos draudus. Mēs reaģēsim uz krīzēm ātri un efektīvi un stiprināsim savu izturību gan valstī, gan ārvalstīs.

Palīdzēt stiprināt uz noteikumiem balstīto starptautisko kārtību un tās institūcijas, veicinot reformas, lai sekmētu augošo lielvaru turpmāku līdzdalību. Mēs sadarbosimies ar saviem partneriem, lai mazinātu konfliktus, un sekmēsim stabilitāti, labu pārvaldību un cilvēktiesību ievērošanu.

Veicināt mūsu labklājību, izvēršot mūsu ekonomiskās attiecības ar augošām lielvarām, piemēram, Indiju un Ķīnu, palīdzot veidot globālu labklājību, ieguldot inovācijās un prasmēs un atbalstot ar Apvienotās Karalistes aizsardzību un drošību saistīto pakalpojumu sniegšanu.”

7. 2015. gada 29. marta IPT spriedums lietā “Belhažs [Belhadj] un citi pret Drošības dienestu, Slepenās izlūkošanas dienestu, Valdības komunikāciju galveno pārvaldi, Iekšlietu departamenta valsts sekretāru un Ārlietu un sadraudzības biroja valsts sekretāru”, IPT/13/132‑9/H un IPT/14/86/CH

99. Pieteikuma iesniedzēji šajā lietā sūdzējās par Konvencijas 6., 8. un 14. panta pārkāpumiem, kas izrietēja no tādu viņu sakaru iespējamās pārtveršanas, ko aizsargā advokāta un klienta saziņas konfidencialitāte. Ciktāl “Liberty” tiesvedībā “Amnesty International” sūdzējās par tādu pasākumu atbilstību, kuru mērķis ir aizsargāt materiālu, ko aizsargā advokāta un klienta saziņas konfidencialitāte (turpmāk tekstā – “*LPP*”), šīs sūdzības bija “novirzītas” izskatīšanai šajā lietā, un “Amnesty International” tajā iestājās kā prasītāja (skat. iepriekš 52. punktu).

100. Tiesvedības gaitā atbildētāji atzina, ka, nepastāvot likumīgai *LPP* regulēšanas sistēmai, ar advokāta un klienta saziņas konfidencialitāti aizsargāta materiāla pārtveršanas/iegūšanas, analizēšanas, izmantošanas, izpaušanas un iznīcināšanas režīms kopš 2010. gada janvāra nav atbildis likumam saskaņā ar Konvencijas 8. panta 2. punktu un līdz ar to bijis pretlikumīgs. Drošības dienests un *GCHQ* apstiprināja, ka tie turpmāko nedēļu laikā strādās pie tā, lai pārskatītu savas politikas nostādnes un procedūras, ņemot vērā *IC* kodeksa projektu un citus attiecīgos dokumentus.

101. Pēc tam *IPT* rīkoja slēgtu paskaidrojumu uzklausīšanu, kurā piedalījās tiesas padomnieks (skat. turpmāk 132. punktu), lai noskaidrotu, vai atbildētāji bija pārtvēruši vai ieguvuši jebkādus dokumentus vai informāciju saistībā ar materiālu, kas aizsargāts ar advokāta un klienta saziņas konfidencialitāti. 2015. gada 29. marta lēmumā tika konstatēts, ka izlūkdienestu rīcībā bija tikai divi dokumenti, kuri piederēja kādam no prasītājiem un kuros bija ietverti ar *LPP* aizsargātie materiāli, un ka tie neatklāja juridiskas konsultācijas un tajos nebija šādu norāžu. Līdz ar to tā konstatēja, ka attiecīgajam prasītājam nav nodarīts kaitējums vai zaudējumi un ka lēmums bija taisnīgs. Tomēr tā uzdeva *GCHQ* iznīcināt vai dzēst tās dokumentu daļas, kurās ietverts ar advokāta un klienta saziņas konfidencialitāti aizsargātais materiāls, iesniegt šo dokumentu kopiju *IC* komisāram saglabāšanai uz pieciem gadiem un četrpadsmit dienu laikā sagatavot konfidenciālu ziņojumu, kurā apstiprināts, ka dokumenti ir iznīcināti un dzēsti.

102. Gan *IC* kodeksa, gan Sakaru datu ieguves un izpaušanas prakses kodeksa grozījumu projekti pēc tam tika nodoti apspriešanai, savukārt kodeksos, kuri tā rezultātā tika pieņemti 2018. gadā, tika izvērstas iedaļas par piekļuvi konfidenciālai informācijai.

B. Izlūkdatu apmaiņa

1. Lielbritānijas–ASV līgums par sakaru izlūkošanu [British-US Communication Intelligence Agreement]

103. 1946. gada 5. marta Lielbritānijas–ASV līgums par sakaru izlūkošanu reglamentēja pasākumus starp Lielbritānijas un Amerikas Savienoto Valstu iestādēm par izlūkošanas informācijas apmaiņu saistībā ar “ārvalstu” sakariem, kas definēti, atsaucoties uz valstīm, kas nav Amerikas Savienotās Valstis, Apvienotā Karaliste un Sadraudzības valstis. Saskaņā ar šo līgumu puses apņēmās apmainīties ar vairāku ar ārvalstu sakariem saistīto pārtveršanas operāciju produktiem.

2. Piemērojamais izlūkdienestu darbības tiesiskais regulējums

104. Apvienotajā Karalistē darbojas trīs izlūkdienesti, proti, drošības dienests (turpmāk tekstā – “*MI5*”), slepenās izlūkošanas dienests (turpmāk tekstā – “*MI6*”) un *GCHQ*.

a) *MI5*

105. Saskaņā ar 1989. gada Drošības dienestu likuma (turpmāk tekstā – “*SSA*”) 2. pantu *MI5* ģenerāldirektoram, kuru iecēla Iekšlietu departamenta valsts sekretārs, bija pienākums nodrošināt pasākumus, lai garantētu, ka *MI5* neiegūst nekādu informāciju, izņemot tiktāl, ciktāl tas ir nepieciešams, lai tas atbilstoši pildītu savas funkcijas, vai to neizpauž, izņemot tiktāl, ciktāl tas ir nepieciešams šim nolūkam vai smagu noziegumu novēršanai vai atklāšanai, vai jebkāda kriminālprocesa nolūkos.

106. Saskaņā ar *SSA* 1. pantu *MI5* funkcijas bija aizsargāt valsts drošību, jo īpaši pret spiegošanas, terorisma un sabotāžas draudiem, ārvalstu aģentu darbībām un tādām darbībām, kuru mērķis ir gāzt vai graut parlamentāro demokrātiju ar politiskiem, rūpnieciskiem vai vardarbīgiem līdzekļiem, kā arī aizsargāt Apvienotās Karalistes ekonomisko labklājību pret draudiem, ko rada ārpus Britu salām esošu personu rīcība vai nodomi, un rīkoties, atbalstot policijas spēku, Valsts Noziedzības apkarošanas aģentūras un citu tiesībsargājošo iestāžu centienus novērst un atklāt smagus noziegumus.

b) *MI6*

107. Saskaņā ar 1994. gada Izlūkdienestu likuma (turpmāk tekstā – “*ISA*”) 2. pantu *MI6* dienesta vadītājam, kuru iecēla (toreizējais) valsts sekretārs ārlietās un sadraudzības lietās, bija pienākums nodrošināt pasākumus, lai garantētu, ka *MI6* neiegūst nekādu informāciju, izņemot tiktāl, ciktāl tas ir nepieciešams, lai tas atbilstoši pildītu savas funkcijas, vai to neizpauž, izņemot tiktāl, ciktāl tas ir nepieciešams šim nolūkam, valsts drošības interesēs, smagu noziegumu novēršanai vai atklāšanai vai arī jebkāda kriminālprocesa nolūkos.

108. Saskaņā ar *ISA* 1. pantu *MI6* funkcijas bija iegūt un sniegt informāciju par ārpus Britu salām esošu personu rīcību vai nodomiem un pildīt savus uzdevumus saistībā ar šādu personu rīcību vai nodomiem. Tas šīs funkcijas varēja pildīt vienīgi valsts drošības interesēs, īpaši atsaucoties uz valsts aizsardzības un ārlietu politiku, Apvienotās Karalistes ekonomiskās labklājības interesēs vai lai sekmētu smagu noziegumu novēršanu vai atklāšanu.

c) *GCHQ*

109. Saskaņā ar *ISA* 4. pantu *GCHQ* direktoram, kuru iecēla (toreizējais) valsts sekretārs ārlietās un sadraudzības lietās, bija pienākums nodrošināt pasākumus, lai garantētu, ka tā neiegūst nekādu informāciju, izņemot tiktāl, ciktāl tas ir nepieciešams, lai tā atbilstoši pildītu savas funkcijas, un to neizpauž, izņemot tiktāl, ciktāl tas ir nepieciešams.

110. Saskaņā ar *ISA* 3. pantu viena no *GCHQ* funkcijām bija pārraudzīt elektromagnētiskās, akustiskās un citas emisijas un visas iekārtas, kas rada šādas emisijas, vai radīt tām traucējumus, kā arī saņemt un sniegt informāciju, kas iegūta no šādām emisijām vai aprīkojuma un šifrētā materiāla vai ir ar to saistīta. Tā šo funkciju varēja pildīt vienīgi valsts drošības interesēs, īpaši atsaucoties uz valsts aizsardzības un ārlietu politiku, Apvienotās Karalistes ekonomiskās labklājības interesēs saistībā ar ārpus Britu salām esošu personu rīcību vai nodomiem vai lai sekmētu smagu noziegumu novēršanu vai atklāšanu.

d) 2008. gada Terorisma apkarošanas likums [*Counter-Terrorism Act 2008*]

111. 2008. gada Terorisma apkarošanas likuma 19. pants ļāva izpaust informāciju jebkuram izlūkdienestam, lai tas varētu pildīt jebkuru no tā funkcijām. Izlūkdienests saistībā ar savu funkciju izpildi iegūto informāciju varēja izmantot saistībā ar jebkuru citu savu funkciju izpildi.

112. *MI5* iegūto informāciju varētu izpaust nolūkos, lai tas pienācīgi pildītu savas funkcijas, novērstu vai atklātu smagus noziegumus, vai jebkura kriminālprocesa nolūkos. *MI6* iegūto informāciju varētu izpaust nolūkos, lai tas pienācīgi pildītu savas funkcijas, aizsargātu valsts drošības intereses, novērstu vai atklātu smagus noziegumus, vai jebkura kriminālprocesa nolūkos. *GCHQ* iegūto informāciju varētu izpaust nolūkos, lai tā pienācīgi pildītu savas funkcijas, vai jebkura kriminālprocesa nolūkos.

e) 1998. gada Datu aizsardzības likums [*Data Protection Act 1998*] (turpmāk tekstā – “*DPA*”)

113. *DPA* bija tiesiskais regulējums, ar ko Apvienotās Karalistes tiesību aktos transponēja Direktīvu 95/46/EK par personas datu aizsardzību. Katrs izlūkdienests *DPA* izpratnē bija “datu pārzinis”, tādēļ tiem bija jāatbilst 1. saraksta 1. daļā minētajiem datu aizsardzības principiem, ņemot vērā izņēmumu saskaņā ar ministra izdotu apliecinājumu, tostarp šādiem noteikumiem:

“5) Personas datus, kas tiek apstrādāti jebkuram nolūkam vai nolūkiem, nedrīkst glabāt ilgāk, nekā tas ir nepieciešams šim nolūkam vai šiem nolūkiem (..)”

un

“7) Jāveic atbilstoši tehniski un organizatoriski pasākumi, lai novērstu neatļautu vai nelikumīgu personas datu apstrādi un nejaušu personas datu nozaudēšanu, iznīcināšanu vai sabojāšanu.”

f) 1989. gada Valsts noslēpumu likums [*Official Secrets Act 1989*] (turpmāk tekstā – “*OSA*”)

114. Tiktu uzskatīts, ka izlūkdienesta darbinieks ir izdarījis noziedzīgu nodarījumu saskaņā ar *OSA* 1. panta 1. punktu, ja viņš vai viņa bez likumīgām pilnvarām izpaudis jebkādu informāciju, dokumentu vai citus datus, kas attiecas uz drošību vai izlūkdatiem un kas bijuši viņa vai viņas rīcībā kā šā dienesta locekļa amata ietvaros.

g) 1998. gada Cilvēktiesību aizsardzības likums [*Human Rights Act 1998*] (turpmāk tekstā – “*HRA*”)

115. Saskaņā ar *HRA* 6. pantu valsts iestāde nedrīkstēja rīkoties, pārkāpjot Konvencijā paredzētās tiesības.

3. Sakaru pārtveršanas prakses kodekss

116. Pēc “Liberty” tiesvedības 9. oktobra paziņojumā ietvertā informācija (skat. iepriekš 33. un 36. punktu) tika iekļauta *IC* kodeksā:

“12. NOTEIKUMI PAR NEANALIZĒTU PĀRTVERTU SAKARU PIEPRASĪŠANU NO KĀDAS ĀRVALSTS VALDĪBAS UN TO APSTRĀDI

**Šīs nodaļas piemērošana**

12.1. Šī nodaļa attiecas uz tām pārtveršanas aģentūrām, kuras veic pārtveršanu atbilstoši 8. panta 4. punktā noteiktajam orderim.

**Palīdzības lūgumi, kas nav iesniegti saskaņā ar starptautisku savstarpējās palīdzības līgumu**

12.2. Šādu pieprasījumu attiecībā uz neanalizētiem pārtvertiem sakariem (un saistītajiem sakaru datiem), izņemot saskaņā ar kādu starptautisku savstarpējās tiesiskās palīdzības līgumu, pārtveršanas aģentūra var iesniegt ārpus Apvienotās Karalistes esošas valsts vai teritorijas valdībai vienīgi tad, ja:

* valsts sekretārs saskaņā ar *RIPA* jau ir izdevis attiecīgu orderi par pārtveršanu, konkrēto sakaru iegūšanai ir nepieciešama ārvalsts valdības palīdzība, jo tos nav iespējams iegūt saskaņā ar attiecīgo *RIPA* noteikto orderi par pārtveršanu, un šo sakaru iegūšana pārtveršanas aģentūras ieskatā ir nepieciešama un samērīga vai
* pieprasījuma iesniegšana saistībā ar konkrētajiem sakariem, ja nav izdots attiecīgais *RIPA* noteiktais pārtveršanas orderis, nav uzskatāma par apzinātu *RIPA* apiešanu un nekā citādi netraucē *RIPA* mērķiem (piemēram, tādēļ, ka sakaru iegūšana saskaņā ar *RIPA* noteikumiem par pārtveršanu tehniski nav iespējama) un šo sakaru iegūšana pārtveršanas aģentūras ieskatā ir nepieciešama un samērīga.

12.3. Pieprasījumu, uz ko attiecas 12.2. punkta otrais ievilkums, var iesniegt vienīgi ārkārtas apstākļos, un to valsts sekretārs izvērtē un izlemj personīgi.

12.4. Atbilstoši tam ar “attiecīgo *RIPA* noteikto pārtveršanas orderi” saprot: a) 8. panta 1. punktā noteikto orderi saistībā ar attiecīgo subjektu; ii) 8. panta 4. punktā noteikto orderi un tam pievienoto apliecinājumu, kurā iekļauts viens vai vairāki “pārtvertā materiāla apraksti” (*RIPA* 8. panta 4. punkta b) apakšpunkta nozīmē), kas attiecas uz subjekta sakariem, ņemot vērā atbilstošās 16. panta 3. punktā noteiktās izmaiņas (attiecībā uz personām, par kurām zināms, ka tās atrodas Britu salās), vai iii) 8. panta 4. punktā noteikto orderi un tam pievienoto apliecinājumu, kurā iekļauts viens vai vairāki “pārtvertā materiāla apraksti”, kas attiecas uz subjekta sakariem (attiecībā uz citām personām).

**Drošības pasākumi, kas piemērojami, apstrādājot neanalizētus pārtvertus sakarus no kādas ārvalsts valdības**

12.5. Ja pieprasījumu, uz kuru attiecas 12.2. punkta otrais ievilkums, valsts sekretārs apstiprina nolūkiem, kas nav saistīti ar konkrētiem selektoriem, pārtveršanas aģentūra nedrīkst pārbaudīt nekādus saņemtos sakarus atbilstoši *RIPA* 16. panta 2. punkta a) un b) apakšpunktā minētajiem faktoriem, ja vien valsts sekretārs nav personīgi izvērtējis un apstiprinājis šo sakaru pārbaudi, atsaucoties uz šādiem faktoriem.[[1]](#footnote-1)

12.6. Ja pārtverto sakaru saturu vai sakaru datus iegūst pārtveršanas aģentūras, kā norādīts 12.2. punktā, vai tās tos kā citādi saņem no kādas ārpus Apvienotās Karalistes esošas valsts vai teritorijas valdības, apstākļos, kad materiāls sevi identificē kā pārtveršanas produktu (izņemot saskaņā ar starptautisku savstarpējās palīdzības līgumu), sakaru saturam un sakaru datiem ir jāpiemēro tādi paši iekšējie noteikumi un drošības pasākumi, kas attiecas uz tām pašām satura vai datu kategorijām, ja pārtveršanas aģentūras tos iegūst tieši, veicot pārtveršanu saskaņā ar *RIPA*.

12.7. Ja nav saņemts attiecīgais *RIPA* noteiktais pārtveršanas orderis, par visiem pieprasījumiem kādai ārpus Apvienotās Karalistes esošas valsts vai teritorijas valdībai saistībā ar neanalizētiem pārtvertiem sakariem (un saistītajiem sakaru datiem) tiks paziņots komisāram sakaru pārtveršanas jautājumos.

C. Sakaru datu iegūšana

117. *RIPA* 1. daļas II nodaļā ir ietverts tiesiskais regulējums, saskaņā ar kuru valsts iestādes varēja iegūt sakaru datus no SPS.

118. Saskaņā ar 22. pantu atļauju sakaru datu iegūšanai no SPS piešķīra “izraudzītā persona” ar tādu profesiju, pakāpi vai amatu attiecīgajās valsts iestādēs, kā noteikts valsts sekretāra rīkojumā. Izraudzītā persona varēja vai nu piešķirt atļauju personām, kuras strādā tajā pašā “attiecīgajā valsts iestādē” kā šī persona, “veikt darbību, uz kuru attiecas šī nodaļa” (atļauja saskaņā ar 22. panta 3. punktu), vai arī, iesniedzot SPS paziņojumu, pieprasīt vai nu atklāt datus, kas jau ir tās rīcībā, vai arī iegūt un izpaust datus (paziņojums saskaņā ar 22. panta 4. punktu). Saskaņā ar 22. panta 3. punktu “attiecīgās valsts iestādes” ietvēra policiju, Valsts Noziedzības apkarošanas aģentūru, Apvienotās Karalistes Ieņēmumu un muitas dienestu, jebkurus izlūkdienestus un jebkuru šādu valsts iestādi, ko ar rīkojumu varētu noteikt valsts sekretārs.

119. 22. panta 2. punktā ir paredzēts, ka izraudzītā persona varēja vienīgi dot 22. panta 3. punktā minēto atļauju vai iesniegt 22. panta 4. punktā minēto paziņojumu, ja tas šīs personas ieskatā bija nepieciešams:

“a) valsts drošības interesēs;

b) nozieguma novēršanai vai atklāšanai vai arī nekārtību novēršanai;

c) Apvienotās Karalistes ekonomiskās labklājības interesēs;

d) sabiedrības drošības interesēs;

e) sabiedrības veselības aizsardzībai;

f) valstij maksājamo nodokļu, nodevu, maksu vai citu maksājumu, iemaksu vai summu novērtēšanai un iekasēšanai;

g) personas nāves vai ievainojuma, vai tās fiziskās vai garīgās veselības kaitējuma novēršanai ārkārtas situācijā vai arī jebkura personas fiziskās vai garīgās veselības kaitējuma mazināšanai vai

h) jebkuriem nolūkiem (uz ko neattiecas a)–g) apakšpunkts), kas atbilstoši šim punktam noteikti ar valsts sekretāra rīkojumu.”

120. Šai personai arī jāpārliecinās, ka datu iegūšana ir samērīga ar šādas rīcības mērķi.

121. *RIPA* II nodaļa tika papildināta ar Sakaru datu iegūšanas un izpaušanas rīcības kodeksu [*Acquisition and Disclosure of Communications Data:* *Code of Practice*], kas izdots saskaņā ar *RIPA* 71. pantu.

D. *IPT* prakse un procedūra

1. RIPA

122. *IPT* tika izveidota saskaņā ar *RIPA* 65. panta 1. punktu, lai uzklausītu pilsoņu apgalvojumus par iespējamu pretlikumīgu iejaukšanos viņu sakaros tādas rīcības dēļ, uz kuru attiecas šis likums. Tai bija ekskluzīva kompetence izskatīt jebkuru sūdzību par personas sakaru pārtveršanu un pārtveršanas gadījumā pārbaudīt šīs pārtveršanas pilnvaras.

123. *IPT* pēc būtības bija iecelti tiesneši, taču tas bija atkarīgs no tā, vai izvirzītais kandidāts bija Anglijas un Velsas, Skotijas vai Ziemeļīrijas augstākā tiesas amatpersona (dēvēta par “tiesas iestādes locekli”) vai arī “ārpustiesas iestādes loceklis”. Ārpustiesas iestādes loceklis varēja būt kādreizējais tiesas iestādes loceklis, kurš vairs šādu amatu neieņem, vai augstākā tiesas amatpersona ar vismaz desmit gadu darba stāžu, kura nebija pilna laika tiesnesis. Ja tiesas iestādes locekļi tika izvēlēti no Anglijas un Velsas tiesas amatpersonu vidus, Tiesu birojs Lorda Augstā tiesneša vārdā vadīja atlases procesu. Tiesu birojs aicināja Anglijas un Velsas Augstās tiesas tiesnešus izteikt ieinteresētību, un pieteikuma iesniedzējus intervēja grupa, kuru veidoja *IPT* priekšsēdētājs, ārpustiesas iestādes *IPT* loceklis un komisārs no Tiesnešu iecelšanas komisijas, kas ir savas jomas speciālists. Pēc tam minētā grupa ziņoja Lordam Augstajam tiesnesim, kurš rakstveidā vērsās pie iekšlietu sekretāra, sniedzot formālus ieteikumus par locekļu iecelšanu. Pēc tam iekšlietu sekretārs rakstveidā vērsās pie Ministru prezidenta, lūdzot Viņas Majestātes Karalienes atļauju izdot patenta apliecinājumu attiecībā uz rekomendēto(-ajiem) kandidātu(-iem). Ministru prezidents rekomendēja izvēlēto(-s) kandidātu(-s) Viņas Majestātei Karalienei, kura formalizēja iecelšanu, izdodot patenta apliecinājumu. Ārpustiesas iestādes locekļi tika iecelti atklāta konkursa kārtībā. *IPT* publicēja sludinājumus par ārpustiesas iestāžu locekļiem konkrētos valsts laikrakstos un personāla atlases vietnēs, lūdzot piemērotās personas ar atbilstošo kvalifikāciju paust interesi. Šis process atšķīrās no tiesas iestāžu locekļu iecelšanas tādējādi, ka netika iesaistīts Lords Augstais tiesnesis, taču visos pārējos aspektos tas bija tāds pats. Pašlaik darbojas pieci tiesas iestāžu locekļi (divi Anglijas Apelācijas tiesas locekļi (viens no tiem priekšsēdētājs), viens Anglijas Augstās tiesas loceklis un divi Skotijas Augstākās tiesas ārpalātas locekļi (viens no tiem priekšsēdētāja vietnieks)) un pieci ārpustiesas iestāžu locekļi (viens no tiem atvaļināts Ziemeļīrijas Augstās tiesas tiesnesis).

124. Saskaņā ar 67. panta 2. punktu un 67. panta 3. punkta c) apakšpunktu *IPT* bija jāpiemēro principi, ko tiesa piemēro, veicot pārskatīšanu tiesā. Tomēr tā nebija pilnvarota iesniegt paziņojumu par nesaderību, ja tā atzina primāros tiesību aktus par nesaderīgiem ar Eiropas Cilvēktiesību konvenciju, jo tā nebija “tiesa” 1998. gada Cilvēktiesību likuma izpratnē.

125. 68. panta 6. un 7. punkts noteica, ka pārtveršanas ordera atļaušanā un izpildē iesaistītajām personām ir jāatklāj vai jāiesniedz *IPT* visi tai nepieciešamie dokumenti un informācija.

126. 68. panta 4. punkts noteica, ka tad, kad *IPT* izskatīja kādu sūdzību, tā bija pilnvarota piešķirt kompensāciju un izdot citus rīkojumus, ko tā uzskata par atbilstošiem, tostarp rīkojumus par jebkura ordera anulēšanu vai atcelšanu, kā arī rīkojumus par tā rezultātā iegūto jebkādu ierakstu iznīcināšanu (67. panta 7. punkts). Ja *IPT* izskatāmā prasība tika apmierināta, *IPT* bija par to jāziņo Ministru prezidentam (68. panta 5. punkts).

127. Saskaņā ar 68. panta 1. punktu *IPT* varēja noteikt pati savu procedūru, lai gan 69. panta 1. punkts paredzēja, ka arī valsts sekretārs var noteikt procesuālos noteikumus.

2. 2000. gada Noteikumi par tiesas izmeklēšanas pilnvarām [Investigatory Powers Tribunal Rules 2000] (turpmāk tekstā – “Noteikumi”)

128. Noteikumus pieņēma valsts sekretārs, lai reglamentētu dažādus *IPT* procedūras aspektus.

129. 9. noteikums ļāva *IPT* jebkurā tiesvedības posmā rīkot mutvārdu paskaidrojumu uzklausīšanu, kurā sūdzības iesniedzējs varēja izteikties, sniegt liecības un izsaukt lieciniekus. Lai gan saskaņā ar 9. noteikumu *IPT* tiesvedībai, tostarp mutvārdu paskaidrojumu uzklausīšanai, bija jābūt slēgtai, lietās “IPT/01/62” un “IPT/01/77” *IPT* pati izlēma, ka atbilstoši vispārīgajam ar 6. noteikuma 1. punktu noteiktajam pienākumam novērst sensitīvas informācijas izpaušanu tā varēja īstenot savu rīcības brīvību, rīkojot atklātu paskaidrojumu uzklausīšanu. Ņemot vērā šo apņemšanos rīkot atklātu paskaidrojumu uzklausīšanu, kad vien tas iespējams, *IPT* ir publicējusi savus svarīgos nolēmumus savā tīmekļa vietnē, ja nepastāv risks, ka tiks atklāta jebkāda informācija, kas var radīt apdraudējumu.

130. Saskaņā ar 11. noteikumu *IPT* varēja iegūt pierādījumus jebkādā formā, pat ja tiesā tie nebūtu pieņemami.

131. Saskaņā ar 6. noteikumu *IPT* bija jāpilda savas funkcijas tā, lai nodrošinātu, ka netiek izpausta informācija, kas ir pretēja sabiedrības interesēm vai apdraud valsts drošību, kā arī nodrošinātu nopietnu noziegumu novēršanu un atklāšanu un Apvienotās Karalistes ekonomisko labklājību vai turpinātu pildīt jebkuru izlūkdienestu funkcijas.

3. Tiesas padomnieks

132. *IPT* varēja iecelt tiesas padomnieku, kas izvirzītu argumentus pieteikumu iesniedzēju vārdā paskaidrojumu uzklausīšanā, kurā viņus nebija iespējams pārstāvēt. “Liberty” tiesvedībā tiesas padomnieks savu funkciju raksturoja šādi:

“Tiesas padomnieks pilda atšķirīgu funkciju [atšķirībā no īpašiem juriskonsultiem slēgtā tiesvedībā konkrētās tiesās] līdzīgi kā *amicus curiae*. Viņa funkcija ir atbalstīt tiesu jebkādā veidā, ko tā uzskata par nepieciešamu. Dažkārt (piemēram, jautājumos, kuros ir pārstāvētas visas puses) tiesa neprecizē, no kādas perspektīvas argumenti tiek izvirzīti. Šādā gadījumā padomniekam ir jāizvirza argumenti, balstoties uz viņa paša veikto attiecīgo juridisko vai faktisko jautājumu analīzi, īpaši akcentējot aspektus, ko puses nav pilnībā precizējušas. Citos gadījumos (jo īpaši tad, ja nav pārstāvētas atsevišķas vai vairākas intereses) tiesa var lūgt padomnieku izvirzīt argumentus no kādas konkrētas perspektīvas (parasti no tās puses vai pušu perspektīvas, kuru intereses kā citādi nav pārstāvētas).”

133. *IPT* šo raksturojumu pieņēma un apstiprināja.

4. Spriedums lietā “R (par “Privacy International” pieteikumu) pret Izmeklēšanas pilnvaru tiesu un citiem” [2019] UKSC 22

134. Šajā spriedumā, kas tika pasludināts 2019. gada 15. maijā, Augstākā tiesa nosprieda, ka *RIPA* 67. panta 8. punkts nebija liedzis *IPT* pārskatīt lēmumu tiesā.

E. Pārraudzība

135. *RIPA* IV daļā bija paredzēts, ka Ministru prezidents ieceļ komisāru sakaru pārtveršanas jautājumos (“*IC* komisārs”) un izlūkošanas dienestu komisāru, kura uzdevums ir pārraudzīt izlūkdienestu darbības.

136. *IC* komisāra uzdevums bija pārskatīt izlūkdienestu, policijas un citu valsts iestāžu veikto sakaru pārtveršanu un sakaru datu iegūšanu un izpaušanu. Pārskatot uzraudzības praksi, *IC* komisāram un viņa inspektoriem bija piekļuve visiem atbilstošajiem dokumentiem, tostarp konfidenciāliem materiāliem, savukārt visām pārtveršanas darbībās iesaistītajām personām bija pienākums izpaust viņam jebkuru viņam nepieciešamo materiālu. Pārtveršanas aģentūru pienākums uzturēt reģistrus nodrošināja, ka *IC* komisārs varēja efektīvi piekļūt informācijai par veiktajām uzraudzības darbībām. Pēc katras pārbaudes attiecīgās valsts iestādes vadītājam tika nosūtīts ziņojums, kurā sniegti formāli ieteikumi un kurš uzlika valsts iestādei par pienākumu divu mēnešu laikā sniegt atbildi, lai apstiprinātu, vai un kādā apmērā ieteikumi tikuši īstenoti. Komisārs reizi pusgadā ziņoja Ministru prezidentam par savu funkciju izpildi un sagatavoja gada ziņojumu. Šis ziņojums bija publisks dokuments (ar nosacījumu, ka konfidenciālie pielikumi netiek izpausti), ko iesniedza parlamentam.

137. Izlūkdienestu komisārs pēc tam nodrošināja neatkarīgu ārēju pārraudzību attiecībā uz izlūkdienestu un Aizsardzības ministrijas struktūru iejaukšanās pilnvaru īstenošanu. Viņš arī iesniedza Ministru prezidentam gada ziņojumus, kas bija iesniegti parlamentam.

138. Ar Izmeklēšanas pilnvaru likumu (skat. turpmāk 183.–190. punktu) šie noteikumi tika atcelti, ciktāl tie attiecās uz Angliju, Skotiju un Velsu, un 2017. gada septembrī izmeklēšanas pilnvaru pārraudzības funkciju pārņēma Izmeklēšanas pilnvaru komisāra birojs (turpmāk tekstā – “*IPCO*”). *IPCO* veido aptuveni piecpadsmit tiesas komisāri no pašreizējo un nesen atvaļināto Augstās tiesas, Apelācijas tiesas un Augstākās tiesas tiesnešu vidus, Tehnisko padomdevēju grupa, kuras sastāvā ir zinātniski eksperti, un gandrīz piecdesmit amatpersonas, tostarp inspektori, advokāti un sakaru eksperti.

F. Izlūkdienestu pārtveršanas darbību pārskatīšana

1. Parlamenta Izlūkošanas un drošības komiteja (turpmāk tekstā – “ISC”), 2013. gada jūlija paziņojums par GCHQ veikto iespējamo sakaru pārtveršanu, izmantojot ASV programmu “PRISM” [July 2013 Statement on GCHQ’s alleged interception of communications under the US PRISM programme]

139. *ISC* sākotnēji izveidoja saskaņā ar *ISA*, lai pārbaudītu *MI5*, *MI6* un *GCHQ* politiku, pārvaldi un izdevumus. Tomēr kopš 2013. gada Likuma par tiesiskumu un drošību [*Justice and Security Act 2013*] ieviešanas *ISC* tika nepārprotami piešķirts Parlamenta komitejas statuss, tai tika piešķirtas lielākas pilnvaras un tās kompetence tika izvērsta, iekļaujot tajā operatīvās darbības pārraudzību un plašākas Valdības izlūkošanas un drošības darbības. Saskaņā ar 2013. gada Likuma par tiesiskumu un drošību 1.–4. pantu tās sastāvā bija deviņi locekļi no abām Parlamenta palātām un šiem locekļiem, pildot savas funkcijas, tika nodrošināta piekļuve konfidenciālam materiālam.

140. Pēc tam, kad Edvards Snoudens bija atklājis informāciju, *ISC* izmeklēja *GCHQ* piekļuvi to sakaru saturam, kas bija pārtverti, izmantojot Amerikas Savienoto Valstu programmu “PRISM”, kā arī pārbaudīja tiesisko regulējumu, kas reglamentē šādu piekļuvi, un pasākumus, ko *GCHQ* īstenoja ar savu ārvalstu kolēģi saistībā ar informācijas apmaiņu. Izmeklēšanas gaitā *ISC* saņēma no *GCHQ* detalizētus pierādījumus un apsprieda programmu ar *NSA*.

141. *ISC* secināja, ka apgalvojumi par to, ka *GCHQ* bija pārkāpusi Apvienotās Karalistes tiesību aktus, izmantojot programmu “PRISM”, lai piekļūtu privātu sakaru saturam, bija nepamatoti, jo *GCHQ* bija izpildījusi tās likumā noteiktos pienākumus, kas paredzēti *ISA*. Tā arī konstatēja, ka ik reizi, kad *GCHQ* pieprasīja informāciju no Amerikas Savienotajām Valstīm, jau bijis izdots Valdības ministra parakstīts pārtveršanas orderis.

2. Privātums un drošība – moderns un pārskatāms tiesiskais regulējums

142. Balstoties uz 2013. gada jūlija paziņojumu, *ISC* veica padziļinātu izlūkdienestu spēju izmeklēšanu. Tās ziņojums, kurā bija iekļauts nepieredzēti daudz informācijas par izlūkdienestu iejaukšanās pilnvarām, tika publicēts 2015. gada 12. martā.

143. *ISC* guva pārliecību, ka Apvienotās Karalistes izlūkdienestu un drošības dienestu mērķis nebija apiet likumu, tostarp 1998. gada Cilvēktiesību likumā noteiktās prasības, kuras reglamentēja visas to darbības. Tomēr tā uzskatīja, ka, tā kā tiesiskais regulējums izstrādāts fragmentāri, tas bija pārlieku sarežģīts. Tādēļ *ISC* bija nopietnas bažas par pārskatāmības trūkumu, kas nebija sabiedrības interesēs. Līdz ar to tās galvenais ieteikums bija aizstāt esošo tiesisko regulējumu ar jaunu parlamenta likumu, kurā skaidri izklāstītas izlūkdienestiem pieejamās iejaukšanās pilnvaras, nolūki, kādiem varētu tās īstenot, un atļauja, kas nepieciešama šādu pilnvaru īstenošanai.

144. Attiecībā uz *GCHQ* masveida pārtveršanas pilnvarām veiktā izmeklēšana liecināja, ka izlūkdienestiem nebija juridisku pilnvaru, resursu, tehnisko iespēju vai vēlmes pārtvert jebkurus Lielbritānijas pilsoņu sakarus vai interneta sakarus kopumā. Līdz ar to *GCHQ* nebija lasījusi katras Apvienotajā Karalistē esošās personas e-pasta ziņojumus. Gluži pretēji, *GCHQ* masveida pārtveršanas sistēmas tika izmantotas tikai ļoti mazai nesēju daļai, kas veidoja internetu, un *ISC* guva pārliecību, ka *GCHQ* bija piemērojusi filtrēšanas un atlasīšanas līmeņus, tā ka tika savākts vienīgi noteikts daudzums materiāla saistībā ar šiem nesējiem. Turklāt turpmākie specifiskie meklējumi nodrošināja, ka analītiķiem pārbaudei tika nodota vienīgi informācija, kurai, visticamāk, bija visaugstākā izlūkošanas vērtība, tādēļ attiecīgās personas faktiski aplūkoja tikai niecīgu daļu no visas savāktās informācijas.

145. Attiecībā uz interneta sakariem *ISC* uzskatīja, ka “iekšējo” un “ārējo” sakaru nodalīšana bija mulsinoša un tā nebija pārskatāma. Tādēļ tā ierosināja Valdībai publicēt paskaidrojumu par to, kuri interneta sakari ietilpa attiecīgajā kategorijā. Tomēr veiktā izmeklēšana liecināja, ka masveida pārtveršanu nevarēja izmantot, lai pārtvertu Apvienotajā Karalistē esošas personas sakarus, nesaņemot īpašu atļauju, kuru parakstījis valsts sekretārs un kurā norādīts attiecīgās personas vārds un uzvārds.

146. *ISC* piebilda, ka 8. panta 4. punktā noteiktais orderis bijis ļoti rezumējošs. Ciktāl tam pievienotajā apliecinājumā bija norādītas to sakaru kategorijas, ko varētu pārbaudīt, šīs kategorijas bija formulētas ļoti vispārīgi (piemēram, “materiāls, kas sniedz izlūkdatus par terorismu (kā noteikts 2000. gada Terorisma apkarošanas likumā (ar attiecīgajiem grozījumiem)), tostarp, bet ne tikai, teroristu organizācijām, teroristiem, aktīviem piekritējiem, uzbrukumu plānošanu, līdzekļu vākšanu”). Tā kā apliecinājums bija formulēts tik vispārīgi, *ISC* šaubījās, vai to vajadzētu paturēt noslēpumā vai arī pārredzamības nolūkos publicēt.

147. Lai gan 8. panta 4. punktā minētajā apliecinājumā ir noteiktas vispārīgās informācijas kategorijas, kuras var pārbaudīt, *ISC* konstatēja, ka praksē pārbaudāmos sakarus noteica tieši datu nesēju atlase un vienkāršu selektoru un meklēšanas kritēriju piemērošana. Tādēļ *ISC* lūgusi ministrus un/vai komisārus šīs kategorijas rūpīgi pārbaudīt un pārskatīt. Tomēr *ISC* iesniegtie pierādījumi liecināja, ka ne ministriem, ne komisāriem šie jautājumi nav šķituši svarīgi. Tādēļ *ISC* ieteica noteikt *IC* komisāram likumā paredzētu pienākumu pārskatīt dažādos masveida pārtveršanā izmantotos atlases kritērijus, lai nodrošinātu, ka tie izriet tieši no apliecinājuma un spēkā esošajām valsts drošības prasībām.

148. *ISC* norādīja, ka sakaru datiem ir liela nozīme lielākajā daļā izlūkdienestu izmeklēšanas pasākumu, proti, tos bijis iespējams analizēt, lai noskaidrotu iezīmes konkrētai rīcībai internetā, kas saistīta ar tādām darbībām kā uzbrukumu plānošana, lai izveidotu saiknes, palīdzētu pastiprināti pievērst uzmanību personām, kuras varētu radīt draudus, nodrošinātu, ka ir atbilstoši noteikts pārtveršanas mērķis, un salīdzinoši ātri informētu tīklus un asociācijas. Tie bija īpaši noderīgi izmeklēšanas agrīnajos posmos, kad izlūkdienestiem bija jānoskaidro, vai ar mērķi asociētās personas bija saistītas ar attiecīgo plānu (un līdz ar to bija jāveic papildu izmeklēšana) vai arī tās bija nevainīgas. Iekšlietu departamenta valsts sekretārs apgalvoja, ka “tiem bijusi svarīga loma ikvienā Drošības dienesta terorisma apkarošanas operācijā, kas īstenota pēdējo desmit gadu laikā”. Tomēr *ISC* pauda bažas par jēdziena “sakaru dati” definīciju. Lai gan *ISC* atzina, ka ir noteikta sakaru datu kategorija, kura ir mazāk aizskaroša nekā saturs un kurai līdz ar to nav jānodrošina tāda paša līmeņa aizsardzība, tā uzskatīja, ka ir izveidotas konkrētas sakaru datu kategorijas, kuras var atklāt daudz aizskarošas informācijas par personas privāto dzīvi, tādēļ tām jāpiemēro nopietnāki drošības pasākumi.

149. Visbeidzot, *ISC* attiecībā uz *IPT* skaidri atzina, cik svarīgas ir valsts pārsūdzības tiesības.

3. Ziņojums “Uzticības jautājums” – neatkarīgā terorisma apkarošanas tiesiskā regulējuma pārskatītāja ziņojums par izmeklēšanas pilnvaru pārskatīšanu“ [“A Question of Trust”: Report of the Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation] (turpmāk tekstā – “Andersona [Anderson] ziņojums”)

150. Neatkarīgais terorisma apkarošanas tiesiskā regulējuma pārskatītājs ir persona, kura rīkojas pilnībā neatkarīgi no Valdības un kuru ieceļ iekšlietu sekretārs un valsts kase uz trīs gadu termiņu, ko iespējams atjaunot. Viņa uzdevums ir ziņot iekšlietu sekretāram un parlamentam par terorisma apkarošanas tiesību aktu darbību Apvienotajā Karalistē. Šos ziņojumus iesniedz parlamentam, lai informētu sabiedrību un sniegtu informāciju politiskajām debatēm.

151. Andersona ziņojumā, kas tika iesniegts parlamentam un publicēts 2015. gada 11. jūnijā un tika nosaukts par godu tābrīža neatkarīgajam terorisma apkarošanas tiesiskā regulējuma pārskatītājam Deividam Andersonam [*David Anderson*] Q. C., bija izvirzīts konkrēts mērķis, proti, informēt sabiedrību un sniegt informāciju politiskajām debatēm par draudiem Apvienotajai Karalistei, pasākumiem, kas nepieciešami šo apdraudējumu novēršanai, ieviestajiem drošības pasākumiem, lai aizsargātu personas tiesības uz privātās dzīves neaizskaramību, izaicinājumiem mainīgo tehnoloģiju kontekstā, problēmām saistībā ar pārskatāmību un pārraudzību, kā arī par nepieciešamību izstrādāt jaunu vai grozīt jau esošo tiesisko regulējumu. Veicot pārskatīšanu, neatkarīgajam pārskatītājam bija neierobežota piekļuve atbildīgajiem Valdības departamentiem un valsts iestādēm visaugstākajā drošības pielaides līmenī. Viņš arī sadarbojās ar pakalpojumu sniedzējiem, neatkarīgajiem tehniskajiem ekspertiem, nevalstiskajām organizācijām, akadēmiķiem, advokātiem, tiesnešiem un reglamentējošajām institūcijām.

152. Neatkarīgais pārskatītājs bija norādījis, ka izmeklēšanas pilnvaras reglamentējošais tiesiskais regulējums “izstrādāts fragmentāri”, līdz ar to “tikai daži [tiesību akti] ir vēl grūtāk uztverami nekā *RIPA* un ap tiem “riņķojošie satelīti””.

153. Attiecībā uz sakaru datu nozīmi viņš norādīja, ka tie ļāva izlūkdienestiem gūt priekšstatu par attiecīgā subjekta darbībām un bija ārkārtīgi svarīgi, sniedzot informāciju par noziedzīgām un terorisma darbībām. Ar tiem bija iespējams identificēt mērķus turpmākajam darbam, kā arī tie palīdzēja noteikt, vai attiecīgā persona bija pilnībā nevainīga. Īpaši svarīga bija spēja izmantot sakaru datus (ja tas atzīts par nepieciešamu un samērīgu), lai:

a) sasaistītu kādu personu ar kādu kontu vai darbību (piemēram, tīmekļa vietnes apmeklēšana vai e-pasta ziņojuma nosūtīšana), noskaidrojot IP adresi;

b) noskaidrotu kādas personas atrašanās vietu, parasti ar mobilā tālruņa vai *GPRS* datu palīdzību;

c) noskaidrotu, kā aizdomās turamie vai cietušie sazinājušies (proti, ar kādu lietotņu vai pakalpojumu starpniecību);

d) novērotu noziedzību tiešsaistē (piemēram, noskaidrojot tīmekļa vietnes, kuras apmeklētas terorisma, bērnu seksuālas izmantošanas vai šaujamieroču vai nelegālo narkotiku iegādes nolūkos) un

e) mērķtiecīgi izmantotu datus (piemēram, lai noskaidrotu, kur, kad un ar ko kāda persona sazinājusies vai ko tā paziņojusi, kā tikusi piegādāta ļaunprogrammatūra vai noticis pakalpojumatteices uzbrukums, un lai apstiprinātu citus pierādījumus).

154. Turklāt sakaru datus varēja analizēt ātri, līdz ar to padarot tos ārkārtīgi noderīgus ātras reaģēšanas operācijās, un sakaru datu izmantošana varētu vai nu radīt nepieciešamību īstenot daudz aizskarošākus pasākumus, vai arī sniegt informāciju, kuras dēļ citi pasākumi nebūtu vajadzīgi.

155. Neatkarīgā pārskatītāja priekšlikumus reformai var apkopot šādi:

a) izstrādāt visaptverošu un saprotamu jaunu tiesību aktu, kas aizstāj “pašreizējo pilnvaru pārpilnību” un paredz skaidrus ierobežojumus un drošības pasākumus jebkādām iejaukšanās pilnvarām, kuras valsts iestādēm, iespējams, nāktos izmantot;

b) pārskatīt un precizēt jēdzienu “saturs” un “sakaru dati” definīcijas;

c) saglabāt drošības dienestu un izlūkdienestu pilnvaras masveidā apkopot pārtverto materiālu un saistītos sakaru datus, taču vienīgi atbilstoši stingriem papildu drošības pasākumiem, tostarp jaunās Neatkarīgās uzraudzības un izlūkošanas komisijas (turpmāk tekstā – “*ISIC*”) tiesas komisāra atļaujai attiecībā uz visiem orderiem;

d) orderim pievienotajā apliecinājumā formulēt mērķus, kādiem materiāls vai dati nepieciešami, atsaucoties uz konkrētām operācijām vai misijas nolūkiem (piemēram, “*ISIL* uzbrukuma plānošana Irākā/Sīrijā pret Apvienoto Karalisti”);

e) izveidot jaunu masveida pārtveršanas ordera formu, kas attiektos vienīgi uz sakaru datu ieguvi un konkrētos gadījumos būtu samērīgs risinājums;

f) *ISIC* jāpārņem izlūkošanas pārraudzības funkcijas, un tai jābūt publiski pieejamai, pārredzamai un pieejamai plašsaziņas līdzekļiem un

g) *IPT* jābūt iespējai iesniegt paziņojumus par neatbilstību, un tās nolēmumi jāpārbauda kasācijas kārtībā.

4. Ziņojums “Demokrātiska atļauja rīkoties – ziņojums par neatkarīgas uzraudzības pārskatīšanu” [A Democratic Licence to Operate: Report of the Independent Surveillance Review] (turpmāk tekstā – “ISR”)

156. *ISR* pēc toreizējā Ministru prezidenta vietnieka lūguma sagatavoja neatkarīgā ideju laboratorija “Royal United Services Institute”, daļēji atbildot uz Edvarda Snoudena atklāto informāciju. Tās uzdevums bija aplūkot Apvienotās Karalistes uzraudzības programmu likumību un to režīmu efektivitāti, kas tās pārvaldīja, kā arī ierosināt reformas, kas varētu būt nepieciešamas, lai aizsargātu gan personas tiesības uz privātās dzīves neaizskaramību, gan nepieciešamās policijas, drošības dienestu un izlūkdienestu pilnvaras.

157. Pēc pārskatīšanas veikšanas *ISR* nesniedza pierādījumus tam, ka Lielbritānijas valdība apzināti rīkojās pretlikumīgi, pārtverot privātos sakarus, vai ka Valdība izmantojusi iespēju apkopot datus masveidā, lai nodrošinātu tai pastāvīgu iejaukšanos Lielbritānijas pilsoņu tiesībās uz privātās dzīves neaizskaramību. Tomēr tā sniedza pierādījumus, ka pašreizējais tiesiskais regulējums, kas pieļāva sakaru pārtveršanu, bija neskaidrs, atpalicis no sasniegumiem sakaru tehnoloģiju jomā un nebija apmierinošs ne Valdībai, ne sabiedrībai. Tādēļ tajā secināja, ka nepieciešams jauns, visaptverošs un skaidrāks tiesiskais regulējums.

158. Tajā īpaši atbalstīts gan *ISC*, gan Andersona ziņojumā izklāstītais viedoklis, ka, lai gan pašreizējās uzraudzības pilnvaras ir nepieciešamas, ir vajadzīgs gan jauns tiesiskais regulējums, gan pārraudzības režīms. Tajā arī norādīts, ka jēdzienu “saturs” un “sakaru dati” definīcijas jaunā tiesiskā regulējuma izstrādes ietvaros ir jāpārskata, lai tās varētu skaidri noteikt šajā tiesību aktā.

159. Attiecībā uz sakaru datiem ziņojumā norādīts, ka personai bija pieejami lielāki apjomi salīdzinājumā ar saturu, jo katru satura daļu aptver vairākas sakaru datu vienības. Turklāt datu kopu apkopošana varētu sniegt ļoti precīzu priekšstatu par personas dzīvi, ņemot vērā, ka ar pietiekami daudz neapstrādātiem datiem, algoritmiem un jaudīgiem datoriem iespējams ģenerēt skaidru priekšstatu par personu un tās rīcības iezīmēm, pat nepiekļūstot saturam. Tāpat arvien sarežģītāku šifrēšanas metožu izmantošana padarījusi saturu arvien grūtāk pieejamu.

160. Ziņojumā arī norādīts, ka ir jāsaglabā drošības dienestu un izlūkdienestu pilnvaras vākt un analizēt pārtverto materiālu masveidā, taču ar stingrākiem aizsardzības pasākumiem, kā rekomendēts Andersona ziņojumā. Jo īpaši tajā atzīts, ka masveida pārtveršanas orderos jāietver daudz detalizētāka informācija un ka attiecībā uz tiem jāsaņem tiesas atļauja, izņemot tad, kad pieprasījums iesniegts steidzamības kārtā.

161. Papildus tajā atbalstīts gan *ISC*, gan Andersona ziņojumā apgalvotais, ka jāparedz dažādi orderu veidi sakaru un saistīto datu pārtveršanai un iegūšanai. Tajā ierosināts, ka orderi, ko izdod smagu noziegumu un organizētas noziedzības atklāšanai vai novēršanai, vienmēr jāapstiprina tiesas komisāram, savukārt orderi, ko izdod valsts drošības interesēs, jāapstiprina valsts sekretāram un tiesā jāpārskata tiesas komisāram.

162. *ISR* attiecībā uz *IPT* ieteica rīkot atklātu paskaidrojumu uzklausīšanu, izņemot tad, kad tās ieskatā privāta vai slēgta paskaidrojumu uzklausīšana ir nepieciešama taisnīguma vai citu apzināmu sabiedrības interešu dēļ. Turklāt *IPT* jābūt iespējai pārbaudīt tai iesniegtos slepenos pierādījumus, iespējams, ieceļot īpašo padomnieku. Visbeidzot, tajā atbalstīts *ISC* un Andersona ziņojumā apgalvotais, ka valsts pārsūdzības tiesības ir svarīgas un ir jāņem vērā turpmākajā tiesiskajā regulējumā.

5. Ziņojums par masveida pārtveršanas pilnvaru pārskatīšanu

163. Masveida pārtveršanas pilnvaru pārskatīšana tika veikta 2016. gada maijā, lai izvērtētu operatīvo pamatojumu četrām masveida pārtveršanas pilnvarām, ko paredzēja toreizējais Izmeklēšanas pilnvaru likumprojekts [*Investigatory Powers Bill*] (tagad 2016. gada Izmeklēšanas pilnvaru likums, skat. turpmāk 183.–190. punktu). Šīs pilnvaras attiecās uz sakaru datu masveida pārtveršanu un iegūšanu, masveida pārtveršanas iekārtu traucējumiem un personas datu kopu masveida iegūšanu.

164. Neatkarīgais terorisma apkarošanas tiesiskā regulējuma pārskatītājs veica atkārtotu pārskatīšanu. Lai veiktu šo pārskatīšanu, viņš piesaistīja trīs komandas locekļus, kuriem visiem bija nepieciešamā drošības pielaide, lai piekļūtu ļoti konfidenciāliem materiāliem, tostarp personu ar nepieciešamo tehnisko pieredzi, lai izprastu *GCHQ* izmantotās sistēmas, paņēmienus un to izmantošanas veidus, kā arī izmeklētāju ar slepenu, tostarp *GCHQ* radītu, izlūkdatu lietotāja pieredzi un vecāko neatkarīgo konsultantu ar nepieciešamajām prasmēm un pieredzi, lai kriminālistiskā veidā izpētītu pierādījumus un situāciju analīzi, ko iesnieguši drošības dienesti un izlūkdienesti.

165. Šīs pārskatīšanas gaitā grupa aktīvi un detalizēti kontaktējās ar izlūkdienestiem visos līmeņos, kā arī ar attiecīgajām pārraudzības iestādēm (tostarp *IPT* un tiesas padomnieku), NVO un neatkarīgiem tehniskajiem ekspertiem.

166. Lai gan Izmeklēšanas pilnvaru likumprojekts tika pārskatīts, vairāki tā konstatējumi saistībā ar masveida pārtveršanu attiecās uz šo lietu. Pārbaudot lielu apjomu konfidenciāla materiāla, pēc pārskatīšanas tika secināts, ka masveida pārtveršana ir svarīga pilnvara, pirmkārt, tāpēc, ka teroristu, noziedzīgo un naidīgo ārvalstu izlūkdienestu rīcība ir kļuvusi daudz rafinētāka, lai tos nevarētu atklāt ar tradicionāliem līdzekļiem, un, otrkārt, tāpēc, ka globālā interneta iezīmju dēļ maršruts, pa kuru konkrētie sakari tiek pārraidīti, bija kļuvis ļoti neparedzams. Pārskatīšanas grupa izvērtēja masveida pārtveršanas alternatīvas (tostarp mērķētu pārtveršanu, kā arī cilvēkresursu un komerciālo kiberaizsardzības produktu izmantošanu), taču tā secināja, ka neviena alternatīva vai alternatīvu kombinācija nebūtu pietiekama, lai aizstātu masveida pārtveršanas pilnvaras kā nepieciešamo izlūkdatu iegūšanas metodi.

6. Uzbrukumi Londonā un Mančestrā no 2017. gada marta līdz 2017. gada jūnijam – MI5 un policijas iekšējo pārskatu neatkarīgs novērtējums

167. Pēc četriem teroristu uzbrukumiem īsā laika posmā no 2017. gada marta līdz jūnijam, kuros gāja bojā aptuveni trīsdesmit seši nevainīgi cilvēki un vēl gandrīz 200 tika ievainoti, iekšlietu sekretārs lūdza nesen atvaļināto neatkarīgo terorisma apkarošanas tiesiskā regulējuma pārskatītāju Deividu Andersonu Q. C. iesaistīties, lai izvērtētu iesaistītās policijas un izlūkdienestu slepenos iekšējos pārskatus. Uzbrukumu kontekstā ziņojumā bija norādīts turpmāk minētais:

“1.4. Pirmkārt, Apvienotais terorisma analīzes centrs (turpmāk tekstā – “*JTAC*”) ***apdraudējuma līmeni*** Apvienotajā Karalistē no tā dēvētās “starptautiskā terorisma” perspektīvas (praksē islāmistu terorisma neatkarīgi no tā, vai tas ir radīts iekšzemē vai ārvalstīs) no 2014. gada augusta novērtējis kā NOPIETNU, norādot, ka islāmistu teroristu uzbrukumi Apvienotajā Karalistē ir “ļoti iespējami”. Komentētājiem, kuriem ir piekļuve attiecīgajiem izlūkdatiem, vienmēr ir bijis skaidrs, ka šis novērtējums ir reālistisks. Tas atsaucies arī uz mazākiem, bet joprojām nāvējošiem galēji labējā spārna (“*XRW*”) terorisma draudiem, kā piemēru minot parlamenta deputāta Džo Koksa [*Jo Cox*] slepkavību 2016. gada jūnijā un neonacistu grupas “National Action” aizliegšanu 2016. gada decembrī.

1.5. Otrkārt, ***pieaugošais*** islāmistu terorisma ***draudu līmenis*** ir pārsteidzošs. *MI5* ģenerāldirektors Endrjū Pārkers [*Andrew Parker*] 2017. gada oktobrī runāja par “dramatisku draudu pieaugumu šajā gadā”, kas ir “vislielākais temps, kāds manos 34 karjeras gados piedzīvots”. Lai gan islāmistu terorisma izraisītie nāves gadījumi galvenokārt novērojami Āfrikā, Tuvajos Austrumos un Dienvidāzijā, draudi pēdējā laikā ir pieauguši visā Rietumu pasaulē un tiek raksturoti kā “īpaši izkliedēti un daudzveidīgi Apvienotajā Karalistē”. Vēl nav zināms, vai tā dēvētās Islāma valsts fiziskais sabrukums Sīrijā un Irākā šo tendenci ietekmēs pozitīvi vai negatīvi.

1.6. Treškārt, ***uzbrucējiem*** ir daudz kopīgu iezīmju. (..)

1.7. Ceturtkārt, lai gan pirmo trīs uzbrukumu ***mērķi*** neizpaudās to pašreizējā apmērā, tiem bija ļoti līdzīgas iezīmes ar citu neseno uzbrukumu mērķiem Rietumos, proti, politiskie centri (piemēram, Oslo 2011. gadā, Otava 2014. gadā, Brisele 2016. gadā), koncertu apmeklētāji, skaļu pasākumu apmeklētāji un pūļi (piemēram, Orlando 2016. gadā, Parīze 2016. gadā, Barselona 2017. gadā), kā arī policisti (piemēram, Melburna 2014. gadā, Berlīne 2015. gadā un Čarleroja 2016. gadā). Ir precedenti arī uzbrukumiem ticīgiem musulmaņiem, pārejot no naida noziegumiem uz terorismu, piemēram, Muhameda Salēma [*Mohammed Saleem*] nogalināšana Rietummidlendā 2013. gadā.

1.8. Piektkārt, teroristu uzbrukumu ***modus operandi*** (MO) gadu gaitā ir dažādojies un vienkāršojies, jo “Daesh” ir izmantojis savus plašos propagandas centienus, lai iedvesmotu, nevis vadītu teroraktus Rietumos. Aplūkotie uzbrukumi bija tipiski laikam un vietai.

a) Atšķirībā no pēdējā desmitgadē raksturīgajām vērienīgajām organizētajām islāmistu sazvērestībām, visus četrus uzbrukumus pastrādāja ***atsevišķas personas*** vai ***mazas grupas***, kas maz liecina par detalizētu plānošanu vai precīzu mērķa izraudzīšanu.

b) Stingrie šaujamieroču kontroles pasākumi Apvienotajā Karalistē ir iemesls tam, ka kriminālu grupējumu un teroristu noziegumos biežāk tiek izmantoti ***aukstie ieroči***, nevis šaujamieroči.

c) Kopš kravas automobilis Nicā (2016. gada jūlijā) nogalināja 86 nevainīgus cilvēkus, kā ieročus arvien vairāk izmanto ***transportlīdzekļus***, ko izmantoja trīs no četriem aplūkotajiem uzbrukumiem.

d) Transportlīdzekli ***apvienojumā*** ar aukstajiem ieročiem, kā tas notika uz Vestminsteres un Londonas tilta, izmantoja, lai nogalinātu kareivi Lī Rigbiju [*Lee Rigby*] (Vūlvičā 2013. gadā).

e) ***Sprāgstvielas***, kas tika izmantotas Mančestrā, bija vispopulārākais ierocis, ko islāmistu teroristi izmantoja uzbrukumos Eiropā no 2014. līdz 2017. gadam. Pierādīts, ka sprāgstvielu *TATP* iespējams izgatavot (to sekmē pirkumi un montāžas instrukcijas tiešsaistē) vieglāk, nekā reiz tika uzskatīts.”

7. 2016. gada Komisāra sakaru pārtveršanas jautājumos ziņojums

168. *IC* komisārs norādīja, ka, veicot pārtveršanu atbilstoši 8. panta 4. punktā noteiktajam orderim, pārtveršanas aģentūrai ir jāizmanto savas zināšanas par veidu, kādā tiek maršrutēti starptautiskie sakari, kā arī regulāri jāpārbauda attiecīgie sakaru kanāli, lai apzinātu tos individuālos sakaru nesējus, kuri, visticamāk, saturēs ārējos sakarus, kas atbildīs valsts sekretāra apliecinātajiem materiāla aprakstiem saskaņā ar 8. panta 4. punktu. Tai arī jāveic pārtveršana tā, lai ierobežotu tādu sakaru apkopošanu, kas nav ārēji sakari, līdz minimumam, kas atbilst nepieciešamo ārējo sakaru pārtveršanas mērķim.

169. Viņš piebilda, ka, pirms analītiķi var lasīt, aplūkot vai klausīties materiālu, ir jāpamato, kāpēc šāda piekļuve materiālam ir nepieciešama un atbilstoša 16. pantam un kādēļ šāda piekļuve ir samērīga. Pārbaudes un auditi liecināja, ka, lai gan atlasīšanas procedūra bija veikta piesardzīgi un apzinīgi, tā balstījās uz analītiķu profesionālu spriedumu, viņu mācībām un vadības pārraudzību.

170. Saskaņā ar ziņojumu 2016. gadā tika izdoti 3007 orderi un valsts sekretārs noraidīja piecus pieteikumus. *IC* komisāra ieskatā šie skaitļi neraksturo kritiski svarīgo kvalitātes nodrošināšanas funkciju, ko sākotnēji pildījušas pārtveršanas aģentūras vai orderi piešķirošās nodaļas darbinieki un juristi (orderi piešķirošās nodaļas sniegušas valsts sekretāram neatkarīgu viedokli un pārbaudījušas pieteikumus ordera saņemšanai un atjaunošanai pirms atļaujas došanas, lai nodrošinātu, ka tie ir (un paliek) nepieciešami un samērīgi). Pamatojoties uz šīm pārbaudēm, viņš guva pārliecību, ka nelielais noraidīto pieteikumu skaits liecināja par pārdomātu pilnvaru izmantošanu.

171. Ierasta pārtveršanas aģentūras pārbaude paredzēja:

* pārskatīt rīcības punktus vai ieteikumus, ņemot vērā iepriekšējo pārbaudi un tās īstenošanu;
* izvērtēt ieviestās sakaru pārtveršanas sistēmas, lai nodrošinātu, ka tās atbilst *RIPA* 1. daļas 1. nodaļas nolūkiem un ka tiek uzturēti visi attiecīgie reģistri;
* pārbaudīt atlasītos pieteikumus pārtveršanas veikšanai, lai izvērtētu, vai tie vispār bija nepieciešami un vai pieprasījumi atbilda nepieciešamības un samērīguma prasībām;
* intervēt par attiecīgo lietu atbildīgās amatpersonas, analītiķus un/vai lingvistus, kas bija iesaistīti izmeklēšanā vai operācijās, lai izvērtētu, vai pārtveršana un visa materiāla iegūšanas pamatojums bija samērīgi;
* pārbaudīt jebkurus steidzamības kārtā sniegtos mutvārdu apstiprinājumus, lai pārliecinātos, ka process bija pamatots un atbilstošs;
* pārskatīt tos gadījumus, kad sakari, uz ko attiecas juridiska konfidencialitāte vai kas ir citādi konfidenciāla informācija, ir pārtverti un saglabāti, kā arī jebkādus gadījumus, kad attiecībā pret advokātu bija uzsākta izmeklēšana;
* pārskatīt *RIPA* 15. un 16. pantā noteikto drošības pasākumu un citu pasākumu atbilstību;
* izmeklēt ieviestās pārtvertā materiāla un saistīto sakaru datu saglabāšanas, uzglabāšanas un iznīcināšanas procedūras un
* pārskatīt ziņotās kļūmes, tostarp pārliecināties, vai ieviestie pasākumi, ar kuriem paredzēts novērst šo kļūmju atkārtošanos, bija pietiekami.

172. Pēc katras pārbaudes inspektori iesniedza ziņojumu, tostarp:

* novērtējumu par to, ciktāl ir ieviesti iepriekšējās novērtēšanas laikā sniegtie ieteikumi;
* pārbaudei atlasīto pārtveršanas dokumentu skaita un veida kopsavilkums, tostarp detalizētu šo orderu sarakstu;
* detalizētus komentārus par visiem orderiem, kas izraudzīti turpmākai pārbaudei un apspriešanai pārbaudes gaitā;
* novērtējumu par kļūmēm, par kurām *IC* komisāra birojam ziņots pārbaudes periodā;
* pārskatu par datu saglabāšanas, uzglabāšanas un iznīcināšanas procedūru pārbaudi;
* pārskatu par citiem politikas vai operatīviem jautājumiem, ko aģentūra vai orderus piešķirošās nodaļas izvirzījušas pārbaudes laikā;
* novērtējumu par to, kā ticis apstrādāts materiāls, uz ko attiecas advokāta un klienta saziņas konfidencialitāte (vai kāds cits konfidenciāls materiāls), un
* vairākus ieteikumus, kuru mērķis ir uzlabot atbilstību un sniegumu.

173. 2016. gadā *IC* komisāra birojs vienu reizi pārbaudīja visas deviņas pārtveršanas aģentūras un divas reizes – četras galvenās orderus piešķirošās nodaļas. Tas kopā ar papildu apmeklējumiem *GCHQ* telpās kopā veidoja divdesmit divus pārbaudes apmeklējumus. Turklāt komisārs un viņa inspektori rīkoja *ad hoc* apmeklējumus aģentūrās.

174. Ieviestās sistēmas pārtveršanas orderu pieprasīšanai un atļaušanai parasti tika pārbaudītas trīs posmos. Pirmkārt, lai iegūtu orderu reprezentatīvo paraugu, inspektori tos atlasīja, ņemot vērā dažādus noziegumu veidus un valsts drošības draudus. Turklāt inspektori galveno uzmanību pievērsa īpaši interesējošiem vai sensitīviem orderiem (piemēram, tiem, kuri radīja būtisku netiešu iejaukšanos, bija spēkā ievērojami ilgu laiku, bija apstiprināti mutiski, attiecās uz juridisku vai kā citādi konfidenciālu sakaru pārtveršanu, kā arī tā dēvētajiem “tematiskajiem” orderiem). Otrkārt, inspektori detalizēti pārbaudīja atlasītos orderus un saistīto dokumentāciju, ar to rūpīgi iepazīstoties pirms pārbaudes veikšanas. Šajā posmā inspektori varēja pārbaudīt analītiķu apgalvojumus par nepieciešamību un samērīgumu, pievienojot selektoru visai pārbaudes sistēmai. Katrs apgalvojums tika analizēts atsevišķi, un tam bija jāatsaucas uz vispārējo prasību par izlūkdatu vākšanas prioritātēm. Treškārt, viņi apzināja tos orderus, darbības vai procesa jomas, kurās bija nepieciešama papildu informācija vai precizējumi, un organizēja attiecīgā operatīvā, juridiskā vai tehniskā personāla intervijas. Ja nepieciešams, viņi pārbaudīja papildu dokumentāciju vai sistēmas, kas saistītas ar šiem orderiem.

175. Divdesmit divās pārtveršanas pārbaudēs tika pārbaudīti kopumā deviņi simti septiņdesmit orderi (sešdesmit viens procents no gada beigās spēkā esošo orderu skaita un trīsdesmit divi procenti no 2016. gadā izdoto jauno orderu kopskaita).

176. Saglabāšanas periodi tiesiskajā regulējumā nebija noteikti, taču aģentūrām bija jāņem vērā *RIPA* 15. panta 3. punkts, kas paredzēja, ka materiāls vai dati ir jāiznīcina, tiklīdz to saglabāšana vairs nav nepieciešama kādam no 15. panta 4. punktā atļautajiem nolūkiem. Ziņojums liecina, ka katrai pārtveršanas aģentūrai bija atšķirīgs viedoklis par to, kas ir atbilstošs pārtvertā materiāla un saistīto sakaru datu saglabāšanas periods. Tāpēc saglabāšanas periodi dažādās pārtveršanas aģentūrās bija atšķirīgi, proti, attiecībā uz saturu tie svārstījās no trīsdesmit dienām līdz vienam gadam, bet attiecībā uz saistītajiem sakaru datiem – no sešiem mēnešiem līdz vienam gadam. Tomēr praksē lielākā daļa satura tika pārskatīta un automātiski dzēsta pēc ļoti īsa laika perioda, ja vien netika veikts īpašs pasākums, lai saturu saglabātu ilgāk tādēļ, ka tas bija nepieciešams.

177. *IC* komisārs uzsvēra, ka viņu “pārsteidza kvalitāte” saistībā ar paziņojumiem par nepieciešamību un samērīgumu, ko analītiķi sniedza, pievienojot selektoru visai pārbaudes sistēmai.

178. Inspektori pārbaužu ziņojumos kopumā sniedza divdesmit astoņus ieteikumus, no kuriem astoņpadsmit attiecās uz pieteikšanās procesu. Vairums ieteikumu šajā kategorijā attiecās uz nepieciešamības, samērīguma un/vai netiešas iejaukšanās pamatojumu pieteikumos vai uz juridiski konfidenciāla vai citādi konfidenciāla materiāla apstrādi, kas saistīts sensitīvām profesijām.

179. 2016. gadā *IC* komisāram kopumā bija ziņots par 108 pārtveršanas kļūmēm. Galvenie pārtveršanas kļūmju cēloņi bija pārmērīga datu apkopošana (parasti tehniskas programmatūras vai aparatūras kļūmes, kas bija par pamatu pārtvertā materiāla un saistīto sakaru datu pārmērīgai apkopošanai), neatļauta atlase/pārbaude, neatbilstoša izplatīšana, pārtveršanas neatcelšana un nepareizo sakaru adreses vai personas pārtveršana.

180. Visbeidzot attiecībā uz izlūkdatiem *IC* komisārs norādīja:

“*GCHQ* sniedza visaptverošu informāciju par apmaiņas pasākumiem, saskaņā ar kuriem “Five Eyes” partneri savās sistēmās var piekļūt *GCHQ* pārtveršanas ordera produkta elementiem. Mani inspektori arī tikās ar “Five Eyes” kopienas pārstāvjiem, un viņiem tika uzskatāmi parādīts, kā citi “Five Eyes” locekļi var pieprasīt piekļuvi *GCHQ* datiem. Piekļuve *GCHQ* sistēmām tiek stingri kontrolēta, un tai ir jābūt pamatotai saskaņā ar uzņēmējas valsts tiesību aktiem un 15./16. pantā noteiktajiem norādījumiem par drošības pasākumiem. Pirms piekļūt *GCHQ* datiem, “Five Eyes” analītiķiem ir jāpabeidz tādas pašas mācības par juridiskajiem aspektiem kā *GCHQ* darbiniekiem.

8. 2016. gada Izlūkdienestu komisāra gada ziņojums

181. Izlūkdienestu komisārs savā ziņojumā par atbilstību Konsolidētajiem norādījumiem izlūkdienestiem un dienesta personālam par aizturēto personu aizturēšanu un nopratināšanu ārvalstīs, kā arī par izlūkdatu nodošanu un saņemšanu saistībā ar aizturētajām personām [*Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees*] norādīja:

“Katra aģentūra sava darba gaitā cieši sadarbojas ar ārvalstu sadarbības partneriem. Tas ietver ikdienas izlūkdatu apmaiņu un dažkārt arī sadarbības operācijas. Esmu guvis pārliecību, ka aģentūras apzinās ietekmi, ko rada darbs ar partneriem, kuri darbojas saskaņā ar dažādām tiesību sistēmām, un jāpiebilst, ka [Apvienotās Karalistes izlūkdienesti], kas darbojas ārvalstīs, rūpīgi piemēro Apvienotās Karalistes tiesību aktu principus, cik vien tas iespējams.

(..)

*GCHQ* cieši sadarbojas ar sadarbības partneriem un iesaistās regulārā izlūkdatu apmaiņā un dažkārt arī kopējā darbā. Šī joma ir sarežģīta gan *GCHQ*, gan *SIS*, kur aģentūru darbinieki sadarbojas ar partneriem, kas piemēro atšķirīgus un dažkārt pat nesaderīgus tiesiskos regulējumus. Mani patīkami pārsteidza *GCHQ* darbinieku centieni gūt pārliecību no partneriem, jo ​​īpaši attiecībā uz konsolidētajiem norādījumiem. Esmu aicinājis *GCHQ* apsvērt iespēju attiecīgajos pieteikumos atsaukties uz vietējiem tiesību aktiem, kas ietekmēs jebkuru partnera darbību.

Es guvu pārliecību, ka *GCHQ* piesardzīgi piemēro konsolidēto vadlīniju principus, un esmu gandarīts, ka izmaiņas, kas veiktas visu diennakti strādājošā personāla mācībās, paaugstina jau tā augsto nosūtīšanas procesa standartu. Jāpiebilst, ka dažkārt *GCHQ* darbinieki vēlāk atjaunināja konsolidētu vadlīniju reģistru, lai precizētu spriedumus vai informāciju. Lai gan ir svarīgi atspoguļot vispilnīgākos pieejamos faktus, es aicināju *GCHQ* ietvert precizējuma punktus papildus reģistra ierakstam, nevis grozīt sākotnējo reģistra ierakstu. *GCHQ* pēc tam apstiprināja, ka šis ieteikums ticis īstenots.

(..)

Ārlietu sekretārs arī ir atbildīgs par ministru pārraudzību gadījumos, kad izmantotas konsolidētās vadlīnijas un aģentūras to plāno turpināt, apmainoties ar izlūkdatiem vai veicot tiešu operāciju. Esmu sniedzis ieteikumu nodrošināt, lai [Ārlietu un sadraudzības lietu birojs] saņemtu jebkuru tādu paziņojumu kopiju, ko *SIS* ieguvis no sadarbības partnera. Es iesaku tos iesniegt ārlietu sekretāram rūpīgai pārbaudei, ņemot vērā visus konsolidētos, ar norādījumiem saistītos argumentus.”

182. Konsolidēto vadlīniju ievērošanas pārraudzība tagad ir jaunā izmeklēšanas pilnvaru komisāra kompetencē. Vadlīnijas pašlaik tiek pārskatītas, jo izlūkdienestu komisārs savā 2015. gada ziņojumā norādīja, ka, lai gan viņš neuzskatīja, ka “konsolidētajās vadlīnijās ir būtiski trūkumi un ka tās neatbilst mērķim”, viņš tomēr norādīja, ka tās “to pašreizējā formā ir izmantotas vairākus gadus un ka tās var uzlabot”.

G. 2016. gada Izmeklēšanas pilnvaru likums

183. Valdība 2016. gada 29. novembrī sniedza oficiālu piekrišanu 2016. gada Izmeklēšanas pilnvaru likumam. Jaunais režīms, kas tika ieviests ar šo likumu, tagad lielākoties darbojas, un lielākā daļa likumā noteikto pilnvaru ir stājušās spēkā 2018. gada laikā.

184. Saskaņā ar 2016. gada likumu masveida pārtveršanas orderis, kas var attiekties gan uz sakaru “saturu”, gan uz “sekundārajiem datiem”, ir jāizdod vismaz valsts drošības interesēs (taču to var izdot arī nozieguma novēršanai vai atklāšanai vai arī Apvienotās Karalistes ekonomiskās labklājības interesēs, ciktāl šīs intereses sasaucas ar valsts drošību). Orderī jānorāda “operatīvie nolūki”, kuriem jebkuru atbilstoši orderim iegūto materiālu var atlasīt, lai to pārbaudītu. Ir izstrādāti detalizēti noteikumi par “operatīvo nolūku” saraksta izveidi, ko veic izlūkdienestu vadītāji. Operatīvo nolūku šajā sarakstā var norādīt tikai ar valsts sekretāra apstiprinājumu. Operatīvo nolūku saraksts jāiesniedz *ISC* reizi trijos mēnešos, bet Ministru prezidentam tas ir jāpārskata vismaz reizi gadā.

185. Pieteikumu masveida pārtveršanas ordera saņemšanai iesniedz izlūkdienesta vadītājs vai arī tas tiek iesniegts izlūkdienesta vadītāja vārdā. Pilnvaras izdot orderi ir jāīsteno valsts sekretāram(-ei) personīgi, un, lemjot par masveida pārtveršanas ordera izdošanu, viņam vai viņai ir jāpiemēro nepieciešamības un samērīguma principi. Ordera izdošanu iepriekš apstiprina tiesas komisārs, kuram ir jāpiemēro tiesas pārskatīšanas (tā dēvētās “dubultās bloķēšanas”) principi. Tāpēc tiesas komisāram pašam jāizvērtē, vai iejaukšanās ir pamatojama kā samērīga saskaņā ar Konvencijas 8. panta 2. punktu.

186. Orderis ir spēkā sešus mēnešus, ja vien tas netiek atcelts vai atjaunots. Ordera atjaunošanu apstiprina tiesas komisārs.

187. Ordera “galvenajam nolūkam” ir jābūt “ar ārvalstīm saistītu sakaru” iegūšanai. Tas ir saziņu saturs, ko personas nosūta vai saņem ārpus Britu salām. Uz pārbaudes nolūkos pārtvertā satura vai “aizsargājamā materiāla” atlasi attiecas “Britu salu drošības pasākumi”, kas nozīmē, ka to jebkurā laikā nevar atlasīt pārbaudei, ja kādi kritēriji, kas izmantoti pārtvertā satura atlasei pārbaudes nolūkos, attiecināmi uz personu, par kuru zināms, ka tā attiecīgajā brīdī atrodas Britu salās, un šo kritēriju izmantošanas mērķis ir identificēt šīs personas nosūtīto vai tai paredzēto sakaru saturu.

188. Ar 2016. gada likumu arī tika noteiktas *IPT* pārsūdzības tiesības, savukārt komisāru sakaru pārtveršanas jautājumos aizstāja jaunais izmeklēšanas pilnvaru komisārs (skat. iepriekš 138. punktu).

189. 2018. gada 8. martā spēkā stājās vairāki jauni prakses kodeksi, tostarp jaunais Sakaru pārtveršanas prakses kodekss (skat. iepriekš 102. punktu).

190. 2016. gada likuma 4. daļa, kas stājās spēkā 2016. gada 30. decembrī, paredzēja pilnvaras izdot “paziņojumus par saglabāšanu” telekomunikāciju operatoriem, kas pieprasa datu saglabāšanu. Pēc “ Liberty” tiesvedības Valdība atzina, ka 2016. gada likuma 4. daļa tās pašreizējā formā neatbilst Eiropas Savienības tiesību aktu prasībām. 4. daļa netika grozīta, un 2018. gada 27. aprīlī Augstā tiesa atzina, ka 4. daļa nav saderīga ar Eiropas Savienības tiesību aktos garantētajām pamattiesībām, jo krimināltiesību jomā uz piekļuvi saglabātajiem datiem neattiecās vienīgi mērķis apkarot “smagu noziegumu”, turklāt piekļuvi saglabātajiem datiem iepriekš nepārskatīja tiesa vai kāda neatkarīga pārvaldes iestāde.

II. PIEMĒROJAMIE STARPTAUTISKIE TIESĪBU AKTI

A. Apvienoto Nāciju Organizācija

191. Ģenerālās asamblejas 2013. gada 18. decembra rezolūcijā Nr. 68/167 noteikts:

“Ģenerālā asambleja,

(..)

4. *aicina* visas valstis:

(..)

*c)* pārskatīt savas procedūras, praksi un tiesību aktus attiecībā uz sakaru uzraudzību, pārtveršanu un personas datu vākšanu, tostarp masveida uzraudzību, pārtveršanu un vākšanu, lai ievērotu tiesības uz privātās dzīves neaizskaramību, nodrošinot visu savu pienākumu pilnīgu un efektīvu izpildi saskaņā ar starptautiskajām cilvēktiesībām;

*d)* izveidot jaunus vai uzturēt pašreizējos neatkarīgos, efektīvos valsts pārraudzības mehānismus, kas pēc vajadzības spēj nodrošināt pārredzamību un atbildību par valsts sakaru uzraudzību, to pārtveršanu un personas datu vākšanu. (..)”

B. Eiropas Padome

1. Eiropas Padomes 1981. gada Konvencija par personu aizsardzību attiecībā uz personas datu automātisko apstrādi

192. Konvencija, kas attiecībā uz Apvienoto Karalisti stājās spēkā 1987. gada 1. decembrī, nosaka datu aizsardzības standartus automātiskās personas datu apstrādes jomā publiskajā un privātajā sektorā. Ciktāl tas attiecas uz šo lietu, Konvencijā noteikts:

**Preambula**

“Eiropas Padomes dalībvalstis, kas parakstījušas šo Konvenciju,

uzskatīdamas, ka Eiropas Padomes mērķis ir panākt lielāku vienotību tās dalībnieku starpā, it īpaši balstoties uz tiesiskas valsts principiem, kā arī cilvēktiesību un pamatbrīvību ievērošanu;

uzskatīdamas, ka ir vēlams paplašināt katras personas tiesību un pamatbrīvību aizsardzību, it īpaši tiesības uz privātās dzīves neaizskaramību, ņemot vērā arvien pieaugošo automātiski apstrādāto personas datu plūsmu pāri robežām;

vēlreiz vienlaicīgi apstiprinādamas savu apņemšanos nodrošināt informācijas brīvību neatkarīgi no robežām;

atzīdamas, ka ir nepieciešams saskaņot privātuma neaizskaramības pamatvērtības un informācijas brīvu plūsmu starp cilvēkiem,

ir vienojušās:”

**1. pants. Mērķis un nolūks**

“Šīs Konvencijas mērķis ir katras Puses teritorijā nodrošināt jebkurai personai neatkarīgi no nacionalitātes [pilsonības] vai dzīves vietas [pastāvīgās dzīvesvietas] tās tiesību un pamatbrīvību, it īpaši tiesību uz privātumu, ievērošanu attiecībā uz personas datu automātisko apstrādi (“datu aizsardzība”).”

(..)

**8. pants. Datu subjekta papildu aizsardzība**

“Jebkurai personai ir iespēja:

a) noskaidrot automātiskā personas datu faila esību, tā galvenos nolūkus, kā arī faila pārziņa identitāti un ierasto uzturēšanās vietu vai galveno uzņēmējdarbības veikšanas vietu;

b) saprātīgos intervālos un bez pārmērīgas novilcināšanas vai izdevumiem saņemt apstiprinājumu par to, vai ar šo personu saistītie personas dati tiek uzglabāti automātiskā datu failā, kā arī iepazīties ar šiem datiem saprotamā formā;

c) panākt, ja tas nepieciešams, šādu datu labošanu vai dzēšanu, ja tie ir tikuši apstrādāti pretēji nacionālo normatīvo [valsts tiesību] aktu noteikumiem, kas ievieš šīs Konvencijas 5. un 6. pantā paredzētos [noteiktos] pamatprincipus;

d) izmantot tiesiskās aizsardzības līdzekļus, ja netiek izpildīts lūgums sniegt apstiprinājumu, vai, attiecīgā gadījumā, iepazīties, labot vai dzēst datus, kā noteikts šī panta b) un c) apakšpunktos [lūgums pēc apstiprinājuma vai attiecīgi paziņošanas, labošanas vai dzēšanas, kā noteikts šā panta b) un c) apakšpunktā].”

**9. pants. Izņēmumi un ierobežojumi**

“1. Nav pieļaujami nekādi izņēmumi attiecībā uz šīs Konvencijas 5., 6. un 8. panta noteikumiem, izņemot šajā pantā noteiktajos.

2. Atkāpšanās no šīs Konvencijas 5., 6., un 8. panta noteikumiem var tikt pieļauta, ja šāda atkāpšanās ir paredzēta Puses normatīvajos aktos un ir uzskatāma par demokrātiskā sabiedrībā nepieciešamu pasākumu, lai:

a) aizsargātu Valsts drošību, sabiedrisko drošību, Valsts monetārās intereses vai cīnītos ar noziedzību;

b) aizsargātu datu subjektu vai citu personu tiesības un brīvības.

(..)”

**10. pants. Sankcijas un tiesiskās aizsardzības līdzekļi**

“Katra Puse apņemas noteikt atbilstošas sankcijas un tiesiskās aizsardzības līdzekļus gadījumiem, ja tiek pārkāpti nacionālo normatīvo [valsts tiesību] aktu noteikumi, ar kuriem ieviesti šajā nodaļā paredzētie datu aizsardzības pamatprincipi.”

193. Iepriekšminētās konvencijas paskaidrojuma rakstā ir precizēts turpmākais.

**9. pants. Izņēmumi un ierobežojumi**

“55. Izņēmumi attiecībā uz datu aizsardzības pamatprincipiem attiecas tikai uz tiem principiem, kas ir nepieciešami pamatvērtību aizsardzībai demokrātiskā sabiedrībā. Šā panta otrā punkta teksts ir veidots pēc Eiropas Cilvēktiesību konvencijas 6., 8., 10. un 11. panta otrā punkta teksta parauga. No Komisijas un Cilvēktiesību tiesas lēmumiem saistībā ar jēdzienu “nepieciešamie pasākumi” izriet, ka šā jēdziena kritērijus nevar noteikt visām valstīm un uz visiem laikiem, bet tie ir jāapsver, ņemot vērā attiecīgo situāciju katrā valstī.

56. 2. punkta a) apakšpunktā ir uzskaitītas galvenās valsts intereses, kurām, iespējams, jāpiemēro izņēmumi. Šie izņēmumi ir ļoti specifiski, lai izvairītos no tā, ka attiecībā uz konvencijas vispārējo piemērošanu valstīm būtu pārmērīgi liela rīcības brīvība.

Saskaņā ar 16. pantu valstis saglabā iespēju atsevišķos gadījumos atteikties piemērot konvenciju svarīgu iemeslu dēļ, tostarp 9. pantā uzskaitīto iemeslu dēļ.

Jēdziens “valsts drošība” ir jāsaprot tradicionālajā nozīmē kā nacionālās [valsts] suverenitātes aizsardzība pret iekšējiem vai ārējiem apdraudējumiem, tostarp valsts starptautisko attiecību aizsardzība.”

2. 2001. gada 8. novembra Konvencijas par personu aizsardzību attiecībā uz personas datu automātisko apstrādi Papildu protokols par pārraudzības institūcijām un pārrobežu datu plūsmām (CETS Nr. 181)

194. Ciktāl tas attiecas uz šo lietu, protokols, ko Apvienotā Karaliste vēl nav ratificējusi, paredz turpmāko.

**1. pants. Pārraudzības institūcijas**

“1. Katra Puse nosaka vienu vai vairākas institūcijas, kuras ir atbildīgas par to, lai tiktu nodrošināta to valsts iekšējās tiesībās paredzēto pasākumu ievērošana, ar kuriem tiek ieviesti Konvencijas II un III sadaļas un šī [šā] Protokola principi.

2. a) Šajā sakarā [Šādā nolūkā] minētajām institūcijām ir jāpiešķir izmeklēšanas un iejaukšanās pilnvaras, kā arī pilnvaras iesaistīties tiesvedībā vai pievērst kompetentu tiesu iestāžu uzmanību to valsts iekšējo tiesību noteikumu pārkāpumiem, ar kuriem tiek ieviesti šī [šā] Protokola 1. panta 1. punktā minētie principi.

b) Katra pārraudzības institūcija savas kompetences robežās izskata jebkuras personas iesniegtās prasības saistībā ar minētās personas tiesību un pamatbrīvību aizsardzību attiecībā uz personas datu apstrādi.

3. Pārraudzības institūcijas ir pilnīgi neatkarīgas attiecībā uz savu funkciju izpildi.

4. Par pārraudzības institūcijas lēmumiem var iesniegt sūdzību tiesā.

(..)”

**2. pants. Personas datu pārrobežu plūsma saņēmējam, kurš neatrodas Konvencijas Līgumslēdzējas Puses jurisdikcijā**

“1. Katra Puse nodrošina, ka personas datu pārsūtīšana tādam saņēmējam, kurš atrodas tādas valsts vai tādas organizācijas jurisdikcijā, kas nav šīs Konvencijas Līgumslēdzēja Puse, ir atļauta tikai tādā gadījumā, ja šāda valsts vai organizācija nodrošina adekvātu pārsūtāmo datu aizsardzības līmeni.

2. Atkāpjoties no šī [šā] Protokola 2. panta 1. punkta noteikumiem, katra Puse var atļaut pārsūtīt personas datus:

a) ja valsts iekšējās tiesības paredz datu pārsūtīšanu:

– lai aizsargātu noteiktas datu subjekta intereses, vai [intereses vai]

– tādās [tādas] likumīgas intereses, kurām ir augstāks juridiskais spēks, it īpaši svarīgas sabiedrības intereses, vai

b) [ja] par datu pārsūtīšanu atbildīgais datu pārzinis piemēro aizsardzības pasākumus, kurus kompetentas institūcijas saskaņā ar valsts iekšējām tiesībām ir atzinušas par adekvātiem aizsardzības pasākumiem.”

3. Ministru komitejas ieteikums par personas datu aizsardzību telekomunikāciju pakalpojumu jomā

195. Ciktāl tas attiecas uz šo lietu, Ministru komitejas ieteikumā Nr. R (95) 4, kas tika pieņemts 1995. gada 7. februārī, noteikts turpmākais:

“2.4. Valsts iestāžu iejaukšanās sakaru saturā, tostarp noklausīšanās vai sarunu ierakstīšanas ierīču vai arī citu uzraudzības vai sakaru pārtveršanas līdzekļu izmantošana, ir pieļaujama vienīgi tad, ja tas paredzēts likumā un nepieciešams demokrātiskā sabiedrībā, lai:

a) aizsargātu valsts drošību, sabiedrisko drošību, valsts monetārās intereses vai cīnītos ar noziedzību;

b) aizsargātu datu subjektu vai citu personu tiesības un brīvības.

2.5. Ja valsts iestādes iejaucas sakaru saturā, valsts tiesību aktiem jāregulē:

a) veids, kādā datu subjekts īsteno savas tiesības uz piekļuvi datiem vai datu labošanu;

b) kādos apstākļos atbildīgās valsts iestādes ir tiesīgas atteikties sniegt informāciju attiecīgajai personai vai kavēt tās sniegšanu;

c) veids, kādā dati tiek uzglabāti vai iznīcināti.

Ja valsts iestāde ir devusi norādījumus tīkla operatoram vai pakalpojumu sniedzējam iejaukties, šādi savāktie dati būtu jāpaziņo vienīgi tai iestādei, kas norādīta atļaujā par šādu iejaukšanos.”

4. Eiropas Komisijas demokrātijas tiesiskai nostiprināšanai (“Venēcijas komisijas”) 2015. gada Ziņojums par sakaru izlūkošanas aģentūru demokrātisku pārraudzību

196. Venēcijas komisija jau sākotnēji norādīja, kāda vērtība masveida pārtveršanai varētu būt attiecībā uz drošības operācijām, jo tā ļāva drošības dienestiem pieņemt proaktīvu pieeju, meklējot līdz šim nezināmas briesmas, nevis izmeklējot jau zināmās. Tomēr tā arī norādīja, ka masveida datu pārtveršana datu pārraidē vai prasības par to, ka telekomunikāciju uzņēmumiem jāuzglabā un pēc tam jāsniedz telekomunikāciju satura dati vai metadati tiesībaizsardzības vai drošības aģentūrām, ir saistīta ar pasaules iedzīvotāju lielākās daļas tiesību uz privātās dzīves neaizskaramību un citu cilvēktiesību pārkāpumu. Šajā ziņā Venēcijas komisija uzskatīja, ka galvenā iejaukšanās personas tiesībās uz privātās dzīves neaizskaramību notika tad, kad aģentūras piekļuva saglabātajiem personas datiem un/vai tos apstrādāja. Tādēļ datoranalīze (parasti ar selektoru palīdzību) bija viens no svarīgajiem posmiem, lai nodrošinātu līdzsvaru starp personas rūpēm par integritāti un citām interesēm.

197. Saskaņā ar ziņojumu divi svarīgākie drošības pasākumi bija atļauja (datu savākšanai un piekļuvei) un procesa pārraudzība. No Tiesas judikatūras izriet, ka pēdējais no minētajiem jāveic neatkarīgai ārējai struktūrai. Lai gan Tiesa deva priekšroku tiesas atļaujai, tā to nebija atzinusi par obligātu prasību. Sistēma drīzāk bija jāvērtē kopumā, un tad, kad atļaujas izsniegšanas posmā trūka neatkarīgu kontroles pasākumu, pārraudzības posmā bija jāīsteno īpaši stingri drošības pasākumi. Šajā ziņā Venēcijas komisija izskatīja Amerikas Savienoto Valstu sistēmas piemēru, kur atļauju piešķīra *FISC*. Tomēr, lai gan tiesas atļauja ir paredzēta, neatkarīgas pārraudzības trūkums attiecībā uz tiesas noteiktajiem nosacījumiem un ierobežojumiem sagādāja problēmas.

198. Tāpat Komisija norādīja, ka uzraudzības subjekta informēšana nebija absolūta Konvencijas 8. pantā noteikta prasība, jo vispārēja sūdzību procedūra neatkarīgai pārraudzības iestādei varētu kompensēt neinformēšanu.

199. Ziņojumā iekšējie kontroles pasākumi arī bija norādīti kā “primārie drošības pasākumi”. Personu piesaistīšana un mācības bija galvenie jautājumi; turklāt bija svarīgi, lai aģentūras, izsludinot iekšējos noteikumus, balstītos uz tiesībām uz personas privātās dzīves neaizskaramību un citām cilvēktiesībām.

200. Ziņojumā atzina, ka žurnālisti ir grupa, kurai nepieciešama īpaša aizsardzība, jo viņu kontaktu meklēšana varētu atklāt viņu avotus (un atklāšanas risks varētu būt spēcīgs trauksmes cēlējus atturošs faktors). Tomēr tā uzskatīja, ka nav absolūta aizlieguma meklēt žurnālistu kontaktus, ja ir ļoti nopietni iemesli šādi rīkoties. Ziņojumā norādīts, ka žurnālista profesija nav viegli identificējama, jo NVO iesaistās arī sabiedriskās domas veidošanā un pat emuāru autori var apgalvot, ka viņiem ir tiesības uz līdzvērtīgu aizsardzību.

201. Visbeidzot, ziņojumā īsumā aplūkots jautājums par izlūkdatu apmaiņu un jo īpaši risku, ka valstis tādējādi varētu apiet stingrākas vietējās uzraudzības procedūras un/vai jebkādus juridiskus ierobežojumus, kas varētu attiekties uz aģentūrām attiecībā uz iekšzemes izlūkošanas operācijām. Tās ieskatā atbilstošs drošības pasākums būtu nodrošināt, ka pārraidīto masveida materiālu varētu pārbaudīt vienīgi tad, ja ir izpildītas visas galvenās valsts līmeņa meklēšanas prasības un tas atbilstoši atļauts tāpat kā tāda masveida materiāla pārbaude, ko sakaru izlūkošanas aģentūra ieguvusi, izmantojot savas metodes.

III. EIROPAS SAVIENĪBAS TIESĪBU AKTI

A. Eiropas Savienības Pamattiesību harta

202. Hartas 7., 8. un 11. pantā ir noteikts:

**7. pants. Privātās un ģimenes dzīves neaizskaramība**

“Ikvienai personai ir tiesības uz savas privātās un ģimenes dzīves, dzīvokļa un saziņas neaizskaramību.”

**8. pants. Personas datu aizsardzība**

“1. Ikvienai personai ir tiesības uz savu personas datu aizsardzību.

2. Šādi dati ir jāapstrādā godprātīgi, noteiktiem mērķiem un ar attiecīgās personas piekrišanu vai ar citu likumīgu pamatojumu, kas paredzēts tiesību aktos. Ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un tiesības ieviest labojumus šajos datos.

3. Atbilstību šiem noteikumiem kontrolē neatkarīga iestāde.”

**11. pants. Vārda un informācijas brīvība**

“1. Ikvienai personai ir tiesības uz vārda brīvību. Šīs tiesības ietver uzskatu brīvību un brīvību saņemt un izplatīt informāciju vai [un] idejas bez valsts iestāžu iejaukšanās un neatkarīgi no valstu robežām.

2. Tiek ievērota plašsaziņas līdzekļu brīvība un plurālisms.”

B. Eiropas Savienības direktīvas un regulas saistībā ar personas datu aizsardzību un apstrādi

203. 1995. gada 24. oktobrī pieņemtā Datu aizsardzības direktīva (Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti) daudzus gadus regulēja personas datu aizsardzību un apstrādi Eiropas Savienībā. Tā kā Kopienu tiesību akti neattiecās uz dalībvalstu darbībām saistībā ar sabiedrisko drošību, aizsardzību un valsts drošību, šī direktīva šīm darbībām nebija piemērojama (3. panta 2. punkts).

204. Vispārīgā datu aizsardzības regula, kas pieņemta 2016. gada aprīlī, aizstāja Datu aizsardzības direktīvu un stājās spēkā 2018. gada 25. maijā. Regula, kas ir tieši piemērojama dalībvalstīs,[[2]](#footnote-2) paredz noteikumus un prasības par datu subjektu personu identificējošas informācijas apstrādi Eiropas Savienībā, un tā attiecas uz visiem uzņēmumiem neatkarīgi no to atrašanās vietas, kuri veic uzņēmējdarbību Eiropas Ekonomikas zonā. Uzņēmējdarbības procesiem, kuros tiek apstrādāti personas dati, ir jāparedz integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, proti, personas dati ir jāuzglabā, tos pseidonimizējot vai pilnībā anonimizējot, kā arī jāizmanto pēc iespējas stingrāki privātuma noklusējuma iestatījumi, lai dati nebūtu publiski pieejami, ja datu subjekts nav sniedzis nepārprotamu piekrišanu, un lai tos nevarētu izmantot subjekta identificēšanai bez papildu informācijas uzglabāšanas. Personas datus nedrīkst apstrādāt, ja vien tas netiek darīts saskaņā ar likumīgu pamatu, kas noteikts regulā, vai ja datu pārzinis vai apstrādātājs ir saņēmis nepārprotamu piekrišanu, ko datu īpašnieks devis pēc savas izvēles. Datu īpašniekam ir tiesības jebkurā brīdī atsaukt šo atļauju.

205. Personas datu apstrādātājam ir skaidri jāatklāj jebkura datu vākšana, jānorāda datu apstrādes likumīgais pamats un nolūks un jāprecizē, cik ilgi dati tiek saglabāti un vai ar tiem apmainās ar jebkurām trešām personām vai ārpus Eiropas Savienības. Lietotājiem ir tiesības pieprasīt apstrādātāja savākto datu pārnēsājamu kopiju vienotā formātā, kā arī viņu datu dzēšanu noteiktos apstākļos. Valsts iestādēs un uzņēmumos, kuru pamatdarbība ir saistīta ar personas datu regulāru un sistemātisku apstrādi, ir jābūt datu aizsardzības speciālistam (turpmāk tekstā – “DAS”), kura pienākums ir nodrošināt atbilstību VDAR. Uzņēmumiem ir jāziņo par datu aizsardzības pārkāpumiem 72 stundu laikā, ja tie negatīvi ietekmē lietotāja privātumu.

206. 2. un 11. apsvērumā Direktīvā par privāto dzīvi un elektronisko komunikāciju (Direktīvā 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē), kas tika pieņemta 2002. gada 12. jūlijā, ir noteikts:

“(2) Šī direktīva respektē pamattiesības un ievēro principus, kas jo īpaši ir atzīti Eiropas Savienības Pamattiesību hartā. Šī direktīva jo īpaši nodrošina pilnībā tiesības, kas izklāstītas minētās hartas 7. un 8. pantā [Šīs direktīvas mērķis jo īpaši ir nodrošināt minētās hartas 7. un 8. pantā noteikto tiesību pilnīgu ievērošanu].

(..) (..) (..)

(11) Tāpat kā Direktīva 95/46/EK, arī šī direktīva neattiecas uz pamattiesību un pamatbrīvību aizsardzības jautājumiem, kas saistīti ar darbībām, kuras neregulē Kopienas tiesību akti. Tāpēc tā nemaina esošo līdzsvaru starp fizisku personu tiesībām uz privāto dzīvi un iespēju dalībvalstīm pieņemt šīs direktīvas 15. panta 1. punktā minētos pasākumus, kas nepieciešami sabiedrības drošībai, aizsardzībai, valsts drošībai (tostarp valsts ekonomisko labklājību [ekonomiskajai labklājībai], ja darbības attiecas uz valsts drošības jautājumiem) un krimināltiesību aktu piemērošanai. Tādējādi šī direktīva neietekmē dalībvalstu iespēju veikt komunikāciju likumīgu pārtraukšanu vai pieņemt citus pasākumus, ja tie nepieciešami jebkuram no šiem nolūkiem un ir saskaņā ar Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvenciju, kā skaidrots Eiropas Cilvēktiesību tiesas nolēmumos. Šādiem pasākumiem jābūt atbilstošiem, stingri samērīgiem ar paredzēto nolūku un nepieciešamiem demokrātiskā sabiedrībā, un tiem jāatbilst attiecīgajiem drošības pasākumiem saskaņā ar Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvenciju.”

207. Ciktāl tas attiecas uz šo lietu, direktīvā arī noteikts:

**1. pants. Darbības joma un mērķis**

“1. Šajā direktīvā paredzēta dalībvalstu to noteikumu saskaņošana, ar kuriem jānodrošina pamattiesību un pamatbrīvību līdzvērtīgs aizsardzības līmenis, un jo īpaši attiecībā uz tiesībām uz privāto dzīvi saistībā ar personas datu apstrādi elektronisko komunikāciju nozarē, kā arī jānodrošina šo datu un elektronisko komunikāciju iekārtu un pakalpojumu brīva aprite Kopienā.

2. Šīs direktīvas noteikumi precizē un papildina Direktīvas [Direktīvu] 95/46/EK 1. punktā minētajam nolūkam. Turklāt ar tiem paredz to abonentu likumīgo interešu aizsardzību, kuri ir juridiskas personas.

3. Šī direktīva neattiecas uz darbībām, uz kurām neattiecas Eiropas Kopienas dibināšanas līgums, tādām kā tās, kas iekļautas Līguma par Eiropas Savienību V un VI sadaļā, un jebkurā gadījumā uz darbībām, kas attiecas uz sabiedrības drošību, aizsardzību, valsts drošību (tostarp valsts ekonomisko labklājību, ja darbības attiecas uz valsts drošības jautājumiem) un uz valsts darbībām krimināltiesību jomā.”

**15. pants. Direktīvas 95/46/EK dažu noteikumu piemērošana**

“1. Dalībvalstis var pieņemt tiesību aktus, lai ierobežotu šīs direktīvas 5. un 6. pantā, 8. panta 1., 2., 3. un 4. punktā un 9. pantā minēto tiesību un pienākumu darbības jomu, ja šādi ierobežojumi ir vajadzīgi saskaņā ar nepieciešamiem, atbilstīgiem un samērīgiem pasākumiem demokrātiskā sabiedrībā, lai garantētu valsts drošību, aizsardzību, sabiedrības drošību un kriminālpārkāpumu vai elektroniskās komunikāciju sistēmas nevēlamas izmantošanas novēršanu, izmeklēšanu, noteikšanu un kriminālvajāšanu, kā noteikts Direktīvas 95/46/EK 13. panta 1. punktā. Tālab dalībvalstis, cita starpā [*inter alia*], var pieņemt tiesību aktus, paredzot datu saglabāšanu ierobežotā laikposmā, kas pamatots ar šajā punktā noteiktajiem iemesliem. Visi šajā punktā minētie pasākumi ir saskaņā ar Kopienas tiesību aktu vispārējiem principiem, tostarp tie [tiem], kas minēti Eiropas Savienības dibināšanas līguma [Eiropas Savienības līguma] 6. panta 1. un 2. punktā.”

208. 2006. gada 15. martā tika pieņemta Datu saglabāšanas direktīva (Direktīva 2006/24/EK par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK). Pirms 2014. gadā tika pasludināts spriedums, ar kuru šī direktīva tika atzīta par spēkā neesošu (skat. turpmāk 209. punktu), tajā bija noteikts turpmākais, ciktāl tas attiecas uz šo lietu:

**1. pants. Priekšmets un darbības joma**

“1. Šīs direktīvas mērķis ir saskaņot dalībvalstu noteikumus attiecībā uz publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzēju vai publiski pieejamu komunikāciju tīklu operatoru pienākumiem, kas attiecas uz noteiktu datu, kurus tie iegūst vai apstrādā, saglabāšanu, lai nodrošinātu, ka šie dati ir pieejami smagu noziegumu, kas katrā dalībvalstī noteikti tiesību aktos, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem.

2. Šī direktīva attiecas uz noslodzes datiem un atrašanās vietas datiem par juridiskām personām un fiziskām personām un uz datiem, kas ar tiem saistīti, kuri ir nepieciešami abonenta vai reģistrēta lietotāja identificēšanai. To nepiemēro elektronisko komunikāciju saturam, tostarp informācijai, kura skatīta, izmantojot elektronisko komunikāciju tīklu.”

**3. pants. Pienākums saglabāt datus**

“1. Atkāpjoties no Direktīvas 2002/58/EK 5., 6. un 9. panta, dalībvalstis pieņem pasākumus, lai nodrošinātu, ka šīs direktīvas 5. panta [pantā] minētie dati tiek saglabāti saskaņā ar šīs direktīvas noteikumiem tiktāl, ciktāl tos ir ieguvuši vai apstrādājuši publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzēji vai publiski pieejamu komunikāciju tīklu operatori, sniedzot attiecīgos komunikāciju pakalpojumus šo valstu jurisdikcijā.”

C. Attiecīgā Eiropas Savienības Tiesas (turpmāk tekstā – “EST”) judikatūra

1. Spriedums lietā ““Digital Rights Ireland Ltd” pret komunikāciju, jūras un dabas resursu ministru un citiem, un Karintijas Federālās zemes valdību un citiem” (lietas C‑293/12 un C‑594/12; ECLI:EU:C:2014:238)

209. 2014. gada 8. aprīļa spriedumā EST pasludināja par spēkā neesošu Datu saglabāšanas direktīvu 2006/24/EK, kurā noteikts publiski pieejamu elektronisko sakaru pakalpojumu sniedzēju vai publiski pieejamu sakaru tīklu operatoru pienākums saglabāt visus datplūsmas datus un atrašanās vietas datus uz laiku no sešiem mēnešiem līdz diviem gadiem, lai nodrošinātu, ka šie dati ir pieejami katrā valstī attiecīgajos tiesību aktos noteiktu smagu noziegumu izmeklēšanas, atklāšanas un kriminālvajāšanas nolūkam. EST norādīja, ka, lai gan sakaru satura saglabāšana saskaņā ar šo direktīvu nebija atļauta, datplūsmas un atrašanās vietas dati, uz kuriem šī direktīva attiecās, varēja ļaut ļoti precīzi secināt par to personu privāto dzīvi, kuru dati tikuši saglabāti. Līdz ar to pats pienākums saglabāt šos datus uzskatāms par iejaukšanos personas tiesībās uz privātās dzīves neaizskaramību un saziņas sakaros, kas garantētas Eiropas Savienības Pamattiesību hartas 7. pantā, un tiesībās uz personas datu aizsardzību, kas paredzētas minētās hartas 8. pantā.

210. Kompetento valsts iestāžu piekļuve datiem radīja papildu iejaukšanos šajās pamattiesībās, ko EST uzskatīja par “īpaši būtisku”. Tas, ka datu saglabāšana un to vēlāka izmantošana notika, abonentu vai reģistrēto lietotāju par to neinformējot, varēja, kā to norādījusi EST, attiecīgajām personām radīt sajūtu, ka viņu privātā dzīve tiek pastāvīgi novērota. Tā arī norādīja, ka šī iejaukšanās atbilda vispārējo interešu mērķim, proti, sekmēt smagu noziegumu un terorisma apkarošanu un līdz ar to arī sekmēt sabiedrisko drošību. Tomēr tā neatbilda samērīguma prasībai.

211. Pirmkārt, šī direktīva vispārīgā veidā aptvēra visas personas un visus elektronisko sakaru līdzekļus, kā arī visus datplūsmas datus bez jebkādām atšķirībām, ierobežojumiem vai izņēmumiem saistībā ar mērķi apkarot smagus noziegumus. Tādējādi tā radīja iejaukšanos gandrīz visu Eiropas iedzīvotāju pamattiesībās, kā norādījusi EST. Tā attiecās pat uz personām, attiecībā uz kurām nebija nekādas norādes, kas ļautu uzskatīt, ka viņu rīcībai varētu būt sakars – kaut vai netiešs vai attāls – ar smagiem noziegumiem.

212. Otrkārt, direktīvā nebija ietverti atbilstošie materiālie un procesuālie nosacījumi saistībā ar kompetento valsts iestāžu piekļuvi datiem un to turpmāko izmantošanu. Vispārīgi atsaucoties uz smagu noziegumu, ko katra dalībvalsts definējusi savos valsts tiesību aktos, direktīvā nebija paredzēti nekādi objektīvi kritēriji, kas nosaka, kādus noziedzīgus nodarījumus varētu uzskatīt par pietiekami smagiem, lai attaisnotu šādu plašu iejaukšanos Hartas 7. un 8. pantā garantētajās pamattiesībās. Turklāt attiecībā uz kompetento valsts iestāžu piekļuvi saglabātajiem datiem nebija noteikta iepriekšēja pārskatīšana, ko veiktu vai nu tiesa, vai kāda neatkarīga administratīva struktūra, kuras lēmums paredzētu ierobežot piekļuvi datiem un to izmantošanu ar to, kas ir absolūti nepieciešams izvirzītā mērķa sasniegšanai.

213. Treškārt, direktīvā bija noteikts pienākums saglabāt visus datus vismaz sešus mēnešus, nenosakot nekādas atšķirības starp datu kategorijām atkarībā no to iespējamā noderīguma izvirzītā mērķa sasniegšanai vai personām, uz kurām tie attiecas. EST secināja, ka ar direktīvu tika pieļauta plaša apjoma un īpaši būtiska iejaukšanās Hartas 7. un 8. pantā paredzētajās pamattiesībās un ka šī iejaukšanās nebija precīzi reglamentēta ar noteikumiem, lai nodrošinātu, ka tā patiešām attiecas vienīgi uz absolūti nepieciešamo. EST arī norādīja, ka direktīvā nebija paredzēti pietiekami drošības pasākumi, piemēram, tehniski vai organizatoriski pasākumi, lai nodrošinātu saglabāto datu efektīvu aizsardzību pret ļaunprātīgas izmantošanas risku, kā arī pret jebkādu nelikumīgu piekļuvi šiem datiem un to nelikumīgu izmantošanu.

2. Spriedumi lietās ““Tele2 Sverige AB” pret “Post- och telestyrelsen”” un “Iekšlietu valsts sekretārs pret Tomu Vatsonu [Tom Watson] un citiem” (lietas C‑203/15 un C‑698/15; ECLI:EU:C:2016:970)

214. Lietā “Iekšlietu valsts sekretārs pret Vatsonu [*Watson*] un citiem” pieteikuma iesniedzēji lūdza tiesu izvērtēt 2014. gada Datu saglabāšanas un izmeklēšanas pilnvaru likuma [*Data Retention and Investigatory Powers Act 2014*] (turpmāk tekstā – “*DRIPA*”) 1. panta likumību. Saskaņā ar šo pantu valsts sekretārs varēja pieprasīt publisko telekomunikāciju operatoram saglabāt attiecīgos sakaru datus, ja viņš to uzskatīja par nepieciešamu un samērīgu vienam vai vairākiem nolūkiem, ko paredz *RIPA* 22. panta 2. punkta a)–h) apakšpunkts. Pieteikuma iesniedzēji *inter alia* apgalvoja, ka 1. pants neatbilda Hartas 7. un 8. pantam un Konvencijas 8. pantam.

215. 2015. gada 17. jūlijā Augstā tiesa nosprieda, ka ar lietā “Digital Rights” pasludināto spriedumu bija noteiktas “obligātās ES tiesību aktu prasības”, kas attiecas uz dalībvalstu tiesību aktiem par sakaru datu saglabāšanu un piekļuvi šiem datiem. Tā kā EST šajā spriedumā nosprieda, ka Direktīva 2006/24 neatbilda samērīguma principam, arī valsts tiesību akti ar tādiem pašiem noteikumiem kā minētajā direktīvā nevarēja atbilst šim principam. Patiesībā no sprieduma lietā “Digital Rights” pamatā esošās loģikas izrietēja, ka ar tiesību aktiem, kas nosaka vispārēju regulējumu par sakaru datu saglabāšanu, tika pārkāptas Hartas 7. un 8. pantā garantētās tiesības, ja vien šos tiesību aktus nepapildināja vispārējs regulējums par piekļuvi datiem, ko definējuši valsts tiesību akti, kas paredz pietiekamus drošības pasākumus šo tiesību aizsardzībai. Līdz ar to *DRIPA* 1. pants neatbilda Hartas 7. un 8. pantam, jo tajā nebija iekļauti skaidri un precīzi noteikumi, kas paredz piekļuvi saglabātajiem datiem un to izmantošanu, turklāt attiecībā uz piekļuvi šiem datiem nebija noteikta iepriekšēja pārskatīšana, ko veiktu vai nu tiesa, vai arī kāda neatkarīga administratīva struktūra.

216. Valsts sekretāram iesniedzot apelācijas sūdzību, Apelācijas tiesa lūdza EST sniegt prejudiciālu nolēmumu.

217. EST šī lieta tika apvienota ar Stokholmas Apelācijas tiesas [*Kammarrätten i Stockholm*] lūgumu sniegt prejudiciālu nolēmumu lietā C‑203/15 ““Tele2 Sverige AB” pret “Post- och telestyrelsen””. Pēc mutvārdu paskaidrojumu uzklausīšanas, kurā iesaistījās aptuveni piecpadsmit Eiropas Savienības dalībvalstis, EST 2016. gada 21. decembrī pasludināja spriedumu. EST nosprieda, ka Direktīvas 2002/58 15. panta 1. punkts, to aplūkojot kopā ar Hartas 7., 8. un 11. pantu un 52. panta 1. punktu, ir interpretējams tādējādi, ka tas aizliedz valsts tiesību aktus, kas regulē datplūsmas un atrašanās vietas datu aizsardzību, jo īpaši kompetento valsts iestāžu piekļuvi saglabātajiem datiem, ja šīs piekļuves mērķis noziegumu apkarošanas kontekstā nav vienīgi smagu noziegumu apkarošana, kad attiecībā uz piekļuvi nav noteikta iepriekšēja pārskatīšana, ko veiktu vai nu tiesa, vai arī kāda neatkarīga administratīva iestāde, un kad nav prasības, ka attiecīgie dati ir jāsaglabā Eiropas Savienībā.

218. Apelācijas tiesas jautājumu par to, vai Hartas 7. un 8. pantā paredzētā aizsardzība ir plašāka nekā Konvencijas 8. pantā paredzētā aizsardzība, EST atzina par nepieņemamu.

219. Pēc EST sprieduma pasludināšanas lietu nodeva atpakaļ izskatīšanai Apelācijas tiesai. 2018. gada 31. janvārī tā pasludināja konstatējošu spriedumu, proti, ka *DRIPA* 1. pants bija pretrunā ar Eiropas Savienības tiesību aktiem, ciktāl tas ļāva piekļūt saglabātajiem datiem, ja piekļuves mērķis nebija vienīgi smaga nozieguma apkarošana vai attiecībā uz piekļuvi nebija noteikta iepriekšēja pārskatīšana, ko veiktu vai nu tiesa, vai arī kāda neatkarīga administratīva iestāde.

3. Spriedums lietā “Ministerio Fiscal” (lieta C-207/16; ECLI:EU:C:2018:788)

220. Šis lūgums sniegt prejudiciālu nolēmumu tika iesniegts pēc tam, kad Spānijas policija, izmeklējot naudas maka un mobilā tālruņa zādzību, lūdza izmeklēšanas tiesnesi piešķirt tai piekļuvi datiem, ar ko var identificēt lietotājus, kuriem pieder tālruņa numuri, kas aktivizēti ar nozagtu mobilo tālruni divpadsmit dienu laikā pirms zādzības. Izmeklēšanas tiesnesis noraidīja šo lūgumu, *inter alia* to pamatojot ar argumentu, ka apstākļi, kas bija par pamatu kriminālizmeklēšanas uzsākšanai, nebija “smags” noziedzīgs nodarījums. Iesniedzējtiesa pēc tam vērsās EST, lūdzot sniegt norādījumus par noziedzīga nodarījuma smaguma sliekšņa noteikšanu, kuru pārsniedzot ir attaisnojama iejaukšanās personas pamattiesībās, piemēram, kompetento valsts iestāžu piekļuve elektronisko sakaru pakalpojumu sniedzēju saglabātajiem personas datiem.

221. 2018. gada 2. oktobrī EST Lielā palāta nosprieda, ka Direktīvas 2002/58/EK 15. panta 1. punkts, to aplūkojot kopā ar Eiropas Savienības Pamattiesību hartas 7. un 8. pantu, ir interpretējams tādējādi, ka valsts iestāžu piekļuve datiem nolūkā identificēt to SIM karšu īpašniekus, kas aktivizētas ar zagtu mobilo tālruni, piemēram, īpašnieku uzvārdiem, vārdiem un, ja nepieciešams,, viņu adresēm, ir radījusi iejaukšanos viņu pamattiesībās, kas nebija tik būtiska, lai šī piekļuve noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas jomās attiektos vienīgi uz smagu noziegumu apkarošanu. Tā jo īpaši norādīja:

“Atbilstoši samērīguma principam noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas jomā būtisku iejaukšanos var pamatot ar cīņu pret noziegumu, kas kvalificējams kā “smags”.

Savukārt, ja šādas piekļuves radīta iejaukšanās nav būtiska, minēto piekļuvi var pamatot ar “noziedzīgu nodarījumu” novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas nolūku vispārīgā veidā.”

222. Tā neuzskatīja, ka ar piekļuvi pieprasītajiem datiem tiek pieļauta īpaši būtiska iejaukšanās, jo

“tie paredzēti vienīgi tam, lai noteiktā laikposmā ar zagto mobilo tālruni aktivizētās SIM kartes varētu sasaistīt ar šo SIM karšu īpašnieku identitāti. Neveicot kontrolpārbaudes ar datiem par sakariem ar šīm SIM kartēm un atrašanās vietas datiem, šie dati neļauj noskaidrot nedz ar vienu vai vairākām attiecīgajām SIM kartēm pārraidīto sakaru datumu, laiku, ilgumu un adresātus, nedz šo sakaru vietu vai to biežumu ar noteiktām personām konkrētā laika posmā. Tādējādi pēc minētajiem datiem nevar precīzi secināt par to personu privāto dzīvi, kuru dati tikuši aizskarti.”

4. Spriedums lietā “Maksimilians Šrēmss [Maximillian Schrems] pret datu aizsardzības komisāru (lieta C‑362/14; ECLI:EU:C:2015:650)

223. Šis lūgums sniegt prejudiciālu nolēmumu izrietēja no sūdzības pret “Facebook Ireland Ltd”, ko pret Īrijas datu aizsardzības komisāru bija iesniedzis Šrēmss, privātās dzīves neaizskaramības atbalstītājs no Austrijas. Šrēmss apstrīdēja “Facebook Ireland” veikto viņa datu pārsūtīšanu Amerikas Savienotajām Valstīm un šo datu saglabāšanu serveros, kas atrodas šajā valstī. Datu aizsardzības komisārs noraidīja sūdzību, jo Eiropas Komisija savā 2000. gada 26. jūlija lēmumā bija atzinusi, ka Amerikas Savienotās Valstis ir nodrošinājušas atbilstošu pārsūtīto personas datu aizsardzības līmeni (turpmāk tekstā – “drošības zonas lēmums”).

224. EST savā 2015. gada 6. oktobra nolēmumā norādīja, ka ar Komisijas lēmumu, kurā atzīts, ka trešā valsts ir nodrošinājusi atbilstošu pārsūtīto personas datu aizsardzības līmeni, nav bijis iespējams anulēt vai pat mazināt pilnvaras, kas valsts pārraudzības iestādēm pieejamas saskaņā ar Hartu vai Datu aizsardzības direktīvu. Līdz ar to pat tad, ja Komisija būtu pieņēmusi lēmumu, valsts pārraudzības iestādēm bija jābūt iespējai pilnīgi neatkarīgi izvērtēt, vai personas datu pārsūtīšana trešai valstij atbildusi direktīvā noteiktajām prasībām.

225. Tomēr vienīgi EST var atzīt Komisijas lēmumu par spēkā neesošu. Tā šajā ziņā norādīja, ka drošības zonas sistēma attiekusies vienīgi uz Amerikas Savienoto Valstu uzņēmumiem, kas to ievēro, un ka tā uz Amerikas Savienoto Valstu valsts iestādēm nav attiekusies. Turklāt Amerikas Savienoto Valstu valsts drošības, sabiedrības interešu un tiesībaizsardzības prasības bijušas pārākas par drošības zonas sistēmu, tādēļ Amerikas Savienoto Valstu uzņēmumiem bija pienākums bez ierobežojumiem atstāt bez ievērības šajā sistēmā paredzētos aizsardzības noteikumus, ja tie ir pretrunā ar šīm prasībām. Līdz ar to drošības zonas sistēma ļāva Amerikas Savienoto Valstu publiskajām iestādēm iejaukties personu pamattiesībās, un Komisija drošības zonas lēmumā nebija atsaukusies uz šādu iejaukšanos ierobežojošu noteikumu esību Amerikas Savienotajās Valstīs vai efektīvu tiesisko aizsardzību pret šādu iejaukšanos.

226. Izvērtējot, vai aizsardzības līmenis Amerikas Savienotajās Valstīs pamatā bijis līdzvērtīgs Eiropas Savienībā garantētajām pamattiesībām un brīvībām, EST atzina, ka tiesiskais regulējums neattiecās vienīgi uz absolūti nepieciešamo, ja tas vispārīgi pieļauj visu to personu personas datu saglabāšanu, kuru dati no Eiropas Savienības ir pārsūtīti uz Amerikas Savienotajām Valstīm bez šķirošanas, ierobežojumiem vai izņēmumiem saistībā ar nolūku, kam tie kalpo, vai bez objektīva kritērija, kas ļauj ierobežot valsts iestāžu piekļuvi datiem un to vēlāku izmantošanu. Tāpēc saskaņā ar Eiropas Savienības tiesību aktiem tiesiskais regulējums, saskaņā ar kuru valsts iestādēm vispārīgi tiek ļauts piekļūt elektronisko sakaru saturam, bijis jāuzskata par tādu, kas apdraud pamattiesību uz privātās dzīves neaizskaramību būtību. Tāpat tiesiskais regulējums, kurā personām nav paredzētas nekādas iespējas izmantot tiesiskās aizsardzības līdzekļus, lai piekļūtu personas datiem, kas uz tiem attiecas, vai panākt šādu datu labošanu vai dzēšanu, ir apdraudējis pamattiesību uz efektīvu tiesisko aizsardzību būtību.

227. Visbeidzot Tiesa atzina, ka ar drošības zonas lēmumu valsts pārraudzības iestādēm tiek atņemtas pilnvaras tad, kad persona apšauba lēmuma saderīgumu ar privātās dzīves neaizskaramības un personu pamatbrīvību un pamattiesību aizsardzību. Komisijai nebija pilnvaru, lai ierobežotu valsts pārraudzības iestāžu pilnvaras, līdz ar to EST atzina drošības zonas lēmumu par spēkā neesošu.

5. Spriedums lietās “Datu aizsardzības komisārs pret “Facebook Ireland”” un “Maksimilians Šrēmss” (lieta C-311/18; ECLI:EU:C:2020:559)

228. Pēc tam, kad EST 2015. gada 6. oktobrī bija pasludinājusi spriedumu, iesniedzējtiesa atcēla lēmumu, ar kuru tika noraidīta Šrēmsa sūdzība, un nodeva to atpakaļ izskatīšanai komisāram. Komisāra veiktās izmeklēšanas gaitā “Facebook Ireland” paskaidroja, ka liela daļa personas datu bija pārsūtīta “Facebook Inc.”, pamatojoties uz datu aizsardzības standartklauzulām, kas ietvertas Komisijas Lēmuma 2010/87/ES pielikumā un tā grozījumos.

229. Šrēmss pārformulēja šo sūdzību, *inter alia* apgalvojot, ka Amerikas Savienoto Valstu tiesību akti uzlikuši “Facebook Inc.” par pienākumu nodrošināt tam pārsūtītos personas datus pieejamus konkrētām Amerikas Savienoto Valstu iestādēm, piemēram, *NSA* un Federālajam izmeklēšanas birojam. Tā kā šie dati tika izmantoti dažādu novērošanas programmu kontekstā pretēji Hartas 7., 8. un 47. pantam, ar Lēmumu 2010/87/ES nebija iespējams pamatot minēto datu pārsūtīšanu uz Amerikas Savienotajām Valstīm. Šādos apstākļos viņš lūdza komisāru aizliegt vai apturēt šo personas datu pārsūtīšanu “Facebook Inc.”.

230. 2016. gada 24. maijā publicētajā lēmumprojektā komisārs provizoriski uzskatīja, ka pastāv risks, ka ar Eiropas Savienības pilsoņu personas datiem, kurus pārsūtīja uz Amerikas Savienotajām Valstīm, var iepazīties Amerikas Savienoto Valstu iestādes un tās tos var apstrādāt veidā, kas nav saderīgs ar Hartas 7. un 8. pantu, un ka Amerikas Savienoto Valstu tiesību aktos šiem pilsoņiem nav paredzēti tiesiskās aizsardzības līdzekļi, kas atbilst Hartas 47. pantam. Komisārs uzskatīja, ka ar Lēmuma 2010/87/ES pielikumā ietvertajām datu aizsardzības standartklauzulām nevar izlabot šo trūkumu, jo tās nav saistošas Amerikas Savienoto Valstu iestādēm.

231. Ņemot vērā Amerikas Savienoto Valstu izlūkošanas darbības, kas noteiktas *FISA* 702. pantā un izpildrīkojumā Nr. 12333, Augstā tiesa secināja, ka Amerikas Savienotās Valstis veica personas datu masveida apstrādi, nenodrošinot Hartas 7. un 8. pantā garantētajam aizsardzības līmenim būtībā līdzvērtīgu aizsardzības līmeni, un ka Eiropas Savienības pilsoņiem nebija pieejami tādi paši līdzekļi, kādi ir Amerikas Savienoto Valstu pilsoņiem, jo Amerikas Savienoto Valstu tiesību akti neparedz Eiropas Savienības pilsoņiem Hartas 47. pantā garantētajam aizsardzības līmenim būtībā līdzvērtīgu aizsardzības līmeni. Tā apturēja tiesvedību un uzdeva EST vairākus prejudiciālus jautājumus. Tā *inter alia* jautāja, vai Eiropas Savienības tiesību akti attiekušies uz personas datu pārsūtīšanu no privāta uzņēmuma Eiropas Savienībā uz privātu uzņēmumu trešā valstī; ja tas tā ir, kā jānovērtē drošības līmenis trešā valstī un vai ar Amerikas Savienoto Valstu nodrošināto aizsardzības līmeni tika ievērota Hartas 47. pantā garantēto tiesību būtība.

232. EST savā 2020. gada 16. jūlija spriedumā atzina, ka Vispārīgā datu aizsardzības regula (turpmāk tekstā – “VDAR”) attiecas uz personas datu pārsūtīšanu, ko kādā dalībvalstī reģistrēts tirgus dalībnieks veic citam tirgus dalībniekam, kurš ir reģistrēts trešā valstī, neatkarīgi no tā, vai šīs pārsūtīšanas laikā vai pēc tam attiecīgās trešās valsts iestādes šos datus apstrādā sabiedriskās drošības, aizsardzības un valsts drošības nolūkā. Turklāt VDAR noteiktajiem atbilstošajiem drošības pasākumiem, izmantojamajām tiesībām un efektīvajiem tiesiskās aizsardzības līdzekļiem jānodrošina, lai tiem tiesību subjektiem, kuru personas dati tiek pārsūtīti uz trešo valsti, pamatojoties uz datu aizsardzības standartklauzulām, tiktu piemērots būtībā līdzvērtīgs aizsardzības līmenis tam, kāds ir garantēts Eiropas Savienībā. Tālab, novērtējot aizsardzības līmeni, kāds tiek nodrošināts šādas pārsūtīšanas kontekstā, it īpaši ir jāņem vērā gan līguma noteikumi, par kuriem ir panākta vienošanās starp personas datu pārzini vai apstrādātāju, kas reģistrēts Eiropas Savienībā, un attiecīgajā trešajā valstī reģistrēto saņēmēju, gan – attiecībā uz iespējamu šīs trešās valsts publisko iestāžu piekļuvi šādi pārsūtītajiem personas datiem – šīs trešās valsts tiesību sistēmas būtiskie elementi.

233. Turklāt ja vien pastāv likumīgi pieņemts Komisijas lēmums par aizsardzības līmeņa atbilstību, kompetentajai pārraudzības iestādei bija jāaptur vai jāaizliedz personas datu pārsūtīšana uz trešo valsti, ja šīs pārraudzības iestādes ieskatā un visu šīs pārsūtīšanas specifisko apstākļu kontekstā Komisijas pieņemtās datu aizsardzības standartklauzulas šajā trešā valstī netiek vai nevar tikt ievērotas un ja pārsūtīto datu aizsardzība (kā to nosaka Eiropas Savienības tiesību akti) nevar tikt nodrošināta ar citiem līdzekļiem.

234. Lai Komisija pieņemtu lēmumu par aizsardzības līmeņa atbilstību, tai, atbilstoši minot attiecīgos iemeslus, bija jākonstatē, ka attiecīgā trešā valsts, pamatojoties uz saviem iekšējiem tiesību aktiem vai savām starptautiskajām saistībām, nodrošināja būtībā līdzvērtīgu pamattiesību aizsardzības līmeni tam, kāds tiek garantēts Eiropas Savienības tiesiskajā kārtībā. EST ieskatā drošības zonas lēmums bija spēkā neesošs. No *FISA* 702. panta nekādā veidā neizriet ne tas, ka pastāv tajā paredzētie pilnvaru ierobežojumi attiecībā uz uzraudzības programmu īstenošanu ārējās izlūkošanas nolūkos, ne arī garantiju esība personām, kuras nav Amerikas Savienoto Valstu pilsoņi un kuras potenciāli skar šīs programmas. Šajos apstākļos ar to nevar nodrošināt tādu aizsardzības līmeni, kas būtībā būtu līdzvērtīgs Hartā garantētajam aizsardzības līmenim. Turklāt attiecībā uz pārraudzības programmām, kas balstītas uz izpildrīkojumu Nr. 12333, bija skaidrs, ka arī šis rīkojums nav paredzējis tiesības, ko tiesā varētu īstenot pret Amerikas Savienoto Valstu iestādēm.

6. Spriedumi lietās ““Privacy International” pret valsts sekretāru ārlietās un sadraudzības lietās un citiem” (lieta C-623/17; ECLI:EU:C:2020:790), ““La Quadrature du Net” un citi”, ““French Data Network” un citi” un ““Ordre des barreaux francophones et germanophone” un citi” (lietas C‑511/18, C‑512/18 un C-520/18; ECLI:EU:C:2020:791)

235. 2017. gada 8. septembrī *IPT* pasludināja spriedumu lietā “Privacy International”, kas attiecās uz faktu, ka izlūkdienesti ir ieguvuši masveida sakaru datus saskaņā ar 1984. gada Telekomunikāciju likuma [*Telecommunications Act 1984*] 94. pantu un masveida personas datus. *IPT* nosprieda, ka, pamatojoties uz tās atzinumu, režīmi atbilda Konvencijas 8. pantam. Tomēr tā noteica šādas četras prasības, kas, šķiet, izrietējušas no EST sprieduma lietā “Vatsons [*Watson*] un citi” un pārsniedz Konvencijas 8. pantā noteiktās prasības, proti, nemērķētas piekļuves masveida datiem ierobežošana, nepieciešamība saņemt iepriekšēju atļauju (izņemot gadījumus, kad pamatoti konstatēti ārkārtas apstākļi) pirms piekļuves datiem, turpmāka skarto personu informēšana un visu datu saglabāšana Eiropas Savienībā.

236. 2017. gada 30. oktobrī *IPT* vērsās EST ar lūgumu sniegt prejudiciālu nolēmumu, lūdzot precizēt apmēru, kādā varētu piemērot spriedumā lietā “Vatsons” noteiktās prasības tad, kad jāizmanto datu masveida iegūšanas un automātiskās apstrādes metodes, lai aizsargātu valsts drošību. Šādi rīkojoties, tā pauda nopietnas bažas par to, ka tad, ja spriedumā lietā “Vatsons” noteiktās prasības piemērotu pasākumiem, ko veic, lai garantētu valsts drošību, tās šos pasākumus padarītu neefektīvus un pakļautu dalībvalstu valsts drošību riskam. Tā īpaši uzsvēra datu masveida iegūšanas ieguvumus valsts drošības kontekstā, risku, ka iepriekšējas atļaujas nepieciešamība varētu traucēt izlūkdienestu spēju kontrolēt noteiktus draudus valsts drošībai, bīstamību un nepraktiskumu, kas rodas, izpildot prasību ziņot par masveida datubāzes iegūšanu vai izmantošanu, jo īpaši tad, kad apdraudēta valsts drošība, kā arī to, kā kāds absolūts šķērslis datu pārsūtīšanai ārpus Eiropas Savienībai varētu ietekmēt dalībvalstu līgumsaistības.

237. 2019. gada 9. septembrī notika publiska paskaidrojumu uzklausīšana. Lieta “Privacy International” tika izskatīta kopā ar lietām C‑511/18 un C‑512/18 ““La Quadrature du Net” un citi” un C‑520/18 ““Ordre des barreaux francophones et germanophone” un citi”, kas tāpat attiecās uz Direktīvas 2002/58 piemērošanu darbībām, kas saistītas ar valsts drošību un terorisma apkarošanu. Tiesvedībā attiecīgo valstu atbalstam iesaistījās trīspadsmit valstis.

238. Divi atsevišķi spriedumi tika pasludināti 2020. gada 6. oktobrī. Spriedumā lietā “Privacy International” EST atzina, ka valsts tiesiskais regulējums, kas uzliek elektronisko sakaru pakalpojumu sniedzējiem par pienākumu pārsūtīt datplūsmas datus un atrašanās vietas datus drošības un izlūkošanas aģentūrām, lai aizsargātu valsts drošību, ietilpst direktīvas par privātās dzīves neaizskaramību un elektroniskajiem sakariem piemērošanas jomā. Interpretējot šo direktīvu, bija jāņem vērā Hartas 7. pantā garantētās tiesības uz privātās dzīves neaizskaramību, 8. pantā garantētās tiesības uz personas datu aizsardzību, kā arī 11. pantā garantētās tiesības uz vārda brīvību. Ierobežojumiem šo tiesību īstenošanai bija jābūt noteiktiem tiesību aktos, ņemot vērā šo tiesību būtību, un tiem jābūt samērīgiem un nepieciešamiem un patiešām jāatbilst vispārējo interešu mērķiem, ko atzinusi Eiropas Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības. Turklāt personas datu aizsardzības ierobežojumi jāpiemēro vienīgi absolūti nepieciešamajā apmērā, un, lai izpildītu samērīguma prasību, tiesiskajam regulējumam ir jāparedz skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma tvērumu un piemērošanu un paredz minimālās prasības, lai tā rezultātā personām, kuru personas dati tikuši pārsūtīti, ir pieejamas pietiekamas garantijas, kas ļaus šos datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku.

239. EST ieskatā valsts tiesiskais regulējums, kas uzliek elektronisko sakaru pakalpojumu sniedzējiem par pienākumu izpaust drošības un izlūkošanas aģentūrām datplūsmas datus un atrašanās vietas datus, veicot vispārēju un neselektīvu pārsūtīšanu, kas ietekmējusi visas personas, kuras izmanto elektronisko sakaru pakalpojumus, pārsniedz absolūti nepieciešamo apmēru un nav uzskatāms par pamatotu, kā to nosaka direktīva par privātās dzīves neaizskaramību un elektronisko saziņu, to aplūkojot kopā ar Hartu.

240. Tomēr spriedumā lietā ““La Quadrature du Net” un citi” EST apstiprināja, ka, lai gan direktīva par privātās dzīves neaizskaramību un elektronisko saziņu, to aplūkojot kopā ar Hartu, aizliedz tiesību aktus, kas paredz vispārēju un neselektīvu datplūsmas datu un atrašanās vietas datu saglabāšanu situācijās, kad attiecīgā dalībvalsts sastopas ar nopietniem draudiem valsts drošībai, kuri izrādās patiesi un faktiski vai paredzami, tā neaizliedz tiesību aktus, kas uzliek pakalpojumu sniedzējiem par pienākumu vispārēji un neselektīvi saglabāt datplūsmas datus un atrašanās vietas datus uz laiku, kas ir absolūti nepieciešams, bet ko varētu pagarināt, ja draudi turpinātu pastāvēt. Lai apkarotu smagus noziegumus un novērstu nopietnus draudus sabiedrības drošībai, dalībvalstis uz laiku, kas nepārsniedz absolūti nepieciešamo, arī varēja paredzēt datplūsmas datu un atrašanās vietas datu mērķorientētu saglabāšanu, pamatojoties uz objektīviem un nediskriminējošiem elementiem, ņemot vērā attiecīgo personu kategorijas vai ģeogrāfisko kritēriju, vai interneta savienojuma avotam piešķirtās IP adreses. Tāpat dalībvalsts varēja vispārēji un nespecifiski saglabāt datus par lietotāju pilsonisko identitāti ar elektronisko sakaru starpniecību, nenosakot datu saglabāšanai konkrētu laika periodu.

241. Turklāt direktīvai par privātās dzīves neaizskaramību un elektronisko saziņu, to aplūkojot kopā ar Hartu, nav pretrunā valsts tiesību akti, kas uzliek elektronisko sakaru pakalpojumu sniedzējiem par pienākumu, pirmkārt, veikt datplūsmas datu un atrašanās vietas datu automatizētu analīzi un apkopošanu reāllaikā un, otrkārt, reāllaikā apkopot tehniskos datus par izmantoto gala iekārtu atrašanās vietu, ja analīze attiecas vienīgi uz situācijām, kurās dalībvalsts saskaras ar nopietniem draudiem valsts drošībai, kas izrādās patiesi un faktiski vai paredzami, un šīs analīzes izmantošanu var efektīvi pārbaudīt vai nu tiesa, vai neatkarīga administratīva iestāde, kuras lēmumam ir saistoša iedarbība, un datplūsmas datu un atrašanās vietas datu apkopošana reāllaikā attiecas vienīgi uz personām, attiecībā uz kurām ir pamatots iemesls aizdomām, ka tās kaut kādā veidā ir iesaistītas terorisma darbībās, un tā ir pakļauta iepriekšējai pārbaudei, ko veic vai nu tiesa, vai neatkarīga administratīva iestāde, kuras lēmumam ir saistoša iedarbība.

IV. PIEMĒROJAMIE SALĪDZINĀMIE TIESĪBU AKTI UN PRAKSE

A. Līgumslēdzējas valstis

242. Vismaz septiņas līgumslēdzējas valstis (Somija, Francija, Vācija, Nīderlande, Zviedrija, Šveice un Apvienotā Karaliste) oficiāli īsteno masveida pārtveršanas režīmus ar kabeļu un/vai gaisa līniju starpniecību.

243. Vienā citā valstī (Norvēģijā) tiek apspriests likumprojekts – ja tas tiks pieņemts, tas atļaus veikt masveida pārtveršanu.

244. Sīkāka informācija par Zviedrijas sistēmu ir ietverta spriedumā lietā ““Centrum för rättvisa” pret Zviedriju” (pieteikums Nr. 35252/08), savukārt sīkāka informācija par Vācijas sistēmu ir izklāstīta turpmāk 247.–252. punktā.

245. Attiecībā uz izlūkdatu apmaiņas līgumiem vismaz trīsdesmit deviņas līgumslēdzējas valstis ir vai nu noslēgušas izlūkdatu apmaiņas līgumus ar citām valstīm, vai arī tām ir iespēja šādus līgumus noslēgt. Divas no tām nepārprotami aizliedz, bet divas – nepārprotami atļauj valstij vērsties pie kādas citas valsts, lai tās vārdā pārtvertu materiālu. Pārējās valstīs šī nostāja nav skaidra.

246. Visbeidzot, vairumā valstu piemērojamie drošības pasākumi kopumā ir tādi paši kā attiecībā uz iekšzemes darbībām, paredzot dažādus ierobežojumus saņemto datu izmantošanai un atsevišķos gadījumos pienākumu tos iznīcināt, ja tie vairs nav aktuāli.

B. Vācijas Federālās Konstitucionālās tiesas 2020. gada 19. maija spriedums (1 BvR 2835/17)

247. Šajā spriedumā Konstitucionālā tiesa izvērtēja, vai ar Federālā izlūkdienesta pilnvarām veikt ārvalstu telekomunikāciju stratēģisku (jeb “sakaru”) izlūkošanu tikušas pārkāptas Pamatlikumā [*Grundgesetz*] noteiktās pamattiesības.

248. Attiecīgais režīms attiecās gan uz satura, gan uz saistīto sakaru datu pārtveršanu, un tā mērķis bija vienīgi pārraudzīt ārvalstu telekomunikāciju ārpus Vācijas teritorijas. Šādu uzraudzību varēja veikt, lai iegūtu informāciju par jautājumiem, kas Federālās valdības ieskatā ir svarīgi valsts ārpolitikai un drošības politikai. Tomēr to arī varēja veikt attiecībā uz konkrētām personām. Uzraudzības rīkojumu pieļaujamību un nepieciešamību kontrolēja neatkarīga komiteja. Saskaņā ar Konstitucionālās tiesas spriedumu pēc datu pārtveršanas tika īstenots pilnībā automatizēts vairāku posmu filtrēšanas un izvērtēšanas process. Šim nolūkam Federālais izlūkdienests izmantoja meklēšanas vārdus sešciparu skaitļa apmērā, ko kontrolēja iekšējā apakšnodaļa, kuras uzdevums bija nodrošināt, lai saikne starp izmantotajiem meklēšanas vārdiem un datu pieprasīšanas mērķi tiktu paskaidrota saprātīgi un visaptveroši. Pēc tam, kad tika iesniegts pieteikums automātiskā filtrēšanas procesa veikšanai, pārtvertais materiāls tika vai nu dzēsts, vai uzglabāts, vai arī nosūtīts analītiķim izvērtēšanai.

249. Par pārtvertā materiāla apmaiņu ar ārvalstu izlūkdienestiem bija noslēgts sadarbības līgums, kurā bija jāietver ierobežojumi un garantijas, lai nodrošinātu, ka dati ir apstrādāti un dzēsti atbilstoši tiesiskuma principam.

250. Konstitucionālā tiesa nosprieda, ka attiecīgais režīms neatbilda Pamatlikumam. Lai gan tā atzina, ka efektīva ārvalstu izlūkdatu vākšana notika vispārīgās sabiedrības interesēs, tā tomēr *inter alia* uzskatīja, ka režīms neattiecās uz pietiekami konkrētiem mērķiem, proti, tas nebija strukturēts tā, lai paredzētu atbilstošu pārraudzību un kontroli, turklāt nav paredzēti vairāki drošības pasākumi, jo īpaši saistībā ar žurnālistu, advokātu un citu personu aizsardzību, kuru saziņas aktu saturam bija nepieciešama īpaša konfidencialitātes aizsardzība.

251. Attiecībā uz ārvalsts izlūkošanas rezultātā iegūto izlūkdatu apmaiņu tiesa atkal secināja, ka nav noteikti drošības pasākumi. Proti, nebija pietiekami skaidri precizēts, kādos gadījumos ar svarīgām interesēm var pamatot datu pārsūtīšanu. Turklāt, lai gan tiesa neuzskatīja, ka saņēmējā valstī ir jābūt ieviestiem salīdzināmiem noteikumiem par personas datu apstrādi, tā tomēr uzskatīja, ka datus varēja pārsūtīt uz ārvalstīm vienīgi tad, ja bija nodrošināts atbilstošs datu aizsardzības līmenis un nebija iemesla bažām par to, ka informāciju varētu izmantot, lai pārkāptu tiesiskuma pamatprincipus. Aplūkojot šo jautājumu plašāk, proti, izlūkdatu apmaiņas kontekstā, tiesa uzskatīja, ka sadarbība ar ārvalstīm nav jāīsteno, lai apdraudētu iekšējos drošības pasākumus, un, ja Federālais izlūkdienests vēlējās izmantot meklēšanas vārdus, ko tai norādījis ārvalstu izlūkdienests, tam vispirms bija jāapstiprina, ka starp meklēšanas vārdiem un datu pieprasīšanas mērķi patiešām pastāv saikne un ka iegūtie dati neliecina par īpašu nepieciešamību ievērot konfidencialitāti (piemēram, tādēļ, ka tie attiecās uz trauksmes cēlējiem vai disidentiem). Lai gan tiesa neizslēdza iespēju par datu masveida pārsūtīšanu ārvalstu izlūkdienestiem, tā atzina, ka tas nevarēja būt nepārtraukts process, kas īstenots vienam nolūkam.

252. Visbeidzot tiesa atzina, ka attiecībā uz pārskatāmajām uzraudzības pilnvarām arī trūka plaša neatkarīga un pastāvīga pārraudzība, lai nodrošinātu, ka tiek ievēroti attiecīgie tiesību akti, un kompensētu to, ka faktiski trūkst drošības pasākumu, ko parasti garantē tiesiskuma princips. 564Likumdevējam bija jāparedz divi dažādi pārraudzības veidi, kuriem bija jāizpaužas arī organizatoriskajā struktūrā, proti, tiesai līdzīga struktūra, kuras uzdevums ir īstenot pārraudzību un pieņemt lēmumu formālā procedūrā, nodrošinot *ex ante* vai *ex post* tiesisko aizsardzību, un, otrkārt, pārraudzība, kas pēc būtības ir administratīva un varētu paredzēt, ka pēc pašu iniciatīvas pēc nejaušības principa tiek pārbaudīta visa stratēģiskās uzraudzības procesa likumība. Konstitucionālās tiesas ieskatā noteiktiem galvenajiem procesuālajiem posmiem principā būtu nepieciešama tiesai līdzīgas struktūras *ex ante* atļauja, proti, dažādu uzraudzības pasākumu formāla noteikšana (netika izslēgti izņēmumi steidzamības gadījumos), meklēšanas vārdu izmantošana, ciktāl tie ir tieši vērsti uz personām, kuras varētu radīt apdraudējumu, kas līdz ar to būtu Federālā izlūkdienesta tiešajās interesēs, kā arī tādu meklēšanas vārdu izmantošana, kas tieši attiecas uz personām, kuru saziņas aktu saturam nepieciešama īpaša konfidencialitātes aizsardzība, un tādu ar žurnālistiem, advokātiem un citu profesiju pārstāvjiem saistītu datu apmaiņa ar ārvalstu izlūkdienestiem, kam nepieciešama īpaša konfidencialitātes aizsardzība.

C. Hāgas Apelācijas tiesas 2017. gada 14. marta spriedums

253. Vairākas personas un asociācijas apgalvoja, ka Nīderlandes izlūkošanas un drošības dienesti rīkojušies pretlikumīgi, saņemot datus no ārvalstu izlūkošanas un drošības dienestiem, jo īpaši *NSA* un *GCHQ*, kuri to ieskatā datus bija vai varēja būt saņēmuši “neatļautā” vai “pretlikumīgā” veidā. Prasītāji neapstrīdēja, ka *NSA* un *GCHQ* darbības saskaņā ar valsts tiesību aktiem bija “prettiesiskas” vai “pretlikumīgas”, bet gan drīzāk to, ka *NSA* ar savu rīcību bija pārkāpusi Starptautisko paktu par pilsoniskajām un politiskajām tiesībām (turpmāk tekstā – “*ICCPR*”) un *GCHQ* ar savu rīcību bija pārkāpusi Konvenciju. Prasītāji *inter alia* atsaucās uz “Snoudena atklāto informāciju” (skat. iepriekš 12. punktu).

254. 2014. gada 23. jūlijā Hāgas tiesa noraidīja prasītāju prasības (ECLI:NL:RBDHA:2014:8966). Viņu apelācijas sūdzību pret šo spriedumu Hāgas apelācijas tiesa noraidīja 2017. gada 14. martā (ECLI:NL:GHDHA:2017:535).

255. Apelācijas tiesa uzskatīja, ka principā ir jātic, ka Amerikas Savienotās Valstis un Apvienotā Karaliste ievērotu savus pienākumus, kas noteikti šajos nolīgumos. Šādu uzticību vajadzētu apšaubīt vienīgi tad, ja konstatēti pietiekami konkrēti apstākļi, lai uzskatītu, ka tā nav pamatota.

256. Attiecībā uz *NSA* veikto telekomunikāciju datu apkopošanu nebija skaidru norāžu, ka *NSA* ar savu rīcību bija pārkāpusi *ICCPR*. Ciktāl prasītāji bija centušies iebilst, ka likumā noteiktās pilnvaras, uz ko bija balstīta datu apkopošana, bija plašākas, nekā to pieļauj *ICCPR*, tie nebija pietiekami paskaidrojuši, kādā ziņā attiecīgie normatīvie akti bijuši neatbilstoši.

257. Attiecībā uz *GCHQ* veikto datu apkopošanu prasītāji nekādi nebija pamatojuši savu prasību par to, ka *GCHQ* ar savu rīcību bija pārkāpusi Konvenciju.

258. Līdz ar to prasītāji nebija pierādījuši, ka veids, kādā *NSA* un *GCHQ* bija rīkojušās, vismaz principā bija pretrunā ar *ICCPR* un Konvenciju. Lai gan nevarēja izslēgt, ka konkrētā gadījumā *NSA* vai *GCHQ*, vai arī jebkurš cits ārvalstu izlūkdienests būtu varējis apkopot datus pretēji *ICCPR* vai Konvencijai, saskaņā ar uzticības principu šāda iespējamība vien nevarēja liecināt par to, Nīderlandes izlūkdienesti nevarēja saņemt datus no ārvalstu izlūkdienestiem, katrā atsevišķā gadījumā nepārbaudot, vai šie dati ir iegūti, nepārkāpjot attiecīgos nolīgumā noteiktos pienākumus.

259. Visbeidzot Apelācijas tiesa atzina, ka, pat ja ārvalstu izlūkdienesti rīkojās savu likumā noteikto pilnvaru un nolīgumā noteikto pienākumu ietvaros, tas, ka šīs likumā noteiktās pilnvaras var būt plašākas par Nīderlandes izlūkdienestu pilnvarām, zināmos apstākļos varētu radīt bažas. Piemēram, varēja uzskatīt, ka Nīderlandes izlūkdienesti rīkotos pretēji 2002. gada Izlūkošanas un drošības dienestu likumam [*Intelligence and Security Services Act 2002*] (vai tā būtībai), ja tie sistemātiski vai apzināti saņemtu no ārvalstu izlūkošanas aģentūrām datus par Nīderlandes iedzīvotājiem, ņemot vērā, ka tie nav apkopojuši šos datus savu pilnvaru ietvaros. Šādā gadījumā ierobežojumi, kas izlūkdienestiem noteikti saskaņā ar 2002. gada likumu, varētu zaudēt jēgu. Tomēr prasītāji nebija pamatojuši vai pierādījuši, ka Nīderlandes izlūkdienesti sistemātiski vai apzināti izmantoja šādu neatbilstību starp Nīderlandes un ārvalstu tiesību aktiem.

260. Kasācijas sūdzību, kuras pamatā galvenokārt bija apgalvojums, ka Apelācijas tiesa, iespējams, bija kļūdaini interpretējusi prasītāju prasību, un viņiem uzliktās pierādījumu nastas apmērs, “Hoge Raad” (Augstākā tiesa) noraidīja 2018. gada 7. septembrī (ECLI:NL:HR:2018:1434).

D. Amerikas Savienotās Valstis

261. Amerikas Savienoto Valstu izlūkdienesti izmanto programmu “Upstream” saskaņā ar *FISA* 702. pantu.

262. Valsts izlūkošanas ģenerāladvokāts un direktors katru gadu izdod apliecinājumus, saskaņā ar ko atļauts izlūkot personas, kuras nav ASV pilsoņi un par kurām ir pamats uzskatīt, ka tās atrodas ārpus Amerikas Savienotajām Valstīm. Šīm amatpersonām nav pienākuma minēt *FISC* konkrētas izlūkojamās personas, kuras nav ASV pilsoņi. Tām arī nav pienākuma pierādīt iespējamo iemeslu tam, lai uzskatītu, ka izlūkojamā persona ir ārvalsts aģents. Tā vietā 702. pantā minētajos apliecinājumos ir noteiktas apkopojamās informācijas kategorijas, kurām jāatbilst likumā noteiktajai ārvalstu izlūkdatu definīcijai. Atļautajos apliecinājumos ir bijusi iekļauta informācija par starptautisko terorismu un masu iznīcināšanas ieroču iegādi.

263. Saskaņā ar atļauju *NSA* ar likumā noteiktu palīdzību, ko sniedz pakalpojumu sniedzēji, kopē un meklē interneta datplūsmas straumējumus kā datu plūsmas visā internetā. Tiek apkopoti gan tālruņu zvani, gan interneta sakari. Līdz 2017. gada aprīlim *NSA* ieguva interneta transakcijas “uz”, “no” vai “par” attiecīgo selektoru. “Uz” un “no” sakari bija sakari, attiecībā uz kuriem sūtītājs vai saņēmējs 702. panta izpratnē bija attiecīgā selektora lietotājs. Savukārt “par” sakari bija sakari, kuros iegūtajā interneta transakcijā bija norāde uz attiecīgo selektoru, bet mērķis ne vienmēr bija sakaru dalībnieks. Līdz ar to “par” sakari ietvēra visā internetā cirkulējošo saziņas aktu satura meklēšanu. Tomēr no 2017. gada aprīļa *NSA* nebija saņēmusi vai apkopojusi saziņas aktu saturu, kas bija vienīgi “par” mērķi. Turklāt *NSA* norādīja, ka tā šā ierobežojuma ietvaros pēc iespējas ātrāk dzēš vairumu interneta saziņas aktu satura, kas iepriekš iegūts, izmantojot programmu “Upstream”.

264. 702. pants uzliek Valdībai par pienākumu izstrādāt mērķu noteikšanas un ietekmes mazināšanas procedūras, ko pārskata *FISC*.

265. Izpildrīkojums Nr. 12333, kas tika parakstīts 1981. gadā, ļauj apkopot, saglabāt un izplatīt informāciju, kas iegūta likumīgas ārvalstu izlūkošanas, pretizlūkošanas, starptautiskās narkotiku vai starptautiskā terorisma izmeklēšanas gaitā. Saskaņā ar *FISA* uz ārvalstu pilsoņu uzraudzību atbilstoši izpildrīkojumam Nr. 12333 neattiecas attiecīgās valsts regulējums. Nav zināms, cik daudz datu ir apkopots atbilstoši izpildrīkojumam Nr. 12333 salīdzinājumā ar datiem, kas apkopoti saskaņā ar 702. pantu.

1. TIESĪBU AKTI

266. Kopumā pieteikuma iesniedzēji trīs apvienotajās lietās sūdzējās par trīs diskrētu režīmu neatbilstību 8. un 10. pantam, proti, režīmu par sakaru masveida pārtveršanu saskaņā ar 2000. gada Likuma par izmeklēšanas pilnvaru regulējumu [*Regulation of Investigatory Powers Act 2000*] (turpmāk tekstā – “*RIPA*”) 8. panta 4. punktu, režīmu par izlūkdatu saņemšanu no ārvalstu izlūkdienestiem un režīmu par sakaru datu iegūšanu no sakaru pakalpojumu sniedzējiem (SPS).

267. Pirms katra minētā režīma izvērtēšanas Lielā palāta vispirms pievērsīsies primārajam jautājumam.

I. LIELĀS PALĀTAS IZVĒRTĒJAMAIS SĀKOTNĒJAIS JAUTĀJUMS

268. Saskaņā ar Tiesas pastāvīgo judikatūru Lielajai palātai nodotā “lieta” ietver visus pieteikuma aspektus, ko palāta iepriekš izvērtējusi savā spriedumā. Lielajai palātai nodotā “lieta” ir pieteikums, kas atzīts par pieņemamu, kā arī sūdzības, kas nav atzītas par nepieņemamām (skat. 2020. gada 25. jūnija sprieduma lietā Nr. 60561/14 “S. M. pret Horvātiju” [*GC*] 216. punktu un tajā minētās iestādes).

269. Pieteikuma iesniedzēji šajā lietā iesniedza savas sūdzības attiecīgi 2013., 2014. un 2015. gadā. Šīs sūdzības galvenokārt attiecās uz valsts uzraudzības darbībām saskaņā ar *RIPA* un saistītajiem prakses kodeksiem. Prakses kodeksi pēc tam tika grozīti. Proti, 2016. gada 29. novembrī 2016. gada Izmeklēšanas pilnvaru likumam (turpmāk tekstā – “*IPA*”) tika sniegta karaliskā piekrišana, un tā noteikumi stājās spēkā 2016. gada decembrī. *IPA* noteiktie jaunie uzraudzības režīmi lielākoties stājās spēkā līdz 2018. gada vasarai. *RIPA* I daļas I nodaļas noteikumi tika atcelti 2018. gada gaitā.

270. Palāta pārskatīja Konvencijas atbilstību spēkā esošajam likumam dienā, kad tā izvērtēja pieteikuma iesniedzēju sūdzību pieņemamību, proti, tā ņēma vērā likumu tā 2017. gada 7. novembra redakcijā. Tā kā šis ir “pieteikums, kas atzīts par pieņemamu”, Lielajai palātai tas arī ir jāizvērtē, ņemot vērā tiesisko regulējumu tā 2017. gada 7. novembra redakcijā. Tā šajā gadījumā ir piemērota pieeja, jo tiesiskie regulējumi, kas pakāpeniski ieviesti pēc *IPA* stāšanās spēkā, pašlaik tiek apstrīdēti valsts tiesās, un Lielā kamera nevar izvērtēt jauno tiesisko regulējumu, pirms to vispirms nav veikušas minētās tiesas.

271. Pieteikuma iesniedzēji nav apstrīdējuši palātas atzinumu, ka Izmeklēšanas pilnvaru tiesa (*IPT*) pašlaik ir efektīvs tiesiskās aizsardzības līdzeklis gan attiecībā uz atsevišķām sūdzībām, gan vispārīgām sūdzībām par uzraudzības režīma atbilstību Konvencijai, savukārt Valdība nav apstrīdējusi tās atzinumu, ka, ņemot vērā lietas apstākļus, pieteikuma iesniedzēji bija izmantojuši iekšējos tiesiskās aizsardzības līdzekļus Konvencijas 35. panta 1. punkta izpratnē. Līdz ar to Lielajai palātai nav jāizskata neviens no šiem jautājumiem.

II. SAKARU MASVEIDA PĀRTVERŠANA

A. Teritoriālā jurisdikcija

272. Attiecībā uz 8. panta 4. punktā noteikto režīmu Valdība neizvirzīja nekādus iebildumus saskaņā ar Konvencijas 1. pantu un neapgalvoja, ka sakaru pārtveršana notika ārpus valsts teritoriālās jurisdikcijas. Turklāt Lielās palātas sēdes laikā Valdība skaidri apstiprināja, ka tā šajā sakarā nav izvirzījusi iebildumus, jo vismaz daži no pieteikuma iesniedzējiem nepārprotami atradušās valsts teritoriālajā jurisdikcijā. Līdz ar to šajā lietā Tiesa sniegs izvērtējumu, pieņemot, ka sūdzībā norādītie jautājumi ietilpst Apvienotās Karalistes jurisdikcijas kompetencē, ciktāl pieteikuma iesniedzēji iesnieguši sūdzības par 8. panta 4. punktā noteikto režīmu.

B. Konvencijas 8. panta iespējamais pārkāpums

273. Pieteikuma iesniedzēji visās trīs apvienotajās lietās apgalvoja, ka sakaru masveida pārtveršanas režīms nebija saderīgs ar Konvencijas 8. pantu, kas nosaka:

“1. Ikvienam ir tiesības uz savas privātās un ģimenes dzīves, dzīvokļa un korespondences neaizskaramību.

2. Sabiedriskās institūcijas nedrīkst traucēt nevienam baudīt šīs tiesības, izņemot gadījumos, kas paredzēti likumā un ir nepieciešami demokrātiskā sabiedrībā, lai aizstāvētu valsts drošības, sabiedriskās kārtības vai valsts labklājības intereses, lai nepieļautu nekārtības vai noziegumus, lai aizsargātu veselību vai morāli vai lai aizstāvētu citu tiesības un brīvības.”

1. Palātas spriedums

274. Palāta skaidri atzina, ka valstīm ir plaša rīcības brīvība, lemjot par to, kāds pārtveršanas režīms nepieciešams valsts drošības aizsardzībai, taču tā uzskatīja, ka valstīm piešķirtā rīcības brīvība, izmantojot pārtveršanas režīmu, noteikti būtu šaurāka. Tā šajā ziņā norādīja, ka Tiesa ir noteikusi sešus “minimālos drošības pasākumus”, kuriem jābūt noteiktiem likumā, lai izvairītos no pilnvaru ļaunprātīgas izmantošanas, proti, to nodarījumu būtība, kas var būt par pamatu pārtveršanas rīkojuma izdošanai, to personu kategorijas, kuru sakarus var pārtvert, pārtveršanas ilguma ierobežojums, iegūto datu pārbaudes, izmantošanas un uzglabāšanas kārtība, veicamie piesardzības pasākumi, paziņojot datus citām pusēm, un apstākļi, kādos pārtvertos datus atļauts vai ir pienākums dzēst vai iznīcināt. Tiesa šos drošības pasākumus, kas pirmo reizi bija izklāstīti 1990. gada 24. aprīļa sprieduma lietā “Huvigs [*Huvig*] pret Franciju” 34. punktā, A sērija Nr. 176 B, un 1990. gada 24. aprīļa sprieduma lietā “Krulēns [*Kruslin*] pret Franciju” 35. punktā, A sērija Nr. 176-A, bija regulāri piemērojusi savā judikatūrā par sakaru pārtveršanu un divās lietās, kas konkrēti attiecas uz sakaru masveida pārtveršanu (skat. lēmumu lietā Nr. 54934/00 “Vēbere un Sarāvija pret Vāciju” (lēmums), ECT 2006-XI, un 2008. gada 1. jūlija spriedumu lietā Nr. 58243/00 ““Liberty” un citi pret Apvienoto Karalisti”).

275. Palātas ieskatā lēmums izmantot masveida pārtveršanas režīmu ietilpa līgumslēdzējām valstīm piešķirtās rīcības brīvības robežās. Tā izvērtēja Apvienotās Karalistes masveida pārtveršanas režīma darbību, atsaucoties uz sešiem minimālajiem drošības pasākumiem, kas minēti iepriekšējā punktā. Tā kā pirmie divi drošības pasākumi tā īsti neattiecās uz masveida pārtveršanu, palāta pārstrukturēja šos drošības pasākumus, ņemot vērā, pirmkārt, vai pamatojums, atbilstoši kuram varētu izdot orderi, ir pietiekami skaidrs, otrkārt, vai valsts tiesību aktos pilsoņiem sniegta atbilstoša norāde par apstākļiem, kādos viņu sakari var tikt pārtverti, un, treškārt, vai valsts tiesību aktos pilsoņiem sniegta atbilstoša norāde par apstākļiem, kādos viņu sakari var tikt atlasīti pārbaudei. Turklāt, ņemot vērā neseno judikatūru (tostarp spriedumu lietā Nr. 47143/06 “Romāns Zaharovs [*Roman Zakharov*] pret Krieviju” [*GC*], ECT 2015), palāta arī ņēma vērā slepenās uzraudzības pasākumu īstenošanas pārraudzības kārtību, paziņošanas mehānismu esību un valsts tiesību aktos paredzētos tiesiskās aizsardzības līdzekļus.

276. Tā 8. panta 4. punktā noteiktajā režīmā konstatēja divus problemātiskus aspektus, pirmkārt, netika pārraudzīts veids, kādā atlasīti pārtveršanai paredzētie nesēji un pārtverto sakaru filtrēšanai izmantotie selektori un process, kādā analītiķi atlasīja pārtvertos sakarus pārbaudei, un, otrkārt, nebija ieviesti reāli drošības pasākumi, kas piemērojami uz saistīto sakaru datu meklēšanu un atlasīšanu pārbaudei. Ņemot vērā neatkarīgo pārraudzību, ko nodrošināja komisārs sakaru pārtveršanas jautājumos (*IC*) un *IPT*, un plašo neatkarīgo izmeklēšanu, ko veica pēc tam, kad Edvards Snoudens bija atklājis informāciju, palāta secināja, ka Apvienotā Karaliste nebija ļaunprātīgi izmantojusi masveida pārtveršanas pilnvaras. Tomēr, ņemot vērā iepriekš minētos trūkumus, tā atzina, ka masveida pārtveršanas režīms lielākoties neatbilda “tiesību aktu kvalitātes” prasībai un nespēja pamatot “iejaukšanos”, kas “nepieciešama demokrātiskā sabiedrībā”.

2. Pušu argumenti

a) Pieteikuma iesniedzēji

277. Pieteikuma iesniedzēji apgalvoja, ka masveida pārtveršana Konvencijas 8. panta nozīmē principā nebija nedz nepieciešama, nedz samērīga un ka tā neietilpa valsts rīcības brīvības robežās.2016. gada 12. janvāra spriedumā lietā Nr. 37138/14 “Zabo [*Szabó*] un Visija [*Vissy*] pret Ungāriju” bija norādīts, ka slepenās uzraudzības pasākumiem jābūt “absolūti nepieciešamiem”, lai aizsargātu demokrātiskās institūcijas un iegūtu svarīgus izlūkdatus, un ka nebija pierādīts, ka masveida pārtveršana šim nosacījumam atbilda. Lai gan tā neapšaubāmi bija noderīga spēja, no Tiesas judikatūras skaidri izrietēja, ka ne viss, kas izlūkdienestiem ir noderīgs, ir pieļaujams demokrātiskā sabiedrībā (skat. spriedumu lietā Nr. 30562/04 un Nr. 30566/04 “S. un Mārpers [*Marper*] pret Apvienoto Karalisti” [*GC*], ECT 2008).

278. Pieteikuma iesniedzēji apgalvoja, ka atsevišķa iejaukšanās 8. pantā noteiktajās tiesībās uz privātās dzīves un korespondences neaizskaramību bija notikusi, veicot sakaru (satura un/vai saistīto sakaru datu) pārtveršanu, uzglabāšanu, automātisko apstrādi un pārbaudi. Lai gan viņi piekrita, ka “būtiska” iejaukšanās notika pārtverto sakaru pārbaudes brīdī, viņi uzskatīja, ka bija nepareizi apgalvot, ka pirms tam nenotika “nozīmīga” iejaukšanās. Gluži pretēji, no Tiesas judikatūras izriet, ka pat tad, ja valsts uzglabā personas datus, šāda rīcība ir kvalificējama kā būtiska iejaukšanās personas tiesībās, kas garantētas Konvencijas 8. pantā (skat., piemēram, spriedumu lietā Nr. 28341/95 “Rotaru pret Rumāniju” [*GC*], ECT 2000 V, un iepriekš minētajā lietā “S. un Mārpers”). Tas tā bija īpaši gadījumos, kad dati tika apstrādāti automātiski. Patiesībā, ņemot vērā apstrādes jaudas un mašīnmācīšanās straujo attīstību, datu uzglabāšana un elektroniskā apstrāde pašas par sevi var būt ļoti aizkarošas, nevienai personai neizskatot pamatsaturu vai saistītos sakaru datus. Šajā ziņā pieteikuma iesniedzēji apgalvoja, ka pretēji “amorfajam veidojumam”, uz ko atsaucās Valdība (skat. turpmāk 288. punktu), apkoptie dati vairāk līdzinās “labi organizētai un indeksētai bibliotēkai, kurā var ātri atrast visu nepieciešamo informāciju”. Viņi norādīja, ka automātiskās apstrādes pieejamība rada īpaši lielas bažas par privātās dzīves neaizskaramību un, kā apgalvoja Valdība, nemazina iejaukšanos.

279. Pieteikuma iesniedzēji apgalvoja, ka tad, ja masveida pārtveršanas režīms Lielās palātas ieskatā ietilpa valsts rīcības brīvības robežās, 8. panta 4. punktā noteiktais režīms neatbilda likumam. Pirmkārt, *RIPA* bija pārlieku sarežģīts, ko atzinuši visi neatkarīgie pārskatītāji; patiesībā tik sarežģīts, ka veicamās uzraudzības būtība un ietvars kļuva skaidri zināmi tikai pēc tam, kad Edvards Snoudens bija atklājis informāciju. Turklāt “zem ūdenslīnijas” esošos pasākumus noteikusi pati *GCHQ*; tie arī nebija pieejami parlamentam, un parlaments tos nebija apstiprinājis, kā arī tos saskaņā ar iekšējo politiku varēja mainīt pēc izpildvaras gribas, un tie nebija saistoši. Līdz ar to pieteikuma iesniedzēji apgalvoja, ka viņiem nav jāiesaistās Tiesas veicamajā izvērtējumā.

280. Izvērtējot paredzamību, pieteikuma iesniedzēji apgalvoja, ka gan sabiedrības, gan tehnoloģiskās izmaiņas ir iemesls tam, ka Tiesai jāaktualizē pašreizējā pieeja un jāuzlabo nepieciešamie drošības pasākumi, lai nodrošinātu Konvencijā paredzēto tiesību praktiskumu un efektivitāti. Tiesas pašreizējā judikatūra par masveida pārtveršanu izrietēja no lēmuma lietā “Vēbere un Sarāvija” (minēta iepriekš), taču šis lēmums pieņemts 2006. gadā, kad situācija pasaulē bija citāda. Viedtālruņi vēl nebija tik moderni, un to funkcionalitāte bija ierobežota, turklāt “Facebook” izmantoja galvenokārt universitāšu studenti, un “Twitter” vēl bija sākuma stadijā. Pieteikuma iesniedzēji norādīja, ka pašlaik cilvēki lielu savas dzīves daļu pavada tiešsaistē, izmantojot internetu, lai sazinātos, dalītos ar idejām, veiktu pētījumus, uzsāktu attiecības, meklētu medicīniskas konsultācijas, veidotu dienasgrāmatu, organizētu ceļojumu, klausītos mūziku, orientētos konkrētā apvidū un veiktu finanšu darījumus. Turklāt modernās tehnoloģijas rada milzīgu daudzumu sakaru datu, kas ir ļoti izsmeļoši pat tad, ja saistītais saturs netiek pārbaudīts, un ir strukturēti tā, lai datori tos varētu apstrādāt un meklēt tajos sakarības ātrāk un efektīvāk, nekā veicot līdzīgu meklēšanu saturā. Piemēram, mobilie tālruņi nepārtraukti rada sakaru datus, jo tie sazinās mobilajā tīklā, veidojot tālrunī ierakstu par tā atrašanās vietu, kas ļauj sekot līdzi lietotāja kustībai un atklāt viņa interneta lietošanas paradumus.

281. Pieteikuma iesniedzēju ieskatā, aktualizētajiem un uzlabotajiem drošības pasākumiem jāparedz iepriekšēja neatkarīga tiesas atļauja orderiem, selektoru izvēle un pārtvertā materiāla atlasīšana pārbaudei. Turklāt tad, kad selektori vai meklēšanas vārdi attiecas uz kādu konkrētu personu, jābūt objektīviem pierādījumiem par pamatotām šaubām saistībā ar šo personu. Visbeidzot, turpmāk ir jāpaziņo par jebkuru skaidri noteiktu uzraudzības mērķi, ja tas būtiski nekaitē sabiedrības interesēm.

282. Pieteikuma iesniedzēji minēja vairākus Apvienotās Karalistes masveida pārtveršanas režīma elementus, kurus viņi uzskatīja par neatbilstošiem. Pirmkārt, trūkst neatkarīgas uzraudzības atļaujas, nemaz nerunājot par tiesas atļauju. Lai gan tiesas atļauja pati par sevi var nebūt pietiekams drošības pasākums pret ļaunprātīgu izmantošanu, šis apgalvojums nav pamats secinājumam, ka šāda atļauja nav nepieciešams drošības pasākums. Turklāt pieteikuma iesniedzēji uzskatīja, ka *GCHQ* izmantotajiem selektoriem un meklēšanas vārdiem ir jābūt neatkarīgai, ja pat ne tiesas, atļaujai. Tomēr orderī nebija norādīti ne pārtveramie nesēji, ne spēcīgie selektori.

283. Otrkārt, atšķirība starp iekšējiem un ārējiem sakariem ir ne tikai nepietiekami definēta, bet arī bezjēdzīga, jo vairums sakaru, visticamāk, tiks ierindoti “ārējā” kategorijā. Pieteikuma iesniedzēju ieskatā būtu bijis iespējams nodrošināt daudz jēgpilnāku iekšējo saziņas aktu satura aizsardzību. Piemēram, Zviedrijā viss iekšējo saziņas aktu saturs ir nekavējoties jāiznīcina, tiklīdz tas tiek atklāts.

284. Treškārt, ir pieejami ierobežoti drošības pasākumi to personu sakaru saturam, par kurām zināms, ka tās atrodas Britu salās, un attiecībā uz viņu saistītajiem sakaru datiem nav praktiski nekādu drošības pasākumu. *GCHQ* varēja saglabāt visus saistīto sakaru datus, kas iegūti masveida pārtveršanas režīma ietvaros, ievērojot vienīgi ierobežojumus attiecībā uz uzglabāšanas apjomu un maksimālo saglabāšanas periodu. Šos datus, kas bija ļoti aizskaroši, varēja meklēt pēc faktora, kas attiecas uz kādu personu, par kuru zināms, ka tā atrodas Britu salās, bez jebkādas prasības par to, lai valsts sekretārs vispirms apliecina, ka meklēšana ir nepieciešama un samērīga.

285. Ceturtkārt, režīms – ne tiesību aktos, ne detalizēti – neprecizēja, kādam nolūkam materiālu varētu pārbaudīt, un saskaņā ar Parlamenta Izlūkošanas un drošības komiteju (turpmāk tekstā – “*ISC*”) materiāla apraksts valsts sekretāra apliecinājumā bija “vispārīgs”.

286. Visbeidzot, pieteikuma iesniedzēji apgalvoja, ka *IC* komisārs veica tikai daļēju pārraudzību un ka ar ierobežotiem resursiem nav spējis garantēt jēgpilnu un stabilu pārraudzību. Arī *IPT* efektivitāte bija ierobežota, jo tā nevarēja nodrošināt tiesiskās aizsardzības līdzekli saistībā ar iepriekšējas tiesas atļaujas neesību un jebkurā gadījumā personām bija jābūt zināmam pamatam uzskatīt, ka tās ir bijušas pakļautas slepenai uzraudzībai, pirms *IPT* pieņemtu viņu sūdzības.

b) Valdība

287. Valdība uzskatīja, ka masveida pārtveršanas režīmā iegūtā informācija bija ļoti svarīga, lai aizsargātu Apvienoto Karalisti pret draudiem valsts drošībai. Tā ļāva ne tikai atklāt līdz šim nezināmus draudus, bet arī uzraudzīt zināmus mērķus ārpus teritoriālās jurisdikcijas. Elektronisko sakaru pārraides kanāla neparedzamība (un fakts, ka šie sakari bija sadalīti paketēs, ko var pārraidīt pa dažādiem kanāliem) nozīmēja to, ka, lai iegūtu pat nelielu daļu no ārvalstīs esošo zināmo mērķu sakariem, bija jāpārtver visi sakari, kas plūst caur vairākiem izvēlētiem nesējiem. Pēdējos gados vairākas neatkarīgas struktūras ir detalizēti un atkārtoti apsvērušas masveida pārtveršanas pilnvaras, un bija vienprātība par to, ka neviena “alternatīva” (..) “vai alternatīvu kombinācija nebūtu pietiekama, lai aizstātu masveida pārtveršanas pilnvaras kā nepieciešamo izlūkdatu iegūšanas metodi”. Valdība norādīja, ka valstīm pamatoti jāpiešķir plaša rīcības brīvība, izvērtējot, kādas sistēmas ir nepieciešamas, lai aizsargātu sabiedrību pret draudiem, un ka, pakļaujot šīs sistēmas pārbaudei, Tiesai jānodrošina, ka netiek apdraudēta tāda līdzekļa efektivitāte, ar ko iegūst dzīvībai svarīgus izlūkdatus, ko nevarētu iegūt nekādā citā veidā.

288. Valdība apgalvoja, ka sakaru pārtveršana masveida pārtveršanas režīmā būtu radījusi jēgpilnu iejaukšanos personas tiesībās, kas noteiktas 8. pantā, vienīgi tad, ja tās sakari būtu atlasīti pārbaudei (proti, iekļauti to sakaru sarakstā, no kuriem analītiķis varētu izvēlēties pārbaudāmās vienības) vai ja analītiķis tos patiešām pārbaudītu. Nevarētu apgalvot, ka personas tiesības būtu pārkāptas apmērā, kas pārsniedz minimālo apmēru, ja sakaru kopiju vai nu atmestu gandrīz reāllaikā, vai arī saglabātu vispārīgā datu “amorfā veidojumā” ne ilgāk kā dažas dienas, citiem vārdiem sakot, ja sakarus meklētu, izmantojot selektorus un vaicājumus, bet nepārbaudītu vai neizmantotu. Milzīgo sakaru apjomu, kas plūst pa katru pārtverto kabeli, nevarētu “atlasīt pārbaudei”, līdz ar to tas būtu jāatmet.

289. Attiecībā uz nepieciešamajiem drošības pasākumiem Valdība piekrita palātai, ka bija pareizi izvērtēt masveida pārtveršanas režīmu, atsaucoties uz tiem pašiem standartiem, ko bija izstrādājusi Tiesa lietās, kas attiecas uz sakaru mērķētu pārtveršanu. Valdība arī lielākoties piekrita 8. panta 4. punktā noteiktā režīma izvērtējumam, ko palāta bija veikusi, atsaucoties uz šiem standartiem. Tā atkārtoti uzsvēra, ka analītiķis nevarēja izskatīt nekādu saziņas aktu saturu, ja un līdz tas netika atlasīts pārbaudei pēc automātiskā filtrēšanas procesa; atlasīšana un visas tai sekojošās pārbaudes tika ļoti rūpīgi kontrolētas; par saziņas aktu saturu vai sakaru datiem nevarēja sagatavot nevienu izlūkošanas ziņojumu, ja vien tos nebija pārskatījis analītiķis; saskaņā ar *RIPA* 16. panta 2. punktu valsts sekretāram bija pienākums apliecināt sakaru satura meklēšanas nepieciešamību un samērīgumu atbilstoši faktoram, kas attiecas uz kādu personu, par kuru zināms, ka tā atrodas Britu salās, un *ISC*, *IC* komisāra un *IPT* apvienotās pārraudzības funkcijas atbilda Konvencijas prasībām. Piemērojamie drošības pasākumi visos masveida pārtveršanas procesa posmos bija balstīti uz Konvencijā noteiktajiem nepieciešamības un proporcionalitātes principiem. Šie pamatprincipi regulēja materiāla iegūšanu, pārbaudi, izmantošanu, uzglabāšanu, izpaušanu, saglabāšanu un dzēšanu.

290. Attiecībā uz tiem režīma aspektiem, kuri pēc palātas uzskatiem nenodrošināja atbilstošus drošības pasākumus pret ļaunprātīgu izmantošanu, Valdība sniedza papildu precizējumus. Pirmkārt, lai gan tā atzina, ka orderī nebija precizēti atsevišķi izraudzītie nesēji, jo šīs informācijas iekļaušana orderī būtu ļoti nepraktiska un sarežģīta, tajā tomēr bija aprakstīta pārtveršanas gaita un pārtveramo nesēju veidi. *GCHQ* regulāri informēja *IC* komisāru par pamatu, atbilstoši kuram nesējus atlasīja pārtveršanai.

291. Otrkārt, tā precizēja, ka selektoru izvēle patiesībā ir rūpīgi kontrolēta. Ik reizi, kad sistēmai pievienoja kādu jaunu selektoru, to veicošajam analītiķim bija jāizveido rakstveida ieraksts, paskaidrojot, kādēļ selektora piemērošana valsts sekretāra apliecinājumā norādītajos nolūkos ir nepieciešama un samērīga. To veica, atlasot tekstu no nolaižamās izvēlnes, pēc kā analītiķis pievienoja tekstu brīvā formā, paskaidrojot, kādēļ meklēšana bija nepieciešama un samērīga. “Spēcīga selektora” gadījumā analītiķim bija jāpaskaidro, piemēram, pamatojums kāda konkrēta mērķa sakaru meklēšanai, kā arī tas, kā selektors ir saistīts ar saziņas mērķa metodi un kādēļ attiecīgo sakaru atlasīšana neradītu nevēlamu netiešu iejaukšanos personas tiesībās uz privātās dzīves neaizskaramību. Jauna “kompleksa vaicājuma” gadījumā analītiķim bija jāizstrādā atlases kritēriji, lai, visticamāk, noteiktu vērtīgus izlūkdatus saturošus sakarus, un tāpat jāpaskaidro, kādēļ kritēriji bija pamatoti un kādēļ to izmantošana valsts sekretāra apliecinājumā norādītajos nolūkos būtu nepieciešama un samērīga. Mērķa izveidei vai atklāšanai izmantotos selektorus varēja lietot ne ilgāk kā trīs mēnešus, pēc tam tie bija jāpārskata.

292. Ikvienam selektoram bija jābūt pēc iespējas specifiskākam, lai izvēlētos minimālo materiālu, kas nepieciešams izlūkošanas nolūkam, un tam bija jābūt samērīgam. Ja analizēšanas gaitā tika konstatēts, ka selektorus neizmanto tiem paredzētais mērķis, nekavējoties bija jāveic attiecīgie pasākumi, lai dzēstu selektorus no attiecīgajām sistēmām. Selektoru izmantošana bija jāreģistrē kādā apstiprinātā vietā, kurā tos varēja pārbaudīt un izveidot meklējamu izmantojamo selektoru ierakstu un kurā *IC* komisārs tos varēja pārraudzīt. Līdz ar to *IC* komisārs bija pilnvarots veikt selektoru un meklēšanas kritēriju vispārīgu neatkarīgu pārraudzību, proti, līdz 2014. gada ziņojuma izveidei viņš bija konkrēti ieviesis sistēmas un procesus, lai nodrošinātu, ka šāda pārraudzība patiešām tiek īstenota, un pēc palātas sprieduma pasludināšanas Valdība bija sadarbojusies ar *IC* komisāra biroju, lai nodrošinātu, ka tiks uzlabota selektoru un meklēšanas kritēriju pārraudzība saskaņā ar *IPA*. Tomēr Valdība apgalvoja, ka iepriekšēju tiesas atļauju nebūtu bijis iespējams sniegt attiecībā uz katru selektoru, būtiski nemainot to spēju atklāt un novērst draudus. *GCHQ* sistēmās bija jāiekļauj daudzi tūkstoši selektoru, kuri dažkārt bija strauji jāmaina, lai sekotu līdzi straujā tempā notiekošajai izmeklēšanai un draudu atklāšanai.

293. Saziņas aktu saturs, kam piemēroja vienīgi “spēcīgo selektoru” procesu, nekavējoties tika atmests, ja vien tas neatbilda spēcīgajam selektoram. Savukārt sakari, kam piemēroja arī “kompleksā vaicājuma” procesu, tika saglabāti vairākas dienas, lai nodrošinātu procesa norisi, un pēc tam automātiski dzēsti, ja vien tie netika atlasīti pārbaudei. Saziņas aktu saturu, ko atlasīja pārbaudei, varēja saglabāt vienīgi tad, kad tas bija nepieciešami un samērīgi. Standarta nosacījums bija tāds, ka atlasīto sakaru saglabāšanas periods nepārsniedz dažus mēnešus, pēc šā laika perioda sakari tika automātiski dzēsti (lai gan tad, kad materiāls bija minēts izlūkošanas ziņojumā, šis ziņojums tika saglabāts). Izņēmuma kārtā varēja uzsākt lietu, lai saglabātu atlasītos sakarus ilgāku laiku, nekā to paredz *IC* kodekss.

294. Valdība uzsvēra, ka jebkuram analītiķim, kurš pārbaudīja atlasīto materiālu, bija jābūt īpaši pilnvarotam šādi rīkoties un viņš regulāri piedalījās obligātajās mācībās, tostarp saistībā ar prasībām par nepieciešamību un samērīgumu. Šiem analītiķiem veica arī drošības pārbaudes. Pirms materiāla pārbaudes viņiem bija jāizveido ieraksts, pamatojot, kādēļ piekļuve materiālam ir nepieciešama, kādēļ tā atbilst valsts sekretāra apliecinājumam un *RIPA* prasībām un kādēļ tā ir samērīga (tostarp minot jebkurus apstākļus, kas, visticamāk, var radīt zināmu netiešu iejaukšanos personas tiesībās uz privātās dzīves neaizskaramību). Piekļuve šim materiālam *GCHQ* sistēmas bija liegta, kamēr nebija izveidots šāds ieraksts.

295. Attiecībā uz drošības pasākumiem saistībā ar sakaru datiem Valdība apgalvoja, ka vairuma sensitīvo un privāto sakaru pārbaude vienmēr radīja lielāku iejaukšanos nekā saistīto sakaru datu pārbaude neatkarīgi no tā, vai šie dati bija apkopoti, lai sniegtu detalizētu priekšstatu par personas atrašanās vietu, tās apmeklētajām tīmekļa vietnēm vai personām, ar kurām tā izvēlas sazināties. Tādēļ bija lietderīgi, lai saturu reglamentējošie noteikumi būtu stingrāki par saistītos sakaru datus reglamentējošajiem noteikumiem. Tomēr Valdība piekrita, ka valsts sekretāram ir jāapliecina ar sakaru datiem saistītās pārbaudes nepieciešamība atbilstoši masveida pārtveršanas orderim, ievērojot režīmu, kas ir analogs (bet ne identisks) apliecinājuma režīmam, kurš ieviests attiecībā uz sakaru saturu saskaņā ar *RIPA* 16. pantu. Šādā nolūkā bija jāgroza jaunais prakses kodekss.

296. Tomēr līdz tam brīdim sakaru datiem piemēroja to pašu filtrēšanas procesu kā saturam, ar kuru *GCHQ* apstrādes sistēmas automātiski atmeta noteikta veida sakarus gandrīz reāllaikā. Pēc tam tiem automātiski piemēroja vienkāršus vai kompleksus vaicājumus. Tomēr starp satura un saistīto sakaru datu apstrādi bija divas galvenās atšķirības. Pirmkārt, 16. pantā noteiktie drošības pasākumi, kuri paredzēja, ka, lai veiktu materiāla pārbaudi, tam bija jābūt norādītam valsts sekretāra apliecinājumā un to nevarēja atlasīt atbilstoši faktoram, kas attiecināms uz kādu personu, par kuru zināms, ka tā attiecīgajā brīdī atrodas Britu salās, un kuru nolūks bija apzināt šīs personas sakarus, attiecās vienīgi uz saturu. Valdība apgalvoja, ka šā drošības pasākuma piemērošana saistītajiem sakaru datiem nebūtu praktiska. Ievērojami vairāk vaicājumu tika piemēroti sakaru datiem (pat vairāki tūkstoši vienas nedēļas laikā), un daudzos gadījumos tās personas identitāte, uz kuru dati varēja attiekties, nebija zināma. Turklāt saistīto sakaru datu gadījumā bieži vien liela nozīme ir laikam, un, ja šādu datu meklēšana būtu jāatliek, kamēr nav saņemta atsevišķas iestādes piekrišana, izlūkošanas ziņā tiktu nopietni apdraudēta šo datu lietderība. Iespējams, ka katrā atsevišķajā gadījumā pirms meklēšanas uzsākšanas nebūtu iespējams lūgt valsts sekretāru apliecināt meklēšanas nepieciešamību un samērīgumu.

297. Otrkārt, saistītie sakaru dati, kurus neatlasīja pārbaudei, netika nekavējoties atmesti. Galvenais iemesls tam bija tāds, ka sakaru datus lielā mērā izmantoja, lai atklātu draudus vai mērķus, kuri *GCHQ* iepriekš, iespējams, nebija zināmi. Līdz ar to bija jāveic analītiskāks darbs ilgākā laika periodā, lai atklātu “vēl nezināmo”. Lai veiktu šādu atklāšanu, bieži vien atsevišķas nelielas sakaru datu vienības tika liktas kopā, lai izveidotu veselu “kompozīciju”, tādējādi atklājot draudus, un šī atklāšana varēja ietvert arī tādu vienību pārbaudi, par kurām sākumā tika uzskatīts, ka tām nav izlūkošanas vērtības. Atmetot neatlasītus sakaru datu nekavējoties vai tikai pēc dažām dienām, nebūtu iespējams veikt iepriekš minētās darbības.

298. Tomēr Valdība apstiprināja, ka, pirms jebkurš analītiķis vispār varēja pārbaudīt sakaru datus, viņam bija jāizveido ieraksts, paskaidrojot, kādēļ pārbaude ir nepieciešama un samērīga, pildot likumā noteiktās *GCHQ* funkcijas. Pēc tam tika izveidots pārbaudāms ieraksts, kurā norādīts pārbaudes pamatojums, un šie ieraksti bija pieejami pārbaudei. Turklāt nevienu izlūkošanas ziņojumu nevarēja sagatavot, pamatojoties uz sakaru datiem, ja un kamēr tie nebija pārbaudīti. Visbeidzot, saistītos sakaru datus varēja saglabāt vienīgi tad, kad to saglabāšana bija nepieciešama un samērīga, un ne ilgāk kā dažus mēnešus, ja vien izņēmuma kārtā tie nebija jāsaglabā ilgāk. Pretējā gadījumā saistītie sakaru dati pēc maksimālā laika perioda apritēšanas tika automātiski dzēsti.

299. Visbeidzot, ņemot vērā palātas spriedumu, Valdība apstiprināja, ka tā veica pasākumus, lai nodrošinātu, ka tad, kad ar saturu nesaistītus datus paredzēts atlasīt pārbaudei, atsaucoties uz personu, par kuru zināms, ka tā atrodas Britu salās, valsts sekretāram šī atlase jāapliecina kā nepieciešama un samērīga, pamatojoties uz atsevišķo jomu. Kamēr nebija ieviests “atsevišķai jomai” atbilstošs apliecināšanas režīms, veicot izmaiņas kodeksā, kas reglamentē sakaru pārtveršanu saskaņā ar *IPA*, *GCHQ* sadarbojās ar *IC* komisāra biroju, lai izstrādātu pārvaldības informāciju, ko *IC* komisārs varētu izmantot, lai uzlabotu saistīto sakaru datu *ex post facto* pārraudzību. Proti, *GCHQ* bija veikusi izmaiņas savās sistēmās, lai gadījumos, kad analītiķis grasījās atlasīt sekundāros datus pārbaudei saistībā ar personu, par kuru tika uzskatīts, ka tā atrodas Britu salās, atsaucoties uz faktoru, kas attiecas uz šo personu, šis gadījums tiktu atzīmēts līdzās attiecīgo datu atlasīšanas pamatojumam.

3. Trešās personas argumenti

a) Francijas valdība

300. Francijas valdība norādīja, ka, ņemot vērā tādus draudus kā starptautiskā un pārrobežu noziedzība, kā arī sakaru tehnoloģiju pieaugošo sarežģītību, sakaru stratēģiskā masveida novērošana valstīm ir ļoti svarīga, aizsargājot demokrātisku sabiedrību. Turklāt bija nepareizi pieņemt, ka masveida pārtveršana rada lielāku iejaukšanos personas tiesībās uz privātās dzīves neaizskaramību nekā mērķēta pārtveršana, kas pēc savas būtības, visticamāk, būtu par pamatu lielāka apjoma personas sakaru iegūšanai un pārbaudei. Tās ieskatā nebija iemesla, kādēļ kritērijus, ko Tiesa izklāstījusi lietā “Vēbera un Sarāvija” (minēta iepriekš), nevarētu uzskatīt par vienlīdz svarīgiem datu pārtveršanas un apstrādes efektīvai pārraudzībai masveida pārtveršanas režīma ietvaros. Tomēr šie kritēriji jāpiemēro vispārējā izvērtējuma kontekstā, izvērtējot visus trūkumus attiecībā pret pašreizējām garantijām un drošības pasākumu efektivitāti pret ļaunprātīgu izmantošanu.

301. Nebija pamatojuma pievienot šiem kritērijiem nosacījumu par “pamatotām aizdomām”. Iestādes parasti nevar iepriekš zināt, kuru personu elektroniskos sakarus tām varētu būt lietderīgi pārraudzīt likuma un kārtības vai valsts drošības interesēs, un ar šādu prasību jebkuras uzraudzības pasākuma operatīvās intereses būtu neefektīvas. Turklāt Valdības ieskatā tiesu iestādei nebija jāiesaistās šādu izlūkošanas operāciju atļaušanā vai jāveic *ex post facto* kontrole ar nosacījumu, ka pilnvarojošā iestāde ir neatkarīga no izpildvaras, pārraudzības iestādei ir piešķirtas pietiekamas pilnvaras un kompetence īstenot efektīvu un nepārtrauktu kontroli un abas iestādes ir viena no otras neatkarīgas.

302. Visbeidzot, Valdība, kas iestājusies lietā, apgalvoja, ka metadati pēc savas būtības ir mazāk aizskaroši nekā saturs, jo tie nepārprotami satur mazāk sensitīvas informācijas par attiecīgās personas uzvedību un privāto dzīvi. Šī nostāja tika atbalstīta Venēcijas komisijas ziņojumā (skat. iepriekš 196.–201. punktu), un tai piekrita EST spriedumā lietā “Digital Rights Ireland” (skat. iepriekš 209.–213. punktu).

b) Nīderlandes Karalistes valdība

303. Arī Nīderlandes Karalistes valdība apgalvoja, ka masveida pārtveršana ir nepieciešama, lai apzinātu līdz šim nezināmus draudus valsts drošībai. Lai aizsargātu valsts drošību, izlūkdienestiem ir nepieciešami līdzekļi, lai savlaicīgi un efektīvi izmeklētu jaunus draudus. Šim nolūkam tiem ir nepieciešamas pilnvaras, kas tiem ļautu atklāt un/vai novērst ne tikai teroristu darbības (piemēram, uzbrukumu plānošanu, vervēšanu, propagandu un finansēšanu), bet arī aizskarošas valsts vai nevalstisko dalībnieku kiberdarbības, kuru mērķis ir traucēt demokrātisko kārtību (piemēram, ietekmējot valsts vēlēšanas vai kavējot valsts un starptautisko organizāciju veiktās izmeklēšanas. Kā vienu no piemēriem var minēt Hāgas Ķīmisko ieroču aizliegšanas organizācijas centienus uzlauzt lietas par ķīmisko ieroču izmantošanu Sīrijā). Turklāt svarīgo nozaru pieaugošā atkarība no digitālajām infrastruktūrām nozīmēja, ka šādas nozares, tostarp ūdenssaimniecība, enerģētika, telekomunikācijas, transports, loģistika, ostas un lidostas, kļūst arvien neaizsargātākas pret kiberuzbrukumiem. Šādu traucējumu sekas šajās nozarēs uz sabiedrību radītu spēcīgu ietekmi, kas būtu daudzkārt spēcīgāka par būtisku kaitējumu naudas izteiksmē.

304. To visu sarežģī jaunu digitālo sakaru līdzekļu izstrāde un eksponenciāls globāli pārsūtīto un uzglabāto datu pieaugums. Daudzos gadījumos konkrēta apdraudējuma būtība un izcelsme nebija zināma un mērķēta pārtveršana nebija iespējama. Tomēr, lai gan masveida pārtveršana salīdzinājumā ar mērķētu pārtveršanu nav tik stingri definēta, tā nekad nav bijusi pilnībā nemērķēta. To drīzāk izmantoja konkrētiem mērķiem.

305. Valdība, kas iestājusies lietā, uzskatīja, ka nebija nepieciešams ieviest papildu vai aktualizētus minimālos drošības pasākumus, proti, ka Tiesas iepriekš apzinātie pasākumi bija pietiekami stabili un “ilgtspējīgi”. Palātā ierosinātās pieteikuma iesniedzēju papildu prasības, jo īpaši prasība pierādīt “pamatotas aizdomas”, nepieļaujami samazinātu izlūkdienestu efektivitāti, nenodrošinot personu pamattiesību jēgpilnu papildu aizsardzību.

306. Turklāt Valdība, kas iestājusies lietā, norādīja, ka joprojām ir būtiski nošķirt saturu no sakaru datiem, jo sakaru saturs, visticamāk, ir sensitīvāks nekā sakaru dati. Valdība, kas iestājusies lietā, arī piekrita palātas viedoklim, ka nebija pareizi automātiski pieņemt, ka masveida pārtveršana rada lielāku iejaukšanos personas tiesībās uz privātās dzīves neaizskaramību nekā mērķēta pārtveršana, jo bija pilnībā iespējams, ka ar mērķētu pārtveršanu būtu analizēti visi vai gandrīz visi pārtvertie sakari. Tas neattiecas uz masveida pārtveršanu tad, kad datu pārbaudes un izmantošanas ierobežojumi nosaka to, cik lielā mērā ar pārtveršanu notiek iejaukšanās personas pamattiesībās.

307. Visbeidzot Valdība, kas iestājusies lietā, apgalvoja, ka jebkura prasība paskaidrot vai pamatot atļaujā selektorus vai meklēšanas kritērijus būtiski ierobežotu masveida pārtveršanas efektivitāti, ņemot vērā lielo nenoteiktību saistībā ar draudu avotu. *Ex post* pārraudzība nodrošināja pietiekamus drošības pasākumus.

c) Norvēģijas Karalistes valdība

308. Norvēģijas valdība norādīja, ka attiecībā uz valstu lēmumu ieviest un izmantot noteikta veida masveida pārtveršanas režīmu valsts drošības nolūkos rīcības brīvībai ir jābūt plašai. Tas bija tādēļ, ka izlūkdienestiem jāseko līdzi straujajai attīstībai informācijas un komunikāciju tehnoloģiju jomā. Naidīgi noskaņoti dalībnieki mainīja savas ierīces un digitālo identitāti tik strauji, ka laika gaitā viņu izsekošana kļuva sarežģīta. Bija arī grūtāk savlaicīgi atklāt un novērst naidīgas kiberoperācijas bez līdzekļiem, kas spēj atklāt anomālijas un atbilstošās līdzības personas rīcībā. Līdz ar to neapšaubāmi bija nepieciešamas modernas iespējas, piemēram, masveida pārtveršana, lai atklātu nezināmus draudus digitālajā vidē un ļautu izlūkdienestiem atklāt un izsekot attiecīgos izlūkošanas draudus.

309. Norvēģijas valdība uzskatīja, ka Tiesas pārraudzībai jābalstās uz vispārēju novērtējumu par to, vai procesuālās garantijas pret ļaunprātīgu izmantošanu bija atbilstošas un pietiekamas. Tiesai ir jāizvairās no absolūtām prasībām. Tāpat tai nav jāpiemēro kritēriji, kas netieši apdraudētu valstīm piešķirto plašo rīcības brīvību, pieņemot lēmumu par masveida pārtveršanas režīma izmantošanu valsts drošības mērķiem. Šādu ietekmi radītu prasība par “pamatotām šaubām” vai “turpmāku informēšanu”.

310. Visbeidzot Valdība, kas iesaistījusies lietā, mudināja Tiesu atturēties no EST koncepciju un kritēriju piemērošanas. Pirmkārt, attiecīgajā brīdī deviņpadsmit Eiropas Padomes līgumslēdzējas valstis nebija Eiropas Savienības dalībvalstis. Otrkārt, lai gan Konvencijai un Pamattiesību hartai ir daudz kopēju iezīmju, ir arī noteiktas atšķirības, jo īpaši Hartas 8. pants, kurā paredzētas tiesības uz personas datu aizsardzību. EST arī formulējusi “samērīgumu” atšķirīgi, izmantojot “absolūtas nepieciešamības” metodi, kas nav salīdzināma ar Tiesas izmantoto metodi.

d) Apvienoto Nāciju Organizācijas īpašais ziņotājs vārda brīvības jautājumos

311. Īpašais ziņotājs apgalvoja, ka uzraudzība met ēnu uz sakariem, līdz ar to personas var atturēties no iesaistīšanās darbībās, kas aizsargātas ar starptautiskajām cilvēktiesību normām. Tas nenozīmē, ka visas uzraudzības operācijas pārkāpj cilvēktiesību normas, proti, dažas no tām varētu būt pieļaujamas, ja ir izpildīti likumības, nepieciešamības un leģitimitātes nosacījumi. Tomēr attiecībā uz jebkuru uzraudzību ir stingri jāizvērtē, vai šīs operācijas atbilst starptautisko cilvēktiesību normām.

312. Īpašā ziņotāja ieskatā tiesības uz privātās dzīves neaizskaramību ir jāaizsargā ne tikai kā pamattiesības neatkarīgi no visām citām tiesībām, bet arī tādēļ, lai aizsargātu citas tiesības, piemēram, tiesības uz uzskatu un vārda brīvību, kuru īstenošana atkarīga no attiecīgās privātuma jomas. Kā īpašais ziņotājs norādījis savā 2015. gada ziņojumā, uzraudzības sistēmas var apdraudēt personas tiesības paust viedokli, jo bailes no tiešsaistes darbības izpaušanas piespiedu kārtā varētu atturēt personas no piekļuves informācijai.

313. ANO augstās komisāres ziņojumā tika ieteikts nenošķirt metadatus no satura, kad tiek izvērtēts, cik lielā mērā notika iejaukšanās *ICCPR* noteiktajās tiesībās. Viņas 2014. gada ziņojumā bija norādīts, ka metadatu apkopošana Valdības veiktās uzraudzības rezultātā par personu varētu atklāt vairāk privātās informācijas nekā privāta saziņa. Īpašais ziņotājs arī norādīja, ka iekšējo un ārējo sakaru nošķiršana var būt pretrunā ar *ICCPR*. *ICCPR* uzliek valstīm par pienākumu ievērot un nodrošināt visas tajā noteiktās tiesības visām personām to jurisdikcijā, turklāt Cilvēktiesību komisija savā pēdējā vispārējā komentārā šo standartu interpretēja kā tādu, kas ietver valsts darbības, kuras tieši ietekmē tiesības ārpus tās teritorijas.

314. Visbeidzot īpašais ziņotājs uzsvēra, cik svarīgi ir drošības pasākumi, lai nodrošinātu aizsardzību pret ļaunprātīgu izmantošanu, jo īpaši nepieciešamība tiesai, tribunālam vai kādai citai tiesu iestādei pārraudzīt iejaukšanās pasākuma piemērošanu, kā arī turpmāka informēšana par uzraudzības subjektiem, informācijas publicēšana saistībā ar uzraudzības metožu un pilnvaru tvērumu un tiesības uz efektīviem tiesiskās aizsardzības līdzekļiem ļaunprātīgas izmantošanas gadījumā.

e) “Access Now”

315. “Access Now” apgalvoja, ka šajā lietā aplūkotā masveida uzraudzība neatbilda *ICCPR* un Starptautiskajiem principiem par cilvēktiesību piemērošanu sakaru uzraudzībai, jo Apvienotā Karaliste nebija pierādījusi, ka šāda uzraudzība bija absolūti nepieciešama vai samērīga. Šī organizācija arī norādīja, ka uzraudzības programmas nedrīkst izvērtēt atsevišķi, bet gan saistībā ar visu valsts uzraudzības darbību kopumu, jo mašīnmācīšanās, ar kuras palīdzību ar matemātiskiem algoritmiem varētu izgūt secinājumus no datu apkopojumiem, ir palielinājusi lielo datu kopu un datu iegūšanas izplatību.

f) “Article 19”

316. “Article 19” apgalvoja, ka personu sakaru neselektīva vākšana, analizēšana un saglabāšana bez aizdomu pamata pēc būtības ir nesamērīga. Pēc “Article 19” domām, vienīgi ar mērķētu uzraudzību, kas balstīta uz pamatotām aizdomām un ko atļāvis tiesnesis, tiktu leģitīmi ierobežotas tiesības uz privātās dzīves neaizskaramību.

g) “European Digital Rights” (turpmāk tekstā – “*EDRi*”) un citas organizācijas, kas darbojas cilvēktiesību jomā informācijas sabiedrībā

317. *EDRi* un citas organizācijas apgalvoja, ka šī lieta Tiesai sniedza būtisku iespēju pārskatīt savu metadatu aizsardzības sistēmu. Valstu valdības ir veidojušas savas uzraudzības programmas, balstoties uz noteikto atšķirību starp saturu un metadatiem, kā norādīts 1984. gada 2. augusta spriedumā lietā “Malons pret Apvienoto Karalisti”, A sērija Nr. 82, taču minētās lietas izskatīšanas laikā nebija ne interneta, ne mobilo tālruņu. Mūsdienās metadati varētu sniegt detalizētu un ļoti privātu priekšstatu par personu, proti, tie ļauj kartēt sociālos tīklus, noteikt atrašanās vietu, sekot līdzi interneta pārlūkošanai, kartēt līdzības saziņā, kā arī uzzināt, ar ko attiecīgā persona sazinās. Turklāt detalizācijas pakāpe, ko varētu iegūt, ir palielinājusies, veicot analīzi plašā mērogā. Proti, *NSA* galvenais padomnieks Stjuarts Beikers [*Stewart Baker*] norādīja, ka metadati varētu atklāt visu par kādas personas dzīvi un ka tad, ja kādam ir pietiekams metadatu apjoms, saturs nebūtu nepieciešams. Tādēļ uz personas datiem nav jāattiecina dažādas aizsardzības pakāpes, balstoties uz satura un metadatu patvaļīgu un neatbilstošu nošķiršanu – tā vietā jābalstās uz secinājumiem, ko var izgūt no datiem.

h) “Open Society Justice Initiative” (turpmāk tekstā – “*OSJI*”)

318. *OSJI* norādīja, ka gan pašlaik pārtveršanai pieejamo datu apjoms, gan valstu valdību vēlme iegūt datus ievērojami pārsniedz to, kas bija iespējams kādreiz. Līdz ar to masveida pārtveršana rada īpaši būtisku iejaukšanos privātajā dzīvē, kas ar savu “atturošo ietekmi” varētu iejaukties citās tiesībās, piemēram, tiesībās uz vārda brīvību un biedrošanās brīvību. Tādēļ, lai masveida pārtveršana būtu likumīga, tai ir jāatbilst vairākiem priekšnosacījumiem, proti, reglamentējošajam tiesību aktam jābūt pietiekami precīzam, ievāktās informācijas apjoms ir jāierobežo laika un atrašanās vietas ziņā un informācija ir jāievāc, vienīgi balstoties uz “pamatotām aizdomām”.

i) Helsinku Cilvēktiesību fonds (turpmāk tekstā – “*HFHR*”)

319. *HFHR* raksturoja savu pieredzi, apstrīdot valsts iestāžu īstenoto sakaru uzraudzību Polijā, kā rezultātā Konstitucionālā tiesa atzina noteiktus attiecīgā tiesiskā regulējuma aspektus par neatbilstīgiem konstitūcijai. Pēc tam tiesiskais regulējums tika grozīts.

j) Starptautiskā Juristu komisija (turpmāk tekstā – “*ICJ*”)

320. *ICJ* norādīja, ka, ņemot vērā masveida uzraudzības radītās iejaukšanās tiesībās uz privātās dzīves neaizskaramību apjomu un tvērumu, atšķirība starp metadatiem un saturu ir novecojusi. Turklāt fakts, ka masveida uzraudzības operācijā šādas iejaukšanās tiesībās elementi varētu tikt īstenoti ārpus valsts teritoriālās jurisdikcijas, neizslēdz šīs valsts atbildību, jo tās kontrole pār informāciju ir pietiekama, lai noteiktu jurisdikciju.

k) Anglijas un Velsas Juridiskā biedrība

321. Juridiskā biedrība pauda nopietnas bažas par 8. panta 4. punktā noteiktā režīma ietekmi uz advokāta un klienta saziņas konfidencialitātes principu. Tās ieskatā režīms ļāva pārtvert juridiski priviliģētus un konfidenciālus sakarus starp advokātiem un klientiem, pat ja abi atradušies Apvienotajā Karalistē. Tas arī ļāva regulāri apkopot šiem sakariem pievienotos metadatus. Turklāt pēc šo juridiski priviliģēto sakaru pārtveršanas tos varēja izmantot ar nosacījumu, ka ordera primārais nolūks un mērķis bija ārējo sakaru apkopošana. Šis pasākums, tostarp atbilstošu šā materiāla izmantošanas ierobežojumu neesība, varēja radīt “atturošu ietekmi” uz advokāta un klienta saziņas godīgumu un atklātību.

4. Tiesas vērtējums

a) Sākotnējās piezīmes

322. Šī sūdzība attiecas uz izlūkdienestu veikto pārrobežu sakaru masveida pārtveršanu. Lai gan šī nav pirmā reize, kad Tiesa izvērtē šāda veida uzraudzību (skat. spriedumu iepriekš minētajās lietās “Vēbere un Sarāvija” un ““Liberty” un citi”), tiesvedības gaitā ir kļuvis skaidrs, ka jebkura šāda režīma izvērtēšana rada noteiktas grūtības. Pašreizējā, aizvien digitālākā laikmetā sakari ir lielākoties digitāli un tie tiek pārraidīti pa globālajiem telekomunikāciju tīkliem, izmantojot ātrāko un lētāko kanālu kombināciju, bez jebkādas jēgpilnas atsauces uz valstu robežām. Līdz ar to uzraudzība, kas nav tieši vērsta uz personām, var būt ļoti tālejoša gan uzraudzības valsts teritorijā, gan ārpus tās. Tāpēc drošības pasākumi ir izšķiroši un tajā pašā laikā grūti īstenojami. Atšķirībā no mērķētās pārtveršanas, uz kuru attiecas liela daļa Tiesas judikatūras un ko galvenokārt izmanto noziegumu izmeklēšanai, masveida pārtveršanu izmanto arī – vai pat galvenokārt – tamdēļ, lai ievāktu ārvalstu izlūkdatus un apzinātu jaunus draudus gan no zināmu, gan nezināmu personu puses. Darbojoties šajā jomā, līgumslēdzējām valstīm ir leģitīma nepieciešamība ievērot slepenību, līdz ar to publiski būs pieejams maz informācijas par sistēmas darbību vai šāda informācija nebūs pieejama vispār, turklāt šādu informāciju, kas ir pieejama, var izmantot terminoloģijā, kas ir neskaidra un dažādās valstīs var ievērojami atšķirties.

323. Lai gan tehnoloģiskās iespējas ir ievērojami palielinājušas to sakaru apjomu, kas šķērso globālo internetu, ir palielinājušies arī draudi, ar kuriem saskaras līgumslēdzējas valstis un to pilsoņi. Tie tostarp ietver globālo terorismu, narkotiku tirdzniecību, cilvēku tirdzniecību un bērnu seksuālu izmantošanu. Daudzi no šiem draudiem izriet no starptautiskiem tīkliem, kuros darbojas naidīgi dalībnieki, kam ir piekļuve aizvien sarežģītākām tehnoloģijām, kuras tiem ļauj sazināties nepamanīti. Piekļuve šādām tehnoloģijām arī ļauj naidīgiem valsts un nevalstiskajiem dalībniekiem traucēt digitālo infrastruktūru un pat demokrātisko procesu atbilstošu darbību, izmantojot kiberuzbrukumus, kas ir nopietns drauds valsts drošībai, kas pēc definīcijas pastāv vienīgi digitālajā vidē un tādējādi var tikt atklāts un izmeklēts vienīgi šajā vidē. Līdz ar to Tiesai ir jāizvērtē līgumslēdzēju valstu masveida pārtveršanas režīmi, kas ir vērtīga tehnoloģiska iespēja jaunu draudu apzināšanai digitālajā vidē, lai nodrošinātu atbilstību Konvencijai, atsaucoties uz ieviestajiem drošības pasākumiem aizsardzībai pret patvaļību un ļaunprātīgu izmantošanu un pamatojoties uz ierobežotu informāciju par šo režīmu darbības veidu.

c) Pārtveršanas esība

324. Valdība nav apstrīdējusi, ka ir notikusi iejaukšanās 8. pantā noteiktajās pieteikuma iesniedzēju tiesībās, lai gan tā apgalvoja, ka saskaņā ar Konvencijas 8. pantu jēgpilna iejaukšanās varēja notikt vienīgi tad, kad sakarus atlasīja pārbaudei.

325. Tiesa uzskata, ka masveida pārtveršana ir pakāpenisks process, kurā iejaukšanās 8. pantā noteiktajās personas tiesībās kļūst nopietnāka procesa gaitā. Masveida pārtveršanas režīmi var neatbilst tieši vienam un tam pašam modelim, un dažādi procesa posmi ne vienmēr būs diskrēti vai īstenoti stingrā hronoloģiskā secībā. Tomēr, ņemot vērā šos brīdinājumus, Tiesa uzskata, ka masveida pārtveršanas procesa posmus, kas jāņem vērā, var raksturot šādi:

a) sakaru un saistīto sakaru datu (proti, pārtvertajiem sakariem piederošo datplūsmas datu) pārtveršana un sākotnējā saglabāšana;

b) konkrētu selektoru piemērošana saglabātajiem sakariem / saistītajiem sakaru datiem;

c) atlasīto sakaru / saistīto sakaru datu pārbaude, ko veic analītiķis, un

d) turpmāka datu saglabāšana un “galaprodukta” izmantošana, tostarp apmaiņa ar trešām personām.

326. Posmā, kas Tiesas ieskatā ir pirmais posms, izlūkdienesti masveidā pārtvers elektroniskos sakarus (vai elektronisko sakaru “paketes”). Šie sakari piederēs lielam skaitam personu, no kurām daudzas izlūkdienestus vispār neinteresēs. Šajā posmā var tikt izfiltrēti daži tāda veida sakari, kas, visticamāk, izlūkdienestiem interesi neradīs.

327. Sākotnējā meklēšana, kas parasti ir automātiska, notiek posmā, ko Tiesa uzskata par otro posmu, kad dažāda veida selektorus, tostarp “spēcīgos selektorus” (piemēram, e-pasta adreses), un/vai kompleksus vaicājumus piemēro saglabātajām sakaru paketēm vai saistītajiem sakaru datiem. Tas var būt posms, kurā minētā procesa ietvaros uzsāk personu izraudzīšanu, izmantojot spēcīgos selektorus.

328. Posmā, ko Tiesa uzskata par trešo posmu, analītiķis pirmo reizi pārbauda pārtverto materiālu.

329. Posmā, ko Tiesa uzskata par pēdējo posmu, izlūkdienesti faktiski izmanto pārtverto materiālu. Tas var ietvert izlūkošanas ziņojuma sagatavošanu, materiāla izplatīšanu citiem izlūkdienestiem pārtveršanu veicošajā valstī vai pat materiāla pārraidīšanu ārvalstu izlūkdienestiem.

330. Tiesa uzskata, ka 8. pants attiecas uz visiem iepriekš minētajiem posmiem. Lai gan sākotnējā pārtveršana pēc sakaru daļu tūlītējas atmešanas nerada būtisku iejaukšanos, šādas iejaukšanās pakāpe personas 8. pantā noteiktajās tiesībās masveida pārtveršanas procesa gaitā palielināsies. Šajā ziņā Tiesa ir skaidri norādījusi, ka ar personas privāto dzīvi saistīto datu saglabāšana vien 8. panta nozīmē ir kvalificējama kā iejaukšanās (skat. 1987. gada 26. marta sprieduma lietā “Leanders pret Zviedriju” 48. punktu, A sērija Nr. 116) un ka vajadzība pēc drošības pasākumiem būs lielāka tad, kad tas skar automātiski apstrādātu personas datu aizsardzību (skat. sprieduma iepriekš minētajā lietā “S. un Mārpers” 103. punktu). Tas, ka uzglabātais materiāls ir kodēts, saprotams vienīgi ar datortehnoloģiju palīdzību, un tas, ka to var interpretēt tikai ierobežots personu skaits, nevar ietekmēt šo secinājumu (skat. sprieduma lietā Nr. 27798/95 “Amans [*Amann*] pret Šveici” [*GC*] 69. punktu, ECT 2000-II, un sprieduma iepriekš minētajā lietā “S. un Mārpers” 67. un 75. punktu). Visbeidzot, procesa beigās, kad analītiķis analizē informāciju par konkrētu personu vai pārbauda sakaru saturu, radīsies vislielākā nepieciešamība pēc drošības pasākumiem. Šī Tiesas pieeja atbilst Venēcijas komisijas secinājumam, kura savā ziņojumā par izlūkošanas aģentūru demokrātisko pārraudzību uzskatīja, ka masveida pārtveršanas procesā visbūtiskākā iejaukšanās tiesībās uz privātās dzīves neaizskaramību notiek brīdī, kad aģentūras apstrādā uzglabātos personas datus un/vai tiem piekļūst (skat. iepriekš 196. punktu).

331. Līdz ar to pakāpe, kādā notiek iejaukšanās tiesībās uz privātās dzīves neaizskaramību, palielināsies procesa gaitas dažādajos posmos. Izvērtējot, vai šī pastiprinātā iejaukšanās bija pamatota, Tiesa veiks savu novērtējumu par 8. panta 4. punktā noteikto režīmu, pamatojoties uz tās izpratni par iejaukšanās būtību.

c) Vai iejaukšanās bija pamatota

i) Vispārīgie principi attiecībā uz slepeniem uzraudzības pasākumiem, tostarp sakaru pārtveršanu

332. Jebkura iejaukšanās personas 8. pantā noteiktajās tiesībās ir pamatota saskaņā ar 8. panta 2. punktu vienīgi tad, ja tā notiek atbilstoši likumam, tai ir viens vai vairāki leģitīmi mērķi, uz kuriem šis punkts attiecas, un ir nepieciešama demokrātiskā sabiedrībā jebkura šāda mērķa sasniegšanai (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 227. punktu un 2010. gada 18. maija sprieduma lietā Nr. 26839/05 “Kenedijs pret Apvienoto Karalisti” 130. punktu). Formulējums “saskaņā ar likumu” pieprasa, lai apstrīdētajam pasākumam būtu kāds pamatojums valsts tiesību aktos (pretēji praksei, kas neparedz konkrētu tiesisko pamatu, skat. 2007. gada 1. marta sprieduma lietā “Heglass [*Heglas*] pret Čehijas Republiku” Nr. 5935/02 74. punktu). Tam arī ir jāatbilst tiesiskumam, kas skaidri norādīts Konvencijas preambulā un ir 8. panta mērķa un nolūka pamatā. Tādēļ tiesību aktiem ir jābūt pieejamiem attiecīgajai personai un to ietekmei ir jābūt paredzamai (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 228. punktu, citu iestāžu starpā arī iepriekš minētā sprieduma lietā “Rotaru” 52. punktu, iepriekš minētā sprieduma lietā “S. un Mārpers” 95. punktu, kā arī iepriekš minētā sprieduma lietā “Kenedijs” 151. punktu).

333. Jēdziena “paredzamība” nozīme slepenās uzraudzības kontekstā nav tāda pati kā daudzās citās jomās. Īpašajā slepeno uzraudzības pasākumu, piemēram, sakaru pārtveršanas, kontekstā “paredzamība” nevar nozīmēt to, ka personām jāspēj paredzēt, kad iestādes varētu īstenot šādus pasākumus, lai tās varētu attiecīgi pielāgot savu rīcību. Tomēr jo īpaši tad, ja izpildvarai piešķirtās pilnvaras īsteno slepeni, patvaļas risks ir acīmredzams. Tāpēc ir svarīgi, lai būtu skaidri, detalizēti noteikumi par slepeniem uzraudzības pasākumiem, jo īpaši tādēļ, ka lietošanai pieejamās tehnoloģijas pastāvīgi kļūst arvien sarežģītākas. Valsts tiesību aktiem ir jābūt pietiekami skaidriem, lai sniegtu pilsoņiem atbilstošas norādes par apstākļiem un nosacījumiem, kādos valsts iestādes ir pilnvarotas īstenot jebkādus šādus pasākumus (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 229. punktu, iepriekš minētā sprieduma lietā “Malons” 67. punktu, iepriekš minētā sprieduma lietā “Leanders” 51. punktu, iepriekš minētā sprieduma lietā “Huvigs” 29. punktu, iepriekš minētā sprieduma lietā “Krulēns” 30. punktu, 1998. gada 30. jūlija sprieduma lietā “Valensvela Kontrerass [*Valenzuela Contreras*] pret Spāniju” 46. punktu, *Reports of Judgments and Decisions* 1998‑V, iepriekš minētā sprieduma lietā “Rotaru” 55. punktu, iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 93. punktu, kā arī 2007. gada 28. jūnija sprieduma lietā Nr. 62540/00 “Eiropas integrācijas un cilvēktiesību asociācija un Ekimdžijevs [*Ekimdzhiev*] pret Bulgāriju” 75. punktu). Turklāt tiesību aktos pietiekami skaidri jānorāda jebkuras kompetentajām iestādēm piešķirtās rīcības brīvības apjoms un īstenošanas veids, lai nodrošinātu personai atbilstošu aizsardzību pret patvaļīgu iejaukšanos (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 230. punktu, citu iestāžu starpā arī iepriekš minētā sprieduma lietā “Malons” 68. punktu, iepriekš minētā sprieduma lietā “Leanders” 51. punktu, iepriekš minētā sprieduma lietā “Huvigs” 29. punktu, iepriekš minētā sprieduma lietā “Krulēns” 30. punktu, kā arī iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 94. punktu).

334. Lietās, kad Tiesā tiek apstrīdēts tiesību akts, kas pieļauj slepenu uzraudzību, iejaukšanās likumība ir cieši saistīta ar jautājumu, vai ir ievērots “nepieciešamības” nosacījums, tāpēc Tiesai ir lietderīgi kopīgi izvērtēt prasības par tādiem apstākļiem kā “saskaņā ar likumu” un “nepieciešamība”. Jēdziens “tiesību aktu kvalitāte” šajā ziņā nozīmē to, ka valsts tiesību aktiem jābūt ne tikai pieejamiem un paredzamiem saistībā ar to piemērošanu, bet arī jānodrošina, lai slepenie uzraudzības pasākumi tiktu piemēroti vienīgi tad, kad tas “nepieciešams demokrātiskā sabiedrībā”, jo īpaši paredzot atbilstošus un efektīvus drošības pasākumus un garantijas pret ļaunprātīgu izmantošanu (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 236. punktu un iepriekš minētā sprieduma lietā “Kenedijs” 155. punktu).

335. Šajā ziņā jāatkārto, ka Tiesa savā judikatūrā par sakaru pārtveršanu kriminālizmeklēšanā ir izstrādājusi šādas minimālās prasības, kas jānosaka tiesību aktos, lai izvairītos no pilnvaru ļaunprātīgas izmantošanas: i) to nodarījumu būtība, kas var būt par pamatu pārtveršanas rīkojuma izdošanai; ii) to personu kategorijas, kuru sakarus var pārtvert; iii) pārtveršanas ilguma ierobežojums; iv) iegūto datu pārbaudes, izmantošanas un uzglabāšanas kārtība; v) veicamie piesardzības pasākumi, paziņojot datus citām pusēm, un vi) apstākļi, kādos pārtvertos datus atļauts vai ir pienākums dzēst vai iznīcināt (skat. iepriekš minētā sprieduma lietā “Huvigs” 34. punktu, iepriekš minētā sprieduma lietā “Krulēns” 35. punktu, iepriekš minētā sprieduma lietā “Valensvela Kontrerass” 46. punktu, iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 95. punktu, kā arī iepriekš minētā sprieduma lietā “Eiropas integrācijas un cilvēktiesību asociācija un Ekimdžijevs” 76. punktu). Spriedumā lietā “Romāns Zaharovs” (minēts iepriekš, 231. punkts) Tiesa apstiprināja, ka tie paši seši minimālie drošības pasākumi attiecas arī uz gadījumiem, kad pārtveršana tiek veikta valsts drošības interesēs, taču, nosakot, vai ar apstrīdēto tiesisko regulējumu pārkāpts 8. pants, tā ņēma vērā arī slepenās uzraudzības pasākumu īstenošanas pārraudzības kārtību, jebkurus paziņošanas mehānismus un valsts tiesību aktos paredzētos tiesiskās aizsardzības līdzekļus (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 238. punktu).

336. Slepenās uzraudzības pasākumus var pārskatīt un pārraudzīt trīs posmos, proti, kad izdots pirmais rīkojums par uzraudzību, uzraudzības laikā vai pēc uzraudzības pabeigšanas. Attiecībā uz pirmajiem diviem posmiem jānorāda, ka slepenās uzraudzības pati būtība un loģika nosaka, ka bez personas ziņas veicama ne tikai pati uzraudzība, bet arī ar to saistītā pārskatīšana. Līdz ar to, tā kā personai būs liegts pašai meklēt efektīvus tiesiskās aizsardzības līdzekļus vai tieši piedalīties jebkurā pārskatīšanas procesā, ir svarīgi, lai noteiktās procedūras pašas par sevi nodrošinātu atbilstošas un līdzvērtīgas garantijas, kas aizsargā šīs personas tiesības. Jomā, kurā ļaunprātīga izmantošana atsevišķās lietās, iespējams, ir tik vienkārša un var radīt tik kaitīgas sekas demokrātiskai sabiedrībai kopumā, Tiesa ir atzinusi, ka pārraudzības kontroli principā vēlams uzticēt tiesnesim, tiesas veiktai kontrolei nodrošinot vislabākās neatkarības, objektivitātes un atbilstošas procedūras garantijas (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 233. punktu, kā arī 1987. gada 6. septembra sprieduma lietā “Klass un citi pret Vāciju” 55. un 56. punktu, A sērija Nr. 28).

337. Attiecībā uz trešo posmu pēc uzraudzības pabeigšanas jautājums par turpmāku informēšanu saistībā ar uzraudzības pasākumiem ir svarīgs faktors, tiesā izvērtējot tiesiskās aizsardzības līdzekļu efektivitāti un tādēļ arī to, vai ir ieviesti efektīvi drošības pasākumi pret uzraudzības pilnvaru ļaunprātīgu izmantošanu. Attiecīgajai personai principā ir maz iespēju vērsties tiesā, ja vien šī persona nav informēta par pasākumiem, kas veikti bez tās ziņas, tādēļ tā nevar apstrīdēt to likumību ar atpakaļejošu spēku (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 234. punktu, iepriekš minētā sprieduma lietā “Klass un citi” 57. punktu, kā arī iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 135. punktu), vai ja vien jebkura persona, kurai radušās aizdomas, ka tā tikusi uzraudzīta, nevar vērsties tiesās, kuru jurisdikcija nav atkarīga no tā, vai uzraudzības subjekts ticis informēts par veiktajiem pasākumiem (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 234. punktu, kā arī iepriekš minētā sprieduma lietā “Kenedijs” 167. punktu).

338. Attiecībā uz jautājumu, vai iejaukšanās bija “nepieciešama demokrātiskā sabiedrībā” leģitīma mērķa sasniegšanai, Tiesa ir atzinusi, ka valsts iestādēm ir plaša rīcības brīvība, izvēloties, kā vislabāk sasniegt leģitīmo mērķi aizsargāt valsts drošību (skat. iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 106. punktu).

339. Tomēr šī rīcības brīvība ir pakļauta Eiropas pārraudzībai, kas ietver gan tiesisko regulējumu, gan lēmumus, ar kuriem to piemēro. Ņemot vērā risku, ka slepenās uzraudzības sistēma, kas izveidota, lai aizsargātu valsts drošību (un citas būtiskas valsts intereses), var apdraudēt vai pat iznīcināt demokrātisko procesu atbilstošu darbību to aizsardzības aizsegā, Tiesai ir jāpārliecinās, ka ir pieejamas atbilstošas un efektīvas garantijas pret ļaunprātīgu izmantošanu. Šis izvērtējums ir atkarīgs no visiem lietas apstākļiem, piemēram, iespējamo pasākumu būtības, apjoma un ilguma, to uzdošanas pamatojuma, iestādēm, kuras ir kompetentas tos atļaut, īstenot un pārraudzīt, kā arī no valsts tiesību aktos paredzētā tiesiskās aizsardzības līdzekļa veida. Tiesai ir jānosaka, vai ierobežojošo pasākumu uzdošanas un īstenošanas pārraudzības procedūras ir tādas, lai “iejaukšanās” būtu “nepieciešama demokrātiskā sabiedrībā” (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 232. punktu, iepriekš minētā sprieduma lietā “Klass un citi” 49., 50. un 59. punktu, iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 106. punktu, kā arī iepriekš minētā sprieduma lietā “Kenedijs” 153. un 154. punktu).

ii) Par to, vai nepieciešams izstrādāt judikatūru

340. Lietās “Vēbere un Sarāvija” un ““Liberty” un citi” (minētas iepriekš) Tiesa piekrita tam, ka masveida pārtveršanas režīmi *per se* neietilpa valstu rīcības brīvības robežās. Ņemot vērā to draudu izplatību, ar ko valstis pašlaik saskaras tādu starptautisku dalībnieku tīklos, kuri izmanto internetu gan saziņai, gan kā līdzekli, un to, ka viņu rīcībā ir sarežģīta tehnoloģija, kas ļauj šiem dalībniekiem izvairīties no atklāšanas (skat. iepriekš 323. punktu), Tiesa uzskata, ka lēmums par masveida pārtveršanas režīma izmantošanu, lai apzinātu draudus valsts drošībai vai būtiskām valsts interesēm, joprojām ietilpst šajās rīcības brīvības robežās.

341. Gan lietā “Vēbere un Sarāvija”, gan lietā ““Liberty” un citi” (minētas iepriekš) Tiesa piemēroja iepriekš minētos minimālos sešus drošības pasākumus, kas izstrādāti tās judikatūrā par mērķētu pārtveršanu (skat. iepriekš 335. punktu). Tomēr, lai gan šajās lietās aplūkotie masveida pārtveršanas režīmi līdzinājās šajā lietā aplūkotajiem režīmiem, abas lietas izskatīja vairāk nekā pirms desmit gadiem, un pēdējos gados tehnoloģiju attīstība ir būtiski mainījusi veidu, kādā cilvēki sazinās. Cilvēki aizvien lielāku daļu savas dzīves pavada tiešsaistē, radot gan ievērojami lielāku elektronisko sakaru apjomu, gan saziņas aktu saturu, kuru būtība un kvalitāte ievērojami atšķiras no tiem, kas, iespējams, tika radīti pirms desmit gadiem (skat. iepriekš 322. punktu). Līdz ar to minētajās lietās aplūkotās uzraudzības darbības apjoms būtu bijis daudz šaurāks.

342. Tas līdzvērtīgi attiecas uz saistītajiem sakaru datiem. Kā savā ziņojumā norādīja *ISR*, pašlaik par personu ir pieejams lielāks sakaru datu apjoms salīdzinājumā ar saturu, jo katru saturu aptver vairākas sakaru datu vienības (skat. iepriekš 159. punktu). Lai gan saturs var būt šifrēts un katrā ziņā var neatklāt neko nozīmīgu par sūtītāju vai saņēmēju, saistītie sakaru dati var atklāt daudz personas datu, piemēram, sūtītāja un saņēmēja identitāti un ģeogrāfisko atrašanās vietu, kā arī ierīces, ar kuru starpniecību sakari tika pārraidīti. Turklāt jebkura iejaukšanās, kam par pamatu bija sakaru datu iegūšana, būs vēl jo nopietnāka, kad šos datus iegūs masveidā, jo tagad tos var analizēt un pārbaudīt, lai radītu ļoti privātu priekšstatu par personu, kartējot sociālos tīklus, nosakot atrašanās vietu, sekojot līdzi interneta pārlūkošanai, kartējot līdzības saziņā, kā arī uzzinot, ar ko attiecīgā persona sazinās (skat. iepriekš 317. punktu).

343. Tomēr, kas ir vēl būtiskāk, Tiesa lietās “Vēbere un Sarāvija” un ““Liberty” un citi” tieši nepieminēja pašu faktu, ka tā izvērtē uzraudzību, kas tās būtības un apmēra ziņā atšķiras no iepriekšējās lietās aplūkotās uzraudzības. Taču mērķēta pārtveršana un masveida pārtveršana atšķiras vairākos svarīgos aspektos.

344. Pirmkārt, masveida pārtveršana parasti ir vērsta uz starptautiskiem sakariem (proti, uz sakariem, kas tiek fiziski pārraidīti pāri valsts robežām), un, lai gan nebūtu izslēgta personu sakaru pārtveršana un pat pārbaude novērošanas valstī, daudzos gadījumos masveida pārtveršanas noteiktais nolūks ir pārraudzīt ārpus valsts teritoriālās jurisdikcijas esošo personu sakarus, kuras nevarētu pārraudzīt ar citiem uzraudzības veidiem. Piemēram, Vācijas sistēmas mērķis ir vienīgi pārraudzīt ārvalstu telekomunikācijas ārpus Vācijas teritorijas (skat. iepriekš 248. punktu). Savukārt Zviedrijā pārtvertais materiāls nevar attiekties uz signāliem tad, kad gan sūtītājs, gan saņēmējs atrodas Zviedrijā (skat. šodienas spriedumu lietā Nr. 35252/08 ““Centrum för rättvisa” pret Zviedriju”).

345. Turklāt, kā jau norādīts iepriekš, nolūki, kādos var īstenot masveida pārtveršanu, šķiet atšķirīgi. Ciktāl Tiesa ir izvērtējusi mērķētu pārtveršanu, to lielākoties ir īstenojušas atbildētājvalstis, lai izmeklētu noziegumus. Tomēr, lai gan masveida pārtveršanu var īstenot, lai izmeklētu noteiktus smagus noziegumus, šķiet, ka Eiropas Padomes dalībvalstis, kas izmanto masveida pārtveršanas režīmu, to izmanto ārvalstu izlūkdatu vākšanai, kiberuzbrukumu agrīnai atklāšanai un izmeklēšanai, pretspiegošanai un terorisma apkarošanai (skat. iepriekš 303., 308. un 323. punktu).

346. Lai gan masveida pārtveršana ne vienmēr tiek īstenota attiecībā uz konkrētām personām, to acīmredzami var izmantot un izmanto šim nolūkam. Tomēr šādā gadījumā izraudzīto personu ierīces neuzrauga. Personas drīzāk tiek “izraudzītas”, piemērojot spēcīgos selektorus (piemēram, viņu e-pasta adreses) sakariem, ko masveidā pārtvēruši izlūkdienesti. Šādā veidā tiek pārtvertas vienīgi tās izraudzīto personu sakaru “paketes”, kas pārraidītas caur izlūkdienestu atlasītajiem nesējiem, un analītiķis var pārbaudīt vienīgi tos pārtvertos sakarus, kas atbilst vai nu spēcīgam selektoram, vai sarežģītam vaicājumam.

347. Gluži kā jebkura pārtveršanas režīma gadījumā, protams, pastāv ievērojama iespējamība, ka masveida pārtveršanu var izmantot ļaunprātīgi, tādējādi negatīvi ietekmējot personu tiesības uz privātās dzīves neaizskaramību. Lai gan Konvencijas 8. pants neaizliedz masveida pārtveršanu, lai aizsargātu valsts drošību un citas būtiskas valsts intereses pret nopietniem ārējiem draudiem, un valstīm ir plaša rīcības brīvība, lemjot par to, kāda veida pārtveršanas režīms ir nepieciešams šiem nolūkiem, izmantojot šādu sistēmu, tām piešķirtajai rīcības brīvībai ir jābūt šaurākai, un būs jāievieš vairāki drošības pasākumi. Tiesa jau ir noteikusi tos drošības pasākumus, kuriem jāietver Konvencijai atbilstošs mērķētas pārtveršanas režīms. Lai gan šie principi nodrošina lietderīgu pamatu šim uzdevumam, tie būs jāpielāgo, lai atspoguļotu masveida pārtveršanas režīma īpašās iezīmes un jo īpaši pieaugošo iejaukšanos personu 8. pantā noteiktajās tiesībās operācijas gaitā dažādajos posmos, kas norādīti iepriekš 325. punktā.

iii) Pieeja, kas izmantojama masveida sakaru pārtveršanas gadījumos

348. Ir skaidrs, ka pirmos divus no sešiem “minimālajiem drošības pasākumiem”, par kuriem Tiesa mērķētas pārtveršanas kontekstā ir atzinusi, ka tie ir skaidri jādefinē valsts tiesību aktos, lai izvairītos no pilnvaru ļaunprātīgas izmantošanas (proti, nodarījumu būtība, kas var būt par pamatu pārtveršanas rīkojuma izdošanai, un to personu kategorijas, kuru sakarus var pārtvert, skat. iepriekš 335. punktu), nav viegli piemērot masveida pārtveršanas režīmam. Līdzīgi arī prasība par “pamatotām aizdomām”, kas paredzēta Tiesas judikatūrā par mērķētu pārtveršanu kriminālizmeklēšanas kontekstā, ir mazāk raksturīga masveida pārtveršanas kontekstā, kuras nolūks principā ir preventīvs, nevis konkrēta mērķa un/vai identificējama noziedzīga nodarījuma izmeklēšanai. Tomēr Tiesa uzskata, ka, ja valsts izmanto šādu režīmu, valsts tiesību aktos ir jāietver detalizēti noteikumi par to, kad iestādes var īstenot šādus pasākumus. Proti, valsts tiesību aktos pietiekami skaidri jānosaka pamatojums, saskaņā ar kuru var atļaut masveida pārtveršanu, un apstākļi, kādos varētu pārtvert personas sakarus. Pārējie četri minimālie drošības pasākumi, ko Tiesa noteica savos iepriekšējos spriedumos, proti, ka valsts tiesību aktos ir jānosaka pārtveršanas ilguma ierobežojums, iegūto datu pārbaudes, izmantošanas un uzglabāšanas kārtība, veicamie piesardzības pasākumi, paziņojot datus citām pusēm, kā arī apstākļi, kādos pārtvertos datus atļauts vai kādos tos ir pienākums dzēst vai iznīcināt, ir vienlīdz svarīgi attiecībā uz masveida pārtveršanu.

349. Tiesa savā judikatūrā par mērķētu pārtveršanu ir ņēmusi vērā pārtveršanas režīma pārraudzības un pārskatīšanas pasākumus (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 233.–234. punktu). Masveida pārtveršanas kontekstā tiks pastiprināta pārraudzības un pārskatīšanas nozīme, jo pastāv ļaunprātīgas izmantošanas risks, turklāt leģitīmā nepieciešamība ievērot slepenību neizbēgami nozīmēs to, ka valsts drošības apsvērumu dēļ valstis bieži vien nevarēs atklāt informāciju par apstrīdētā režīma darbību.

350. Tāpēc, lai samazinātu masveida pārtveršanas pilnvaru ļaunprātīgas izmantošanas risku, Tiesa uzskata, ka attiecībā uz šo procesu ir jāīsteno “no gala līdz galam drošības pasākumi”, kas nozīmē to, ka valsts līmenī izvērtēšana ir jāveic katrā veicamo pasākumu nepieciešamības un samērīguma procesa stadijā, ka minētajai masveida pārtveršanai ir nepieciešama neatkarīga atļauja jau pašā sākumā, kad tiek noteikts operācijas mērķis un tvērums, un ka attiecībā uz operāciju jāīsteno pārraudzība un neatkarīga *ex post facto* pārskatīšana. Tiesa uzskata, ka tie ir fundamentāli drošības pasākumi, kas būs jebkura 8. pantam atbilstoša masveida pārtveršanas režīma stūrakmens (skat. arī Venēcijas komisijas ziņojumu iepriekš 197. punktā, kurā līdzīgi tika atzīts, ka divi no svarīgākajiem drošības pasākumiem masveida pārtveršanas režīmā ir procesa atļauja un pārraudzība).

351. Vispirms pievēršoties atļaujai, Lielā palāta piekrīt palātas viedoklim, ka, lai gan tiesas atļauja ir “svarīgs drošības pasākums pret patvaļu”, tā nav “nepieciešama prasība” (skat. palātas sprieduma 318.–320. punktu). Tomēr masveida pārtveršana jāatļauj kādai neatkarīgai iestādei, proti, no izpildvaras neatkarīgai iestādei.

352. Turklāt, lai nodrošinātu efektīvu aizsardzību pret ļaunprātīgu izmantošanu, neatkarīgā pilnvarotā iestāde jāinformē gan par pārtveršanas nolūku, gan par datu nesējiem vai sakaru kanāliem, kurus varētu pārtvert. Tas ļautu neatkarīgajai pilnvarotajai iestādei izvērtēt masveida pārtveršanas operācijas nepieciešamību un samērīgumu, kā arī to, vai datu nesēju atlase ir nepieciešama un samērīga ar veicamās pārtveršanas nolūkiem.

353. Selektoru, jo īpaši spēcīgo selektoru, izmantošana ir viens no masveida pārtveršanas procesa vissvarīgākajiem posmiem, jo šajā posmā izlūkdienesti var izraudzīties kādas konkrētas personas sakarus. Tomēr, lai gan dažas sistēmas pieļauj iepriekšēju atļauju selektoru kategorijām (skat., piemēram, Zviedrijas sistēmu, kas detalizēti raksturota spriedumā lietā ““Centrum för rättvisa” pret Zviedriju” (pieteikums Nr. 35252/08)), Tiesa norāda, ka gan Apvienotās Karalistes, gan Nīderlandes valdības ir apgalvojušas, ka jebkura prasība atļaujā paskaidrot vai pamatot selektorus vai meklēšanas kritērijus nopietni ierobežotu masveida pārtveršanas efektivitāti (skat. iepriekš 292. un 307. punktu). Tam piekrita *IPT*, kas atzina, ka selektoru iekļaušana atļaujā “lieki apdraudētu un ierobežotu ordera darbību un jebkurā gadījumā būtu praktiski neiespējama” (skat. iepriekš 49. punktu).

354. Ņemot vērā masveida pārtveršanas iezīmes (skat. iepriekš 344.–345. punktu), lielo izmantoto selektoru skaitu un raksturīgo nepieciešamību elastīgi izvēlēties selektorus, ko praksē var izteikt kā ciparu vai burtu tehniskās kombinācijas, Tiesa varētu pieņemt, ka visu selektoru iekļaušana atļaujā praksē var nebūt iespējama. Tomēr, tā kā selektoru un vaicājuma terminu izvēle nosaka to, kuri sakari būs piemēroti analītiķa veiktai pārbaudei, atļaujā jānorāda vismaz izmantojamo selektoru veidi vai kategorijas.

355. Turklāt, ja izlūkdienesti izmanto spēcīgus selektorus, kas saistīti ar identificējamām personām, ir jāievieš pastiprināti drošības pasākumi. Izlūkdienestiem katra šāda selektora izmantošana ir jāpamato, ņemot vērā nepieciešamības un samērīguma principu, turklāt šis pamatojums ir rūpīgi jāfiksē un tam ir nepieciešama iepriekšēja iekšējā atļauja, kuras ietvaros atsevišķi un objektīvi tiek pārbaudīts, vai pamatojums atbilst iepriekš minētajiem principiem.

356. Tāpat kādai neatkarīgai iestādei ir jāpārrauga katrs masveida pārtveršanas procesa posms, tostarp sākotnējā atļaujas sniegšana un jebkura turpmāka atjaunošana, nesēju atlasīšana, selektoru un vaicājumu terminu izvēle un piemērošana, kā arī pārtvertā materiāla izmantošana, uzglabāšana, turpmāka pārraidīšana un dzēšana, turklāt šai pārraudzībai ir jābūt pietiekami stingrai, lai “iejaukšanās” būtu “nepieciešama demokrātiskā sabiedrībā” (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 232. punktu, iepriekš minētā sprieduma lietā “Klass un citi” 49., 50. un 59. punktu, iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 106. punktu, kā arī iepriekš minētā sprieduma lietā “Kenedijs” 153. un 154. punktu). Jo īpaši pārraudzības iestādei ir jābūt iespējai izvērtēt veicamās darbības nepieciešamību un samērīgumu, pienācīgi ņemot vērā atbilstošo apmēru, kādā notiks iejaukšanās šā procesa gaitā, visticamāk, skartās personas tiesībās, kas noteiktas Konvencijā. Lai atvieglotu šo pārraudzību, izlūkdienestiem katrā procesa posmā jāveic detalizēta uzskaite.

357. Visbeidzot, ikvienai personai, kurai radušās aizdomas, ka izlūkdienesti ir pārtvēruši tās sakarus, jābūt pieejamam efektīvam tiesiskās aizsardzības līdzeklim, lai apstrīdētu iespējamās pārtveršanas likumību vai pārtveršanas režīma atbilstību Konvencijai. Mērķētas pārtveršanas kontekstā Tiesa vairākkārt ir atzinusi, ka turpmāka informēšana saistībā ar uzraudzības pasākumiem ir svarīgs faktors, tiesā izvērtējot tiesiskās aizsardzības līdzekļu efektivitāti un līdz ar to arī to, vai ir ieviesti efektīvi drošības pasākumi pret uzraudzības pilnvaru ļaunprātīgu izmantošanu. Tomēr tā ir atzinusi, ka informēšana nav nepieciešama, ja iekšējo tiesiskās aizsardzības līdzekļu sistēma ļauj jebkurai personai, kurai radušās aizdomas, ka tiek vai ir tikuši pārtverti tās sakari, vērsties tiesā, citiem vārdiem sakot, ja tiesu jurisdikcija nav atkarīga no pārtveršanas subjekta informēšanas par to, ka ir notikusi tā sakaru pārtveršana (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 234. punktu un iepriekš minētā sprieduma lietā “Kenedijs” 167. punktu).

358. Tiesa uzskata, ka tiesiskās aizsardzības līdzeklis, kas nav atkarīgs no pārtveršanas subjekta informēšanas, varētu būt efektīvs tiesiskās aizsardzības līdzeklis arī masveida pārtveršanas kontekstā. Patiesībā atkarībā no apstākļiem tas pat var sniegt labākas garantijas atbilstošai procedūras norisei nekā sistēma, kuras pamatā ir informēšana. Neatkarīgi no tā, vai materiāls iegūts mērķētas vai masveida pārtveršanas rezultātā, izņēmuma gadījumā rīkojoties valsts drošības interesēs, informēšanas prasībai nebūs praktiskas ietekmes. Iespējamība, ka informēšanas prasībai būs maza praktiska ietekme vai tādas nebūs vispār, būs lielāka masveida pārtveršanas kontekstā, jo šādu uzraudzību var izmantot ārvalstu izlūkdatu vākšanas nolūkos, un tā lielākoties būs vērsta uz tādu personu sakariem, kuras atrodas ārpus valsts teritoriālās jurisdikcijas. Tāpēc, pat ja mērķa identitāte ir zināma, iestādes var nebūt informētas par tā atrašanās vietu.

359. Iestādes pilnvaras un procesuālās garantijas ir svarīgas, lai noteiktu, vai tiesiskās aizsardzības līdzeklis ir efektīvs. Tāpēc, ja nav noteikta informēšanas prasība, ir svarīgi, lai tiesiskās aizsardzības līdzeklis būtu pieejams iestādē, kura, lai gan ne vienmēr ir tiesu iestāde, ir neatkarīga no izpildvaras un nodrošina tiesvedības godīgumu, piedāvājot uzklausīšanas procesu, ciktāl tas praktiski iespējams. Šādas iestādes lēmumiem jābūt pamatotiem un juridiski saistošiem, *inter alia* attiecībā uz nelikumīgas pārtveršanas pārtraukšanu un nelikumīgi iegūta un/vai uzglabāta pārtvertā materiāla iznīcināšanu (skat. *mutatis mutandis* sprieduma lietā Nr. 62332/00 “Segerstete-Viberga [*Segerstedt-Wiberg*] un citi pret Zviedriju” 120. punktu, ECT 2006-VII, kā arī iepriekš minētā sprieduma lietā “Leanders” 81.–83. punktu, kurā galvenais piedāvātās kontroles trūkums bija tāds, ka nebija paredzētas pilnvaras pieņemt juridiski saistošu lēmumu).

360. Ņemot vērā iepriekš minēto, Tiesa noteiks, vai masveida pārtveršanas režīms atbilst Konvencijai, veicot visaptverošu režīma darbības izvērtējumu. Šāds izvērtējums galvenokārt būs vērsts uz to, vai valsts tiesiskajā regulējumā ir ietvertas pietiekamas garantijas pret ļaunprātīgu izmantošanu un vai process ir pakļauts “no gala līdz galam drošības pasākumiem” (skat. iepriekš 350. punktu). Izvērtēšanas gaitā tā ņems vērā pārtveršanas sistēmas faktisko darbību, tostarp pilnvaru īstenošanas pārbaudes un līdzsvaru, kā arī faktiskas ļaunprātīgas izmantošanas pierādījumu esību vai neesību (skat. iepriekš minētā sprieduma lietā “Eiropas integrācijas un cilvēktiesību asociācija un Ekimdžijevs” 92. punktu).

361. Izvērtējot, vai atbildētāja valsts ir rīkojusies savas rīcības brīvības robežās (skat. iepriekš 347. punktu), Tiesai būtu jāņem vērā vairāk kritēriju, nevis tikai seši spriedumā lietā “Vēbere” noteiktie drošības pasākumi. Proti, kopīgi izvērtējot jēdzienus “saskaņā ar likumu” un “nepieciešamība”, kas šajā ziņā ir jau iedibināta pieeja (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 236. punktu un iepriekš minētā sprieduma lietā “Kenedijs” 155. punktu), Tiesa izvērtēs, vai valsts tiesiskajā regulējumā ir skaidri noteikts turpmākais:

1. pamatojums, saskaņā ar kuru var atļaut masveida pārtveršanu;

2. apstākļi, kādos var pārtvert personas sakarus;

3. atļaujas piešķiršanas kārtība;

4. pārtvertā materiāla atlasīšanas, pārbaudīšanas un izmantošanas kārtība;

5. veicamie piesardzības pasākumi, paziņojot materiālu citām pusēm;

6. ierobežojumi attiecībā uz pārtveršanas ilgumu, pārtvertā materiāla uzglabāšanu un apstākļiem, kādos šis materiāls ir jādzēš un jāiznīcina;

7. kārtība un veidi, kādā neatkarīgā iestāde pārrauga atbilstību iepriekš minētajiem drošības pasākumiem, un to pilnvaras izvērtēt neatbilstības;

8. kārtība, kādā veic šādas atbilstības neatkarīgu *ex post facto* pārskatīšanu, un kompetentās iestādes pilnvaras izvērtēt neatbilstību gadījumus.

362. Lai gan tas ir viens no spriedumā lietā “Vēbere” noteiktajiem kritērijiem, Tiesa līdz šim vēl nav sniegusi īpašus norādījumus par piesardzības pasākumiem, kas jāievēro, paziņojot pārtverto materiālu citām pusēm. Tomēr tagad ir skaidrs, ka dažas valstis regulāri apmainās ar materiālu ar saviem izlūkošanas partneriem un atsevišķos gadījumos pat nodrošina tiem tiešu piekļuvi savām sistēmām. Līdz ar to Tiesa uzskata, ka masveida pārtveršanas ietvaros iegūta materiāla pārsūtīšana uz ārvalstīm vai starptautiskām organizācijām, ko veic līgumslēdzēja valsts, ir jāierobežo, ļaujot pārsūtīt vienīgi materiālu, kas apkopots un uzglabāts saskaņā ar Konvenciju, un uz to jāattiecina noteikti īpaši papildu drošības pasākumi, kas attiecas uz pašu pārsūtīšanu. Pirmkārt, valsts tiesību aktos ir skaidri jānosaka apstākļi, kādos var veikt šādu pārsūtīšanu. Otrkārt, pārsūtošajai valstij ir jānodrošina, lai saņēmēja valsts, apstrādājot datus, būtu ieviesusi drošības pasākumus, ar kuriem iespējams novērst ļaunprātīgu izmantošanu un nesamērīgu iejaukšanos. Saņēmējai valstij jo īpaši ir jāgarantē materiāla droša uzglabāšana un jāierobežo tā tālāka izpaušana. Tas ne vienmēr nozīmē, ka saņēmējai valstij ir jāparedz tāda pati aizsardzība kā pārsūtošajā valstī vai ka garantija būtu jāsniedz pirms katras pārsūtīšanas. Treškārt, pastiprināti drošības pasākumi būs nepieciešami, ja būs skaidrs, ka tiek pārsūtīts materiāls, attiecībā uz kuru jāievēro īpaša konfidencialitāte, piemēram, konfidenciāls žurnālistikas materiāls. Visbeidzot Tiesa uzskata, ka arī materiāla pārsūtīšana ārvalstu izlūkošanas partneriem jāpakļauj neatkarīgai kontrolei.

363. Pamatojoties uz iepriekš 342. punktā izklāstītajiem iemesliem, Tiesa nav guvusi pārliecību, ka saistīto sakaru datu iegūšana, izmantojot masveida pārtveršanu, rada mazāku iejaukšanos nekā satura iegūšana. Tāpēc tā uzskata, ka saistīto sakaru datu pārtveršana, saglabāšana un meklēšana ir jāanalizē, atsaucoties uz tiem pašiem drošības pasākumiem, kurus piemēro saturam.

364. Tomēr, lai gan saistīto sakaru datu pārtveršanu parasti atļauj vienlaikus ar satura pārtveršanu, izlūkdienesti pēc to iegūšanas tos var apstrādāt atšķirīgi (skat., piemēram, iepriekš 153.–154. punktu). Ņemot vērā saistīto sakaru datu atšķirīgās iezīmes un veidus, kā tos izmanto izlūkdienesti, kamēr vien tiek īstenoti iepriekš minētie drošības pasākumi, Tiesa uzskata, ka tiesību normām, kas reglamentē to apstrādi, ne vienmēr visos aspektos jābūt identiskām satura apstrādi regulējošajām tiesību normām.

iv) Šīs lietas izvērtējums, ko veikusi Tiesa

α) Sākotnējās piezīmes

365. Attiecīgajā brīdī masveida pārtveršanai juridiskais pamats bija noteikts *RIPA* I nodaļā.Turklāt Tiesa ir pārliecināta, ka ar minēto režīmu īstenoja leģitīmus mērķus, proti, aizsargāt valsts drošību, novērst nekārtības un noziedzību un aizsargāt citu personu tiesības un brīvības. Tāpēc, ņemot vērā iepriekš 334. punktā izklāstīto pieeju, ir jāizvērtē, vai valsts tiesību akti bija pieejami un tajos bija noteikti atbilstoši un efektīvi drošības pasākumi un garantijas, lai izpildītu prasības par “paredzamību” un “nepieciešamību demokrātiskā sabiedrībā”.

366. Attiecīgās tiesību normas, kas reglamentē masveida pārtveršanas režīma darbību, neapšaubāmi bija sarežģītas, proti, lielākajā daļā ziņojumu par Apvienotās Karalistes slepenās uzraudzības režīmiem ir kritizēts to skaidrības trūkums (skat. iepriekš 143., 152. un 157. punktu). Tomēr šīs tiesību normas bija precizētas pievienotajā *IC* kodeksā (skat. iepriekš 96. punktu). *IC* kodeksa 6.4. punktā bija skaidri norādīts, ka notiek masveida pārtveršana, kā arī sniegta detalizēta informācija par to, kā šis konkrētais uzraudzības režīms darbojās praksē (skat. iepriekš 96. punktu). *IC* kodekss ir publisks abu parlamenta palātu apstiprināts dokuments, ko Valdība publicē tiešsaistē un drukātā versijā un kas ir jāņem vērā gan personām, kuras veic pārtveršanas pienākumus, gan tiesām (skat. iepriekš 93.–94. punktu). Līdz ar to šī Tiesa ir pieņēmusi, ka tā tiesību normas var ņemt vērā, izvērtējot *RIPA* paredzamību (skat. iepriekš minētā sprieduma lietā “Kenedijs” 157. punktu). Tādējādi Tiesa pieņemtu, ka valsts tiesību akti bija pienācīgi “pieejami”.

367. Pievēršoties nākamajam jautājumam par to, vai tiesību akti paredzēja atbilstošus un efektīvus drošības pasākumus un garantijas, lai izpildītu prasības par “paredzamību” un “nepieciešamību demokrātiskā sabiedrībā”, Tiesa β) apakšiedaļā izvērtēs iepriekš 361. punktā izklāstītās astoņas prasības saistībā ar elektronisko sakaru satura pārtveršanu. Savukārt γ) apakšiedaļā tā konkrētāk izvērtēs saistīto sakaru datu pārtveršanu.

β) Sakaru satura pārtveršana

* 1. Pamatojums, saskaņā ar kuru var atļaut masveida pārtveršanu

368. Saskaņā ar *RIPA* 5. panta 3. punktu un *IC* kodeksa 6.11. punktu (skat. iepriekš 62. un 96. punktu) valsts sekretārs(-e) varēja izdot masveida pārtveršanas orderi vienīgi tad, ja viņš vai viņa bija pārliecināts(-ta), ka tas bija nepieciešams valsts drošības interesēs, lai novērstu vai atklātu nopietnu noziegumu, vai Apvienotās Karalistes ekonomiskās labklājības nodrošināšanai, ciktāl šīs intereses atbilda valsts drošības interesēm.

369. Uz šiem pamatojumiem attiecās turpmāk minētie ierobežojumi. Pirmkārt, *IC* komisārs bija precizējis, ka praksē “valsts drošības” interesēs ir atļauts uzraudzīt darbības, kuras apdraud valsts drošību vai labklājību, un darbības, kuru mērķis ir apdraudēt vai graut parlamentāro demokrātiju ar politiskiem, rūpnieciskiem vai vardarbīgiem līdzekļiem (skat. iepriekš minētā sprieduma lietā “Kenedijs” 333. punktu). Otrkārt, *RIPA* 81. panta 2. punktā b) apakšpunktā smags noziegums ir definēts kā noziegums, par kuru personai (pieņemot, ka tā sasniegusi divdesmit viena gada vecumu un tai nav iepriekšējas sodāmības) pamatoti varētu piespriest brīvības atņemšanu uz trim gadiem vai ilgāk, vai, ja rīcība izpaužas kā vardarbība, tās rezultātā gūts būtisks finansiāls labums vai arī rīcība ir attiecināma uz lielu skaitu personu, kas rīkojās kopēja mērķa sasniegšanai (skat. iepriekš 63. punktu). Treškārt, *RIPA* 17. pantā un *IC* kodeksa 8.3. punktā ir noteikts, ka parasti ne pārtveršanas iespējai, ne pašam pārtvertajam materiālam nevar būt nekādas nozīmes tiesvedībā (skat. iepriekš 83. un 96. punktu). Līdz ar to, lai gan pārtveršanu varētu izmantot, lai novērstu vai atklātu smagus noziegumus, pārtveršanas materiālu nevar izmantot kriminālvajāšanai attiecībā uz kādu noziedzīgu nodarījumu. Turklāt *IC* kodeksa 6.8. punkts paredz, ka 8. panta 4. punktā noteiktā ordera nolūks “parasti atspoguļo vienu vai vairākas Valsts drošības padomes noteiktās izlūkošanas prioritātes” (skat. iepriekš 96. un 98. punktu).

370. Principā, jo plašāks pamatojums, jo lielāka ir ļaunprātīgas izmantošanas iespēja. Tomēr šaurāki un/vai stingrāk definēti pamatojumi nodrošinātu efektīvu garantiju pret ļaunprātīgu izmantošanu vienīgi tad, ja būtu pietiekami ar citiem drošības pasākumiem, lai nodrošinātu, ka masveida pārtveršana ir atļauta vienīgi atbilstoši atļautajam pamatojumam un ka tā ir nepieciešama un samērīga šim nolūkam. Tāpēc ar to cieši saistītais jautājums par to, vai bija pietiekamas garantijas, lai nodrošinātu, ka pārtveršana bija nepieciešama vai pamatota, ir tikpat svarīgs kā tas, cik precīzi ir definēts atļaujas piešķiršanas pamatojums. Līdz ar to Tiesa uzskata, ka režīms, kas ļauj uzdot masveida pārtveršanu atbilstoši salīdzinoši plašam pamatojumam, joprojām var atbilst Konvencijas 8. pantam, ja sistēma, to aplūkojot kopumā, paredz pietiekamas garantijas pret ļaunprātīgu izmantošanu, lai kompensētu šo trūkumu.

371. Apvienotās Karalistes gadījumā, lai gan pamatojums, saskaņā ar kuru varētu atļaut masveida pārtveršanu, bija formulēts samērā plaši, tas joprojām bija vērsts uz valsts drošību, kā arī smagiem noziegumiem un valsts ekonomisko labklājību, ciktāl šīs intereses atbilda valsts drošības interesēm (skat. iepriekš 368. punktu). Tādēļ Tiesa izvērtēs pārējos drošības pasākumus, kas ietverti 8. panta 4. punktā noteiktajā režīmā, lai noteiktu, vai šis režīms, to aplūkojot kopumā, atbilda Konvencijas 8. pantam.

* 2. Apstākļi, kādos var pārtvert personas sakarus

372. *IC* kodeksa 6.2. punktā (skat. iepriekš 96. punktu) ir skaidri noteikts, ka “atšķirībā no 8. panta 1. punktā minētā, 8. panta 4. punktā noteiktajā orderī nav jānosauc vai jāraksturo pārtveršanas subjekts vai jānorāda telpas, saistībā ar kurām veicama pārtveršana. Tāpat 8. panta 4. punkts neuzliek par pienākumu ierobežot to ārējo sakaru apjomu, kas var tikt pārtverti”. Citiem vārdiem sakot, par mērķi tika izvirzīti sakaru nesēji, nevis ierīces, no kurām sakari pārsūtīti, vai sakaru sūtītāji vai saņēmēji. Ja nav noteikti nekādi ierobežojumi attiecībā uz to sakaru apjomu, ko varēja pārtvert, šķiet, ka visas sakaru paketes, ko pārraidīja cauri izraudzītajiem nesējiem, kamēr orderis bija spēkā, bija pārtvertas.

373. Līdz ar to 8. panta 4. punktā noteiktais orderis bija ārējo sakaru pārtveršanas orderis (skat. iepriekš 72. punktu) un *IC* kodeksa 6.7. punkts (skat. iepriekš 96. punktu) uzlika pārtveršanas aģentūrai, kura veica pārtveršanu atbilstoši 8. panta 4. punktā noteiktajam orderim, par pienākumu izmantot tās zināšanas par veidu, kādā tiek maršrutēti starptautiskie sakari, kā arī regulāri pārbaudīt attiecīgos sakaru kanālus, lai apzinātu tos individuālos sakaru nesējus, kuri, visticamāk, saturēs ārējos sakarus, kas atbildīs valsts sekretāra apliecinātajiem materiāla aprakstiem. Tai arī bija jāveic pārtveršana tā, lai ierobežotu tādu sakaru apkopošanu, kas nav ārēji sakari, līdz minimumam, kas atbilst nepieciešamo ārējo sakaru pārtveršanas mērķim. Līdz ar to nesējus neatlasīja pēc nejaušības principa. Gluži pretēji, tos atlasīja, jo tika uzskatīts, ka tie, visticamāk, saturēs ārējos sakarus ar izlūkošanas vērtību.

374. *IC* kodeksa 6.5. punktā “ārējie sakari” definēti kā sakari, ko nosūta vai saņem ārpus Britu salām (skat. iepriekš 96. punktu). Ja gan sūtītājs, gan saņēmējs atrodas Britu salās, runa ir par iekšējiem sakariem. Tādējādi tas, vai sakari ir “ārēji”, ir atkarīgs no sūtītāja un saņēmēja ģeogrāfiskās atrašanās vietas, nevis no maršruta, pa kuru sakari nonāca līdz mērķim. Sakari, kas šķērso Apvienotās Karalistes robežas (starptautiskie sakari), joprojām var būt “iekšēji”, jo no Apvienotās Karalistes nosūtītos un tajā saņemtos sakarus (vai sakaru paketes) tomēr var maršrutēt caur vienu vai vairākām trešām valstīm.

375. Tādējādi iekšējo un ārējo sakaru nošķiršana neliedza pārtvert iekšējos sakarus, kas tiek pārraidīti, šķērsojot Apvienotās Karalistes robežas, un faktiski šādu sakaru “piezveja” bija skaidri atļauta saskaņā ar *RIPA* 5. panta 6. punktu ar nosacījumu, ka rīcība, kas atļauta ar pārtveršanas orderi, ietver tādu sakaru pārtveršanu, kas nav norādīti orderī, ja nepieciešams veikt to, kas orderī skaidri atļauts (skat. iepriekš 68. punktu). Turklāt pati jēdziena “ārējs” definīcija ir pietiekami plaša, lai ietvertu informācijas saglabāšanu mākoņkrātuvē, kā arī personas pārlūkošanas darbības un darbības sociālajos tīklos Apvienotajā Karalistē (skat. iepriekš 75. un 76. punktu). Tomēr, kā atzina palāta, “ārējo sakaru” drošības pasākumam bija nozīme makrolīmenī, atlasot pārtveršanai nesējus (skat. palātas sprieduma 337. punktu); tā kā pārtveršanas aģentūrai bija jāizmanto savas zināšanas par veidu, kādā tiek maršrutēti starptautiskie sakari, lai apzinātu tos sakaru nesējus, kuri, visticamāk, satur operācijai vērtīgus ārējos sakarus, drošības pasākums, lai arī ierobežotā mērā, ierobežoja to cilvēku kategorijas, kuru sakari var tikt pārtverti. Tas attiecās arī uz jautājumu par samērīgumu, jo valstīm varētu būt pieejams mazāk iejaukšanās pasākumu, lai iegūtu to teritoriālajā jurisdikcijā esošo personu sakarus.

376. Ņemot vērā iepriekš minēto, Tiesa uzskata, ka ir skaidrs, ka atbilstoši 8. panta 4. punktā noteiktajam režīmam starptautiskos sakarus (proti, valsts robežas šķērsojošos sakarus) varētu pārtvert un ka izlūkdienesti būtu pilnvaroti pārtvert vienīgi tos nesējus, kuri, visticamāk, satur ārējos sakarus, kas interesētu izlūkošanu. Masveida pārtveršanas kontekstā ir grūti abstrakti iedomāties, kā varētu vēl vairāk ierobežot apstākļus, kādos var tikt pārtverti personas sakari. Jebkurā gadījumā ne elektronisko sakaru sūtītājs, ne to saņēmējs nevarētu kontrolēt to pārraides maršrutu, turklāt praksē jebkuru turpmāki ierobežojumi attiecībā uz nesēju izvēli šajā ziņā nebūtu padarījuši valsts tiesību aktus paredzamākus. Līdz ar to Tiesa varētu atzīt, ka apstākļi, kādos iespējams pārtvert personas sakarus atbilstoši 8. panta 4. punktā noteiktajam orderim, Konvencijas 8. punkta izpratnē bija pietiekami “paredzami”.

* 3. Atļaujas piešķiršanas kārtība

377. Pieteikumu 8. panta 4. punktā noteiktā ordera izdošanai iesniedza valsts sekretāram, kurš vienīgais bija pilnvarots izdot šādu orderi. Pirms iesniegšanas katru pieteikumu pārskatīja aģentūra, kura to sagatavojusi. Tas ietvēra vairāk nekā vienas amatpersonas veiktu rūpīgu pārbaudi, kurām bija jāizvērtē, vai pieteikums bija iesniegts nolūkam, uz kuru attiecas *RIPA* 5. panta 3. punkts, un vai ierosinātā pārtveršana atbilda Konvencijas nepieciešamības un samērīguma standartiem (skat. *IC* kodeksa 6.9. punktu iepriekš 96. punktā). Šāds papildu iekšējās pārbaudes līmenis, protams, bija vērtīgs, taču attiecīgajā brīdī masveida pārtveršanu saskaņā ar 8. panta 4. punktā noteikto režīmu atļāva veikt valsts sekretārs, nevis kāda no izpildvaras neatkarīga iestāde. Līdz ar to 8. panta 4. punkta noteiktajam režīmam trūka viena galvenā drošības pasākuma, proti, neatkarīgai atļaujai attiecībā uz masveida pārtveršanu jābūt saņemtai jau pašā sākumā (skat. iepriekš 350. punktu).

378. Attiecībā uz valsts sekretāra nodrošinātās pārbaudes līmeni *IC* kodeksa 6.10. punktā ir detalizēti izklāstīta pieteikumā iekļaujamā informācija (skat. iepriekš 96. punktu). Tā ietvēra pārtveramo sakaru aprakstu, informāciju par sakaru pakalpojumu sniedzēju(-iem) un operācijas iespējamības izvērtējumu, ja tas nepieciešams, kā arī atļautās rīcības aprakstu, apliecinājumu, kas reglamentētu pārtvertā materiāla pārbaudi (skat. turpmāk 378. un 379. punktu), paskaidrojumu, kādēļ pārtveršana uzskatāma par nepieciešamu vienam vai vairākiem 5. panta 3. punktā minētajiem nolūkiem, apsvērumus, kādēļ šī rīcība ir samērīga ar sasniedzamo mērķi, garantiju par to, ka pārtvertā materiāla lasīšana, aplūkošana vai klausīšanās notiks tikai tiktāl, ciktāl tas ir apliecināts un atbilst *RIPA* 16. panta 2.–6. punktā minētajiem nosacījumiem, kā arī garantiju par to, ka pārtverto materiālu apstrādās saskaņā ar 15. un 16. pantā noteiktajiem drošības pasākumiem.

379. Tāpēc valsts sekretāru informēja par operācijas nolūku (kam bija jābūt vienam no 5. panta 3. punktā noteiktajiem nolūkiem), un pirms ordera izdošanas viņam bija jāpārliecinās, ka tas ir nepieciešams šim nolūkam un ir samērīgs ar sasniedzamo mērķi (skat. *IC* kodeksa 6.11. un 6.13. punktu iepriekš 96. punktā). Izvērtējot samērīgumu, valsts sekretāram bija jāapsver, vai orderis bija pārmērīgs, ņemot vērā lietas vispārējos apstākļus, un vai nepieciešamo informāciju varēja pamatoti iegūt ar mazāk aizskarošu līdzekļu palīdzību (skat. *IC* kodeksa 3.6. punktu iepriekš 96. punktā). Jo īpaši iejaukšanās apmērs un tvērums bija jāizvērtē kopsakarā ar sasniedzamo mērķi, bija jāpaskaidro, kā un kāpēc metodes rada mazāko iespējamo iejaukšanos subjekta un citu personu tiesībās, bija jāizvērtē, vai darbība ir piemērots veids nepieciešamā rezultāta sasniegšanai, ņemot vērā visas saprātīgās alternatīvas, un bija jāsniedz pierādījumi, ciktāl tas praktiski iespējams, par citām apsvērtajām metodēm, kas tika atzītas par nepietiekamām, lai sasniegtu darbības mērķus (skat. *IC* kodeksa 3.7. punktu iepriekš 96. punktā).

380. Lai gan pieteikumā 8. panta 4. punktā noteiktā ordera izdošanai bija jāiekļauj “pārtveramo sakaru apraksts” un “informācija par sakaru pakalpojumu sniedzēju(-iem)”, Valdība sēdē apstiprināja, ka orderī nebija precizēti konkrēti nesēji, jo tas būtu “ļoti nepraktiski un sarežģīti”, ja pastāvētu šāda prasība. Tomēr bija atbilstoši jāapraksta, ko pārtveršana ietvers, kā arī jānorāda informācija par pārtveramo “nesēju veidiem”. Šī informācija liecināja par valsts sekretāra izvērtējumu saistībā ar pieteikumā raksturotās rīcības nepieciešamību un samērīgumu. Turklāt Valdība savos argumentos Lielajai palātai apstiprināja, ka *GCHQ* regulāri informēja *IC* komisāru par pamatojumu, atbilstoši kuram nesējus atlasīja pārtveršanai (skat. iepriekš 290. punktu).

381. Pieteikumā 8. panta 4. punktā noteiktā ordera izdošanai arī nebija jānorāda izmantojamo selektoru kategorijas. Līdz ar to apstiprināšanas posmā nebija iespējas izvērtēt to nepieciešamību un samērīgumu, lai gan attiecībā uz selektoru izvēli pēc tam veica neatkarīgu pārraudzību. Valdība savos argumentos Lielajā palātā apstiprināja, ka ik reizi, kad sistēmai pievienoja kādu jaunu selektoru, to veicošajam analītiķim bija jāizveido rakstveida ieraksts, paskaidrojot, kādēļ selektora piemērošana valsts sekretāra apliecinājumā norādītajos nolūkos ir nepieciešama un samērīga. To veica, atlasot tekstu no nolaižamās izvēlnes, pēc kā analītiķis pievienoja tekstu brīvā formā, paskaidrojot, kādēļ meklēšana bija nepieciešama un samērīga. Turklāt selektoru izmantošana bija jāreģistrē apstiprinātā vietā, kurā tos bija iespējams pārbaudīt un izveidot meklējamu izmantojamo selektoru ierakstu un kurā *IC* komisārs tos varēja pārraudzīt (skat. iepriekš 291.–292. punktu). Līdz ar to *IC* komisāram bija jāpārrauga selektoru izvēle, un savā 2016. gada ziņojumā viņš norādīja, ka viņu “pārsteidza tas, cik kvalitatīvi bija paziņojumi”, kurus bija sagatavojuši analītiķi un kuros bija paskaidrots, kādēļ jauna selektora pievienošana ir nepieciešama un samērīga (skat. iepriekš 177. punktu).

382. Ņemot vērā to, ka selektoru un vaicājumu terminu izvēle nosaka, kuri sakari būtu piemēroti, lai analītiķis tos pārbaudītu, Tiesa ir norādījusi, ka ir ļoti svarīgi, lai atļaujā norādītu vismaz selektoru kategorijas un lai tiem spēcīgajiem selektoriem, kas attiecas uz identificējamām personām, veiktu iepriekšēju iekšēju apstiprināšanu, kas ļautu pārbaudīt, vai pamatojums atbilst iepriekš minētajiem principiem (skat. iepriekš 353.–355. punktu).

383. Šajā lietā selektoru kategoriju pārraudzības neesība apstiprināšanas posmā bija 8. panta 4. punktā noteiktā režīma trūkums. Arī visu individuālo selektoru turpmākā kontrole neatbilda prasībai par pastiprinātiem drošības pasākumiem, lai izmantotu spēcīgus selektorus, kas saistīti ar identificējamām personām, un nepieciešamībai ieviest iepriekšējas iekšējās atļaujas izsniegšanas procesu, kura ietvaros atsevišķi un objektīvi tiek pārbaudīts, vai pamatojums atbilst iepriekš minētajiem principiem (skat. iepriekš 355. punktu). Lai gan analītiķiem ir jāfiksē un jāpamato ikviena selektora izmantošana attiecībā uz Konvencijā noteikto nepieciešamības un samērīguma principu un attiecībā uz šo pamatojumu *IC* komisāram ir jāveic neatkarīga pārraudzība, spēcīgiem selektoriem, kas saistīti ar identificējamām personām, tomēr nav nepieciešama iepriekšēja iekšējā atļauja.

* 4. Pārtvertā materiāla atlasīšanas, pārbaudīšanas un izmantošanas kārtība

384. *IC* kodeksa 6.4. punktā ir noteikts, ka tad, kad atbilstoši 8. panta 4. punktā noteiktajam orderim iegūts liels sakaru apjomus, pilnvarotās personas pārtveršanas aģentūrā nevar piemērot spēcīgos selektorus un kompleksus vaicājumus, lai izveidotu sarakstu (skat. iepriekš 96. punktu). Šo atlases procesu nosaka *RIPA* 16. panta 2. punkts un *IC* kodeksa 7.19. punkts, kas paredz, ka selektors nevar attiekties uz personu, par kuru zināms, ka tā atrodas Britu salās, un tā nolūks ir identificēt tās pārsūtītajos vai tai paredzētajos sakaros ietverto materiālu, ja vien valsts sekretārs nav personīgi atļāvis izmantot selektoru, iepriekš pārliecinoties, ka tas ir nepieciešams valsts drošības interesēs, lai novērstu vai atklātu smagus noziegumus vai nodrošinātu Apvienotās Karalistes ekonomisko labklājību, ciktāl šīs intereses atbilst arī valsts drošības interesēm, kā arī šis atlases process ir samērīgs (skat. iepriekš 85. un 96. punktu).

385. Analītiķis var aplūkot vienīgi sarakstā esošo materiālu (skat. iepriekš 96. un 289. punktu), turklāt nav atļauts sagatavot nevienu izlūkošanas ziņojumu par jebkuriem sakariem vai sakaru datiem, ja vien tos nav aplūkojis analītiķis (skat. iepriekš 289. punktu). Turklāt *IC* kodeksa 7.13. punkts paredzēja, ka attiecīgās personas var pārbaudīt vienīgi valsts sekretāra apliecinājumā raksturoto materiālu un ka nevienai amatpersonai nebija atļauts piekļūt materiālam, kas nav norādīts apliecinājumā (skat. iepriekš 96. punktu). Savukārt 6.4. punktā bija noteikts, ka, pirms pārtveršanas aģentūras pilnvarotā persona var piekļūt konkrētiem sakariem, attiecīgajai personai bija jāpaskaidro, kāpēc tas ir nepieciešams kādam no pievienotajā apliecinājumā norādītajiem iemesliem un kāpēc šāda rīcība konkrētajos apstākļos ir samērīga, izvērtējot, vai informāciju pamatoti nav iespējams iegūt ar mazāk ierobežojošu līdzekļu palīdzību (skat. iepriekš 96. punktu).

386. Valsts sekretāra(-es) apliecinājums bija izdots, kad viņš vai viņa piešķīra orderi, un tā mērķis bija nodrošināt, ka atlasīšanas process pārtvertajam materiālam tiek piemērots tā, lai attiecīgās personas pārbaudītu vienīgi apliecinājumā raksturoto materiālu (skat. *IC* kodeksa 6.3. un 6.14. punktu iepriekš 96. punktā). Lai gan apliecinājumam bija svarīga loma, regulējot piekļuvi pārtvertajam materiālam, gan *ISC*, gan terorisma apkarošanas tiesiskā regulējuma neatkarīgā pārskatītāja ziņojumos kritizēja to, ka šajos apliecinājumos norādītais materiāls ir formulēts ļoti vispārīgi (piemēram, “materiāls, kas sniedz izlūkdatus par terorismu, kā noteikts 2000. gada Terorisma apkarošanas likumā (ar attiecīgajiem grozījumiem)) (skat. palātas sprieduma 342. punktu un iepriekš 146. un 155. punktu). Tiesa piekrīt palātai, ka tas ir 8. panta 4. punkta režīma ietvaros pieejamo drošības pasākumu sistēmas trūkums.

387. Tomēr saskaņā ar *ISC*, lai gan apliecinājumā ir noteiktas vispārīgās informācijas kategorijas, kuras var pārbaudīt, praksē pārbaudāmos sakarus nosaka tieši datu nesēju atlase un vienkāršu selektoru un sākotnējā meklēšanas kritēriju piemērošana, savukārt pēc tam – kompleksā meklēšana (skat. iepriekš 146.–147. punktu). Citiem vārdiem sakot, lai gan apliecinājumi regulē to, kā analītiķi atlasa materiālu no datorizēti izveidota saraksta, tieši datu nesēju un selektoru/meklēšanas vārdu izvēle nosaka, kuri sakari vispār ietverti šajā sarakstā (un kurus līdz ar to var pārbaudīt). Tomēr Tiesa jau ir atzinusi, ka selektoru kategoriju nenorādīšana pieteikumā ordera izdošanai un fakts, ka attiecībā uz spēcīgajiem selektoriem, kas saistīti ar kādu identificējamu personu, netiek saņemta iepriekšēja iekšēja atļauja, ir 8. panta 4. punktā noteiktā režīma trūkumi (skat. iepriekš 382. punktu). Šos trūkumus būtu pastiprinājis valsts sekretāra apliecinājuma vispārīgais veids. Līdzās tam, ka attiecībā uz saraksta izveidei izmantoto selektoru kategorijām neizsniedza iepriekšēju neatkarīgu atļauju un ka šādu atļauju neizsniedza arī attiecībā uz tiem spēcīgajiem selektoriem, kas attiecas uz kādu identificējamu personu, apliecinājumā, kas reglamentēja piekļuvi šajā sarakstā esošajam materiālam, bija lietoti nepietiekami precīzi termini, lai nodrošinātu jēgpilnu ierobežojumu.

388. *IC* kodeksa 7.16. punkts arī nosaka, ka analītiķim, kurš vēlas piekļūt sarakstā esošajam materiālam, ir jānorāda apstākļi, kas, visticamāk, var radīt zināmu netiešu iejaukšanos personas tiesībās uz privātās dzīves neaizskaramību, kā arī pasākumi, kas veikti, lai samazinātu šādas iejaukšanās apmēru (skat. iepriekš 96. punktu). Jebkura turpmāka analītiķa piekļuve ir ierobežota ar noteiktu laika periodu, un, ja šis laika periods tiek atjaunots, ieraksts ir jāatjaunina, norādot atjaunošanas iemeslus (skat. *IC* kodeksa 7.17. punktu iepriekš 96. punktā). Saskaņā ar *IC* kodeksa 7.18. punktu veica regulārus auditus, kas ietver pārbaudes, lai nodrošinātu, ka ieraksti, ar kuriem tiek pieprasīta piekļuve materiālam, ir apkopoti atbilstoši un ka valsts sekretārs ir apliecinājis pieprasīto materiālu (skat. iepriekš 96. punktu).

389. Turklāt saskaņā ar 7.15. punktu atbilstoši 8. panta 4. punktā noteiktajam orderim apkopoto materiālu var lasīt, aplūkot vai klausīties pilnvarotas personas (analītiķi), kuras ir pabeigušas obligātās mācības par *RIPA* normām un prasībām attiecībā uz nepieciešamību un samērīgumu un kurām ir veikta atbilstoša drošības pārbaude (skat. iepriekš 96. punktu). Saskaņā ar 7.10. punktu katra personāla locekļa drošības pārbaudi periodiski pārskata (skat. iepriekš 96. punktu).

390. *IC* kodeksa 7.6. punkts nosaka, ka pārtverto materiālu var kopēt tikai tiktāl, cik tas ir nepieciešams atļautajiem nolūkiem, un stingri piemērojot “informācijas nepieciešamības” principu, tostarp iesniedzot izrakstus vai kopsavilkumus, ja ar to ir pietiekami, lai apmierinātu lietotāja informācijas nepieciešamību. Saskaņā ar *RIPA* 15. panta 5. punktu ir jābūt ieviestai kārtībai, kādā tiek nodrošināta ikvienas materiāla vai datu kopijas droša uzglabāšana visu tās saglabāšanas laiku (skat. iepriekš 81. punktu), savukārt 7.7. punktā ir noteikts, ka pirms pārtvertā materiāla iznīcināšanas šis materiāls un visas tā kopijas, izraksti un kopsavilkumi ir jāuzglabā droši un tie nevar būt pieejami personām bez nepieciešamā drošības pielaides līmeņa (skat. iepriekš 96. punktu).

391. Ņemot vērā iepriekš minētos trūkumus saistībā ar selektoru apstiprināšanu (skat. iepriekš 381. un 382. punktu) un valsts sekretāra apliecinājuma vispārīgo būtību (skat. iepriekš 386. punktu), Tiesa uzskata, ka apstākļi, kādos pārtverto materiālu varēja atlasīt, pārbaudīt, izmantot un uzglabāt saskaņā ar 8. panta 4. punktā noteikto režīmu, Konvencijas 8. panta izpratnē bija pietiekami “paredzami” un ka tie nodrošināja atbilstošus drošības pasākumus pret ļaunprātīgu izmantošanu.

* 5. Veicamie piesardzības pasākumi, paziņojot materiālu citām pusēm

392. *RIPA* 15. panta 2. punkts noteica, ka turpmāk minētie aspekti ir jāierobežo līdz minimumam, kas nepieciešams “atļautajiem nolūkiem”, proti, to personu skaits, kurām materiālu vai datus izpauda vai darīja pieejamus, apmērs, kādā materiālu vai datus izpauda vai darīja pieejamus, apmērs, kādā materiālu vai datus kopēja, un izgatavoto kopiju skaits (skat. iepriekš 78. punktu). Saskaņā ar 15. panta 4. punktu un *IC* kodeksa 7.2. punktu kaut kas bija nepieciešams atļautajiem nolūkiem vienīgi tad, ja tas joprojām ir vai, visticamāk, kļūs nepieciešams *RIPA* 5. panta 3. punktā minētajiem nolūkiem, lai sekmētu jebkuras valsts sekretāra pārtveršanas funkcijas izpildi, lai sekmētu jebkuras *IC* komisāra vai *IPT* funkcijas izpildi, lai nodrošinātu, ka persona, kas veic kriminālvajāšanu, ir informēta par to, ko tās amata pienākums paredz, lai kriminālvajāšanā nodrošinātu godīgumu (lai gan pašu pārtverto materiālu nevar izmantot kriminālvajāšanā attiecībā uz kādu noziedzīgu nodarījumu, skat. *IC* kodeksa 8.3. punktu iepriekš 96. punktā) vai lai izpildītu jebkuru amata pienākumu, ko personai nosaka publisko reģistru tiesiskais regulējums (skat. iepriekš 80. un 96. punktu).

393. Savukārt *IC* kodeksa 7.3. punkts liedza izpaust informāciju personām, kurām nav veikta atbilstoša drošības pārbaude, kā arī atbilstoši “informācijas nepieciešamības” principam, proti, pārtverto materiālu personai nedrīkstēja izpaust, ja vien šīs personas amata pienākumi, kuriem jābūt saistītiem ar kādu no atļautajiem nolūkiem, nenosaka, ka tai ir “nepieciešama informācija” par pārtverto materiālu, lai veiktu savus amata pienākumus. Tāpat pārtverto materiālu atļauts izpaust vienīgi apmērā, kādā tas saņēmējam ir nepieciešams (skat. iepriekš 96. punktu). 7.3. punkts attiecās gan uz informācijas izpaušanu papildu personām aģentūrā, gan ārpus tās (skat. iepriekš 96. punktu). Saskaņā ar 7.4. punktu minētais attiecās ne tikai uz sākotnējo pārtvērēju, bet arī uz jebkuru personu, kurai pārtverto materiālu pēc tam izpauda (skat. iepriekš 96. punktu).

394. Palāta ir norādījusi, ka, tā kā jēdziens “visticamāk kļūs nepieciešams” nav papildus definēts ne *RIPA*, ne *IC* kodeksā vai kur citur, ar 15. panta 4. punktu un 7.2. punktu iestādēm patiesībā varēja tikt piešķirtas plašas pilnvaras izpaust un kopēt pārtverto materiālu. Tomēr materiālu joprojām varēja izpaust vienīgi personai, kurai veikta atbilstoša drošības pārbaude un kurai “ir nepieciešama informācija”, turklāt tādu pārtvertā materiāla apjomu, kāds personai nepieciešams. Līdz ar to Tiesa piekrīt palātai, ka jēdziena “visticamāk kļūs nepieciešams” iekļaušana nav būtiski mazinājusi drošības pasākumus masveida pārtveršanas ietvaros iegūto datu aizsardzībai (skat. palātas sprieduma 368. un 369. punktu).

395. Pievēršoties pārtvertā materiāla pārsūtīšanai ārpus Apvienotās Karalistes, kad materiāls ir pārtverts atbilstoši valsts tiesību aktiem, Tiesa uzskata, ka šī materiāla pārsūtīšana ārvalstu izlūkošanas partnerim vai starptautiskai organizācijai Konvencijas 8. panta izpratnē būtu problemātiska vienīgi tad, ja pārtveršanas valsts vispirms nav nodrošinājusi, ka tās izlūkošanas partneris, apstrādājot materiālu, ir īstenojis drošības pasākumus, ar kuriem iespējams novērst ļaunprātīgu izmantošanu un nesamērīgu iejaukšanos un jo īpaši var garantēt materiāla drošu uzglabāšanu, kā arī ierobežot tā turpmāku izplatīšanu (skat. iepriekš 362. punktu).

396. Šķiet, ka Apvienotajā Karalistē “Five Eyes” partneri varēja piekļūt *GCHQ* pārtveršanas ordera produkta elementiem savās sistēmās (skat. iepriekš 180. punktu). Šādos gadījumos Apvienotās Karalistes izlūkdienesti materiālu pārtveršanu būtu veikuši saskaņā ar valsts tiesību aktiem, tostarp, ciktāl minētais attiecas uz šo lietu, atbilstoši *RIPA* 8. panta 4. punktam. Saskaņā ar *IC* kodeksa 7.5. punktu tad, kad pārtverto materiālu atklāja ārpus Apvienotās Karalistes esošas valsts vai teritorijas iestādēm, izlūkdienestiem bija jāveic saprātīgi pasākumi, lai nodrošinātu, ka attiecīgās iestādes ir ieviesušas un uzturēs nepieciešamās procedūras, lai aizsargātu pārtverto materiālu un nodrošinātu, ka tas tiek izpausts, kopēts, izplatīts un saglabāts vienīgi nepieciešamajā minimālajā apjomā. Pārtverto materiālu nevarēja tālāk izpaust trešās valsts vai teritorijas iestādēm, ja vien tas nav skaidri saskaņots ar izdevējiestādi, un tas bija jāatdod izdevējiestādei vai droši jāiznīcina, tiklīdz tas vairs nav vajadzīgs (skat. iepriekš 96. punktu). *RIPA* 15. panta 7. punkts arī noteica, ka ir jābūt spēkā ierobežojumiem, kas neļautu veikt nekādas darbības saistībā ar tiesvedību ārpus Apvienotās Karalistes, kuras ietvaros varētu tikt izpausts saturs vai pārtverto sakaru saistītie sakaru dati, ja šāda izpaušana Apvienotajā Karalistē nav bijusi iespējama (skat. iepriekš 82. punktu).

397. Attiecībā uz konfidenciālu materiālu *IC* kodeksa 4.30. punkts noteica, ka tad, kad konfidenciālu informāciju izplatīja kādai ārējai iestādei, bija jāveic saprātīgi pasākumi, lai informāciju atzīmētu kā konfidenciālu. Ja radās šaubas par paredzētās konfidenciālās informācijas izplatīšanas likumību, pirms jebkādas turpmākas materiāla izplatīšanas bija jāvēršas pie attiecīgās pārtveršanas aģentūras juriskonsulta (skat. iepriekš 96. punktu).

398. Līdz ar to bija ieviesti drošības pasākumi, lai nodrošinātu, ka izlūkošanas partneri garantē pārsūtītā materiāla drošu uzglabāšanu un ierobežo tā turpmāku izplatīšanu. Galējais drošības pasākums, kuru Tiesa īpaši uzsver, ir *IC* komisāra un *IPT* nodrošinātā pārraudzība (skat. turpmāk 411. un 414. punktu).

399. Ņemot vērā iepriekš minēto, Tiesa uzskata, ka veicamie piesardzības pasākumi, paziņojot pārtverto materiālu citām pusēm, bija pietiekami skaidri un paredzēja pietiekami stabilas garantijas pret ļaunprātīgu izmantošanu.

* 6. Ierobežojumi attiecībā uz pārtveršanas ilgumu, pārtvertā materiāla uzglabāšanu un apstākļiem, kādos šāds materiāls ir jādzēš vai jāiznīcina

400. Attiecībā uz 8. panta 4. punktā noteiktajiem orderiem, kas izdoti Apvienotās Karalistes valsts drošības vai ekonomiskās labklājības apsvērumu dēļ, ciktāl šīs intereses atbilda valsts drošības interesēm, saskaņā ar *RIPA* 9. pantu šie orderi zaudēja spēku pēc sešiem mēnešiem, ja vien tos neatjaunoja. 8. panta 4. punktā noteiktie orderi, ko izdevis valsts sekretārs smaga nozieguma novēršanas nolūkos, zaudēja spēku pēc trim mēnešiem, ja vien tos neatjaunoja. Šos orderus varēja atjaunot attiecīgi uz sešiem un trim mēnešiem, un tos varēja atjaunot jebkurā brīdī pirms to derīguma termiņa beigām, iesniedzot pieteikumu valsts sekretāram. Šajā pieteikumā bija jāiekļauj tāda pati informācija kā sākotnējā pieteikumā, tostarp pārtveršanas vērtības izvērtējums līdz šim brīdim un paskaidrojums par to, kāpēc ordera atjaunošana bija nepieciešama 5. panta 3. punkta izpratnē un bija samērīga (skat. *RIPA* 9. pantu iepriekš 67. punktā un *IC* kodeksa 6.22.–6.24. punktu iepriekš 96. punktā). Valsts sekretāram bija jāatceļ orderis pat pirms sākotnējā derīguma termiņa beigām, ja bija gūta pārliecība, ka orderis vairs nav nepieciešams, pamatojoties uz 5. panta 3. punktu (skat. *RIPA* 9. pantu iepriekš 67. punktā).

401. Ņemot vērā nepārprotamo ierobežojumu attiecībā uz 8. panta 4. punktā noteikto orderu darbības ilgumu un prasību tos nepārtraukti pārskatīt, Tiesa uzskata, ka noteikumi par pārtveršanas ilgumu 8. panta 4. punktā noteikto režīmu ietvaros bija pietiekami skaidri un nodrošināja atbilstošus drošības pasākumus pret ļaunprātīgu izmantošanu.

402. *IC* kodeksa 7.9. punkts paredzēja, ka tad, kad izlūkdienests saņēma neanalizētu pārtverto materiālu un saistītos sakaru datus 8. panta 4. punktā noteiktā ordera ietvaros, tam bija jānorāda maksimālais glabāšanas periods dažādām materiāla kategorijām, kas atspoguļoja tā veidu un iejaukšanās pakāpi. Šie noteiktie laika periodi parasti nepārsniedza divus gadus, un tie bija jāsaskaņo ar *IC* komisāru. Ciktāl tas iespējams, visu saglabāšanas periodu pamatā bija automātiskas dzēšanas process, ko uzsāka, tiklīdz ir sasniegts piemērojamais maksimālais saglabāšanas periods (skat. iepriekš 96. punktu). Saskaņā ar *IC* kodeksa 7.8. punktu saglabātais pārtvertais materiāls bija jāpārskata atbilstošos intervālos, lai pārliecinātos, ka tā saglabāšanas pamatojums joprojām ir spēkā saskaņā ar *RIPA* 15. panta 3. punktu (skat. iepriekš 96. punktu).

403. Valdība savos argumentos Lielajai palātai sniedza papildu informāciju par saglabāšanas periodiem. Saziņas aktu saturs, kam piemēroja vienīgi “spēcīgo selektoru” procesu, nekavējoties tika atmests, ja vien tas neatbilda spēcīgajam selektoram. Savukārt saziņas aktu saturs, kam piemēroja arī “kompleksā vaicājuma” procesu, tika saglabāts vairākas dienas, lai nodrošinātu procesa norisi, un pēc tam automātiski dzēsts, ja vien tas netika atlasīts pārbaudei. Saziņas aktu saturu, ko atlasīja pārbaudei, varēja saglabāt vienīgi tad, kad tas bija nepieciešami un samērīgi. Standarta nosacījums bija tāds, ka atlasīto saziņas aktu satura saglabāšanas periods nepārsniedz dažus mēnešus, pēc kā saziņas aktu saturu automātiski dzēsa (lai gan tad, kad materiāls bija minēts izlūkošanas ziņojumā, šo ziņojumu saglabāja), taču izņēmuma kārtā varēja uzsākt lietu, lai saglabātu atlasītos sakarus ilgāku laiku (skat. iepriekš 293. punktu). Līdz ar to praksē varētu šķist, ka saglabāšanas periodi ir ievērojami īsāki par maksimālo divu gadu saglabāšanas periodu.

404. Visbeidzot, saskaņā ar *RIPA* 15. panta 3. punktu un *IC* kodeksa 7.8. punktu ikviena pārtvertā materiāla kopija (tostarp tā izraksti un kopsavilkumi) bija jāiznīcina drošā veidā, tiklīdz tā vairs nebija nepieciešami nevienam no 5. panta 3. punktā minētajiem nolūkiem (skat. iepriekš 79. un 96. punktu).

405. Spriedumā lietā “Liberty” *IPT* bija izvērtējusi materiāla saglabāšanas un iznīcināšanas kārtību un to atzinusi par atbilstošu (skat. iepriekš 50. punktu). Tiesa arī uzskata, ka “virs ūdenslīnijas” esošie pasākumi, kas paredz apstākļus, kādos pārtvertais materiāls ir jādzēš vai jāiznīcina, bija pietiekami skaidri. Tomēr tā uzskata, ka būtu bijis vēlams, lai īsākie saglabāšanas periodi, ko Valdība noteica šīs tiesvedības laikā, būtu atspoguļoti atbilstošajos tiesību aktos un/vai citās vispārīgās normās.

* 7. Pārraudzība

406. 8. panta 4. punktā noteiktā režīma pārraudzību galvenokārt īstenoja *IC* komisārs, lai gan, pēc komisāra domām, “kritiski svarīgo kvalitātes nodrošināšanas funkciju sākotnēji [bija] pildījušas pārtveršanas aģentūras vai orderi piešķirošās nodaļas darbinieki un juristi”, kuri sniedza valsts sekretāram neatkarīgu viedokli un pārbaudīja pieteikumus orderu izdošanai un atjaunošanai pirms atļaujas došanas, lai nodrošinātu, ka tie ir (un paliek) nepieciešami un samērīgi (skat. iepriekš 170. punktu).

407. *IC* komisārs bija neatkarīgs no izpildvaras un likumdevēja varas, un viņam bija pirms tam jāieņem augsts tiesneša amats. Viņa galvenais pienākums bija pārbaudīt, kā attiecīgie valsts sekretāri un valsts iestādes īsteno un pilda *RIPA* 1. daļā (un ierobežotā mērā arī 3. daļā) noteiktās pilnvaras, un viņš pārraudzīja pārbaudes režīmu, kas viņam ļāva neatkarīgi pārraudzīt tiesību aktu piemērošanu. Viņš reizi pusgadā ziņoja Ministru prezidentam par savu funkciju izpildi un sagatavoja gada ziņojumu, kas tika iesniegts parlamenta palātām. Turklāt pēc katras pārbaudes pārbaudāmās aģentūras vadītājam tika nosūtīts ziņojums, kurā bija ietverti formāli ieteikumi un kurā aģentūrai bija noteikts pienākums divu mēnešu laikā ziņot, lai apstiprinātu, vai ieteikumi ir īstenoti vai ir panākts progress. Viņa periodiskie ziņojumi ir publicēti no 2002. gada, savukārt no 2013. gada tos publicēja pilnībā bez konfidenciāliem pielikumiem. Turklāt *RIPA* 58. panta 1. punkts paredzēja ar likumu noteiktu pienākumu katrai valsts amatpersonai, kura darbojas kādā *IC* komisāram pakļautā organizācijā, izpaust vai sniegt tam visus dokumentus vai informāciju, kas varētu būt nepieciešama, lai viņš varētu veikt savas funkcijas (skat. iepriekš 135. un 136. punktu).

408. *IC* komisāra 2016. gada ziņojumā ir sniegti pierādījumi par viņa pārraudzības pilnvaru apjomu. Kopumā pārbaužu laikā viņš novērtēja sakaru pārtveršanas sistēmas un pārliecinājās, ka tiek uzturēti visi attiecīgie ieraksti, izskatīja atlasītos pārtveršanas pieteikumus, lai izvērtētu, vai tie atbilst nepieciešamības un samērīguma prasībām, intervēja atbildīgos darbiniekus un analītiķus, lai novērtētu, vai pārtveršana un visa materiāla iegūšanas pamatojums ir samērīgs, izskatīja visus steidzamos mutiskus apstiprinājumus, lai pārbaudītu, vai process ir pamatots un izmantots atbilstoši, pārskatīja tos gadījumus, kad bija pārtverti un saglabāti sakari, uz kuru attiecas advokāta un klienta saziņas konfidencialitāte vai citādi konfidenciāla informācija, un visas lietas, kurās saistībā ar advokātu tika veikta izmeklēšana, pārskatīja drošības pasākumu un kārtības atbilstību saskaņā ar *RIPA* 15. un 16. pantu, izpētīja ieviestās procedūras pārtvertā materiāla un saistīto sakaru datu saglabāšanai, uzglabāšanai un iznīcināšanai, kā arī pārskatīja ziņotās kļūdas un visu ieviesto pasākumu pietiekamību, lai novērstu kļūdu atkārtošanos (skat. iepriekš 171. punktu).

409. 2016. gadā *IC* komisāra birojs vienu reizi pārbaudīja visas deviņas pārtveršanas aģentūras un divas reizes – četras galvenās orderus piešķirošās nodaļas. Tika pārbaudīti kopumā deviņi simti septiņdesmit orderi, kas atbilst sešdesmit vienam procentam no gada beigās spēkā esošo orderu skaita un trīsdesmit diviem procentiem no 2016. gadā izdoto jauno orderu kopskaita (skat. iepriekš 173. un 175. punktu).

410. Pārbaudes parasti notika trīs posmos. Pirmkārt, lai iegūtu orderu reprezentatīvo paraugu, inspektori tos atlasīja, ņemot vērā dažādus noziegumu veidus un draudus valsts drošībai, pievēršot galveno uzmanību tiem īpaši interesējošiem vai sensitīviem aspektiem. Otrkārt, inspektori detalizēti pārbaudīja atlasītos orderus un saistīto dokumentāciju, ar to rūpīgi iepazīstoties pirms pārbaudes veikšanas. Šajā posmā inspektori pārbaudīja analītiķu apgalvojumus par nepieciešamību un samērīgumu, pārbaudes nolūkos pievienojot selektoru datu apkopošanas sistēmai. Katru apgalvojumu analizēja atsevišķi, un tam bija jāatsaucas uz vispārējo prasību par izlūkdatu vākšanas prioritātēm. Treškārt, viņi apzināja tos orderus, darbības vai procesa jomas, kurās bija nepieciešama papildu informācija vai precizējumi, un organizēja attiecīgā operatīvā, juridiskā vai tehniskā personāla intervijas. Ja nepieciešams, viņi pārbaudīja papildu dokumentāciju vai sistēmas saistībā ar šiem orderiem (skat. iepriekš 174. punktu).

411. *IC* komisārs arī pārraudzīja pārtvertā materiāla apmaiņu ar izlūkošanas partneriem. Viņš savā 2016. gada ziņojumā norādīja, ka *GCHQ* sniedza viņa inspektoriem “visaptverošu informāciju par apmaiņas pasākumiem, saskaņā ar kuriem “Five Eyes” partneri savās sistēmās var piekļūt *GCHQ* pārtveršanas ordera produkta elementiem”. Turklāt viņa inspektori arī tikās ar “Five Eyes” kopienas pārstāvjiem, un viņiem tika uzskatāmi parādīts, kā citi “Five Eyes” locekļi var pieprasīt piekļuvi *GCHQ* pārtvertajam materiālam. Viņš arī norādīja, ka “piekļuve *GCHQ* sistēmām bija stingri kontrolēta, un tai bija jābūt pamatotai saskaņā ar uzņēmējas valsts tiesību aktiem un 15./16. pantā noteiktajiem norādījumiem par drošības pasākumiem”. Viņš arī atzīmēja, ka, pirms piekļūt *GCHQ* datiem, “Five Eyes” analītiķiem bija jāpabeidz tādas pašas mācības par juridiskajiem aspektiem kā *GCHQ* darbiniekiem (skat. iepriekš 180. punktu).

412. Ņemot vērā iepriekš minēto, Tiesa ir guvusi pārliecību, ka *IC* komisārs nodrošināja 8. panta 4. punktā noteiktā režīma darbības neatkarīgu un efektīvu pārraudzību. Proti, *IC* komisārs un viņa inspektori varēja izvērtēt nepieciešamību un samērīgumu ievērojami lielam skaitam pieteikumu par ordera izdošanu un attiecībā uz turpmāko selektoru izvēli, kā arī pārbaudīt ieviesto pārtverto sakaru un saistīto sakaru datu saglabāšanas, uzglabāšanas un iznīcināšanas kārtību. Viņi arī varēja sniegt attiecīgo valsts iestāžu vadītājiem formālus ieteikumus, un šīm iestādēm bija divu mēnešu laikā jāsniedz atbilde, lai apstiprinātu, kādā apmērā šie ieteikumi ir īstenoti. Turklāt Valdība savos argumentos Lielajai palātai apstiprināja, ka *GCHQ* regulāri informēja *IC* komisāru par pamatojumu, atbilstoši kuram nesējus atlasīja pārtveršanai (skat. iepriekš 136. un 290. punktu). Izlūkdienestiem bija jāsaglabā ieraksti katrā masveida pārtveršanas procesa posmā, un tiem bija pienākums nodrošināt inspektoriem piekļuvi šiem ierakstiem (skat. *IC* kodeksa 6.27. un 6.28. punktu iepriekš 96. punktā). Visbeidzot viņš arī pārraudzīja pārtvertā materiāla apmaiņu ar izlūkošanas partneriem (skat. iepriekš 180. punktu).

* 8. Ex post facto pārskatīšana

413. *Ex post facto* pārskatīšanu veica *IPT*, kuru attiecīgajā brīdī vadīja Augstās tiesas tiesnesis. Palāta konstatēja un pieteikuma iesniedzēji nav apstrīdējuši, ka *IPT* nodrošina efektīvu tiesiskās aizsardzības līdzekli pieteikuma iesniedzējiem, kuri sūdzas gan par konkrētiem uzraudzības gadījumiem, gan par uzraudzības režīmu vispārējo atbilstību Konvencijai (skat. palātas sprieduma 265. punktu). Šajā sakarā palāta atzina, ka ir svarīgi, lai *IPT* būtu plaša jurisdikcija izskatīt jebkuru sūdzību par prettiesisku pārtveršanu, kas nebija atkarīga no subjekta informēšanas par pārtveršanu (skat. iepriekš 122. punktu). Līdz ar to jebkura persona, kura uzskatīja, ka bija slepeni uzraudzīta, varēja tai iesniegt pieteikumu. Tās locekļiem bija jābūt augstā tiesneša amatā vai kvalificētiem advokātiem ar vismaz desmit gadu darba stāžu (skat. iepriekš 123. punktu). Tiem, kas bija iesaistīti pārtveršanas ordera apstiprināšanā un izpildē, bija tai jāatklāj visi dokumenti, kas tai varētu būt nepieciešami, tostarp “zem ūdenslīnijas” esošie dokumenti, kurus nevarēja publiskot valsts drošības apsvērumu dēļ (skat. iepriekš 125. punktu). Turklāt tai bija rīcības brīvība organizēt mutisku paskaidrojumu uzklausīšanu, ja iespējams, atklāti (skat. iepriekš 129. punktu), savukārt slēgtā tiesvedībā tā varēja lūgt tiesas padomnieku iesniegt pieteikumus to prasītāju vārdā, kurus nebija iespējams pārstāvēt (skat. iepriekš 132. punktu); kad tā izskatīja sūdzības, tai arī bija tiesības piešķirt kompensāciju un izdot jebkuru citu rīkojumu, ko tā uzskatīja par vajadzīgu, tostarp anulēt vai atcelt jebkuru rīkojumu, kā arī pieprasīt jebkuru ierakstu iznīcināšanu (skat. iepriekš 126. punktu). Visbeidzot, tās juridiskos nolēmumus publicēja tās tīmekļa vietnē, tādējādi paaugstinot kontroles līmeni, ko nodrošina slepenajām uzraudzības darbībām Apvienotajā Karalistē (skat. iepriekš minētā sprieduma lietā “Kenedijs” 167. punktu).

414. Turklāt *IPT* varēja izskatīt jebkuru sūdzību par to, vai pārtvertā materiāla pārsūtīšana trešām personām vai pārtvertā materiāla pārsūtīšanu reglamentējošais režīms atbilst Konvencijai. Tomēr šajā lietā pieteikuma iesniedzēji trešajā no apvienotajām lietām valsts tiesvedības gaitā nav iesnieguši nekādu īpašu sūdzību šajā sakarā. Drīzāk viņu sūdzības par izlūkdatu apmaiņu attiecās vienīgi uz režīmu, kas reglamentē izlūkdatu saņemšanu no trešām valstīm (skat. turpmāk 467.–516. punktu).

415. Līdz ar to Tiesa ir guvusi pārliecību, ka *IPT* nodrošināja stabilu tiesiskās aizsardzības līdzekli ikvienai personai, kurai radās aizdomas, ka izlūkdienesti ir pārtvēruši tās sakarus.

γ) Saistītie sakaru dati

416. Tiesa ir norādījusi, ka masveida pārtveršanas kontekstā saistīto sakaru datu pārtveršana, saglabāšana un meklēšana ir jāanalizē, atsaucoties uz tiem pašiem drošības pasākumiem, kas attiecināmi uz saturu, taču saistīto sakaru datu apstrādi reglamentējošajām tiesību normām ne vienmēr jebkurā aspektā ir jābūt identiskām saturu reglamentējošajām tiesību normām (skat. iepriekš 363.–364. punktu). Apvienotajā Karalistē atbilstoši 8. panta 4. punktā noteiktajiem orderiem atļauts pārtvert gan saturu, gan saistītos sakaru datus. Pēdējos no minētajiem vairumā gadījumu apstrādāja atbilstoši 8. panta 4. punktā noteiktajam režīmam. Tādējādi trūkumi, kas jau konstatēti attiecībā uz šo satura pārtveršanas režīmu (skat. iepriekš 377., 381. un 382. punktu), vienlīdz attiecās arī uz saistītajiem sakaru datiem, proti, neatkarīgas atļaujas neesība (skat. iepriekš 377. punktu), selektoru kategoriju nenorādīšana pieteikumā ordera izdošanai (skat. iepriekš 381. un 382. punktu), fakts, ka attiecībā uz selektoriem, kas attiecas uz identificējamām personām, neveic iepriekšēju iekšējo apstiprināšanu un ka nav iespējams paredzēt apstākļus, kādos sakari varētu tikt pārbaudīti (skat. iepriekš 391. punktu), ņemot vērā gan to, ka pieteikumā ordera izdošanai nav norādītas selektoru kategorijas (skat. iepriekš 381. un 382. punktu), gan valsts sekretāra apliecinājuma vispārīgo būtību (skat. iepriekš 386. punktu).

417. Tajā pašā laikā uz sakaru datu apstrādi lielākoties attiecās tie paši drošības pasākumi, ko piemēroja saturam. Tāpat kā attiecībā uz saturu, arī sakaru dati bija pakļauti automatizētam filtrēšanas procesam gandrīz reāllaikā, un ievērojamu to daļu šajā posmā nekavējoties dzēsa, turklāt tiem piemēroja arī vienkāršus vai sarežģītus vaicājumus, lai iegūtu materiālu, kam bija potenciāla izlūkošanas vērtība. Turklāt uz selektoriem, ko izmantoja attiecībā uz saistītajiem sakaru datiem, attiecās tie paši drošības pasākumi, kas uz saturu, proti, analītiķiem bija jāizveido rakstveida ieraksts, paskaidrojot, kādēļ katra jaunā selektora pievienošana sistēmai bija nepieciešama un samērīga; šo ierakstu pārbaudīja *IC* komisārs; selektori bija jādzēš, ja konstatēja, ka tos neizmanto paredzētajam mērķim, turklāt bija noteikts maksimālais laika periods, kurā selektorus varēja izmantot, pirms bija nepieciešama pārskatīšana (skat. iepriekš 298. punktu).

418. Saturam un saistītajiem sakaru datiem arī bija piemērotas daudzas tās pašas glabāšanas, piekļuves, pārbaudes un izmantošanas procedūras, tādi paši piesardzības pasākumi, sazinoties ar trešām personām, kā arī tā pati dzēšanas un iznīcināšanas kārtība. Šajā sakarā gan uz saturu, gan uz saistītajiem sakaru datiem attiecās *RIPA* 15. pantā noteiktie drošības pasākumi, proti, analītiķiem, kuri vēlējās piekļūt saistītajiem sakaru datiem, bija jāizveido pārbaudāms ieraksts, paskaidrojot, kāpēc piekļuve bija nepieciešama un samērīga, turklāt, pamatojoties uz saistītajiem sakaru datiem, nevarēja sagatavot nevienu izlūkošanas ziņojumu, ja vien šie dati nebija pārbaudīti.

419. Tomēr bija divi galvenie veidi, kā masveida pārtveršanas režīma ietvaros saturu un saistītos sakaru datus apstrādāja atšķirīgi, proti, saistītos sakaru datus izslēdza no 16. panta 2. punktā noteiktā drošības pasākuma piemērošanas jomas, kas nozīmē, ka tad, ja analītiķis vēlējās izmantot selektoru, kas attiecas uz personu, par kuru zināms, ka tā pašlaik atrodas Britu salās, nebija nepieciešams, lai valsts sekretārs apliecinātu šā selektora izmantošanu kā nepieciešamu un samērīgu, savukārt saistītos sakaru datus, kas neatbilda nedz spēcīgam selektoram, nedz sarežģītam vaicājumam, neiznīcināja nekavējoties, bet gan uzglabāja uz laiku, kas nepārsniedz dažus mēnešus (skat. iepriekš 296.–298. punktu). Tādēļ Tiesa izvērtēs, vai valsts tiesību aktos ir skaidri noteiktas procedūras, kas jāievēro, atlasot saistītus sakaru datus pārbaudei, un saistīto sakaru datu uzglabāšanas ilguma ierobežojumi.

420. 8. panta 4. punktā noteiktais režīms paredz, ka 16. panta 2. punkts ir galvenais likumā noteiktais drošības pasākums, kas nosaka kārtību, kādā pārtverto materiālu atlasa pārbaudei. Tomēr tas nebija vienīgais drošības pasākums. Kā jau iepriekš norādīts 417. punktā, analītiķiem bija jāpamato visi jaunie selektori, izveidojot rakstveida ierakstu, kurā paskaidrots, kādēļ selektora izvēle bija nepieciešama un samērīga (skat. iepriekš 291.–292. un 298. punktu); analītiķiem, kuri vēlējās pārbaudīt saistītos sakaru datus, bija jāizveido papildu ieraksts, paskaidrojot, kādēļ šāda rīcība bija nepieciešama vai samērīga, īstenojot *GCHQ* likumā noteiktās funkcijas (skat. *IC* kodeksa 6.4. punktu iepriekš 96. punktā), turklāt *IC* komisāram šie ieraksti bija jāpārbauda un jāpārrauga (skat. iepriekš 135.–136. un 381. punktu). Valdība norādīja, ka nebūtu bijis iespējams attiecināt 16. panta 2. punktā noteikto drošības pasākumu uz saistītajiem sakaru datiem, jo tad valsts sekretāram katrā atsevišķā gadījumā būtu jāapliecina, ka attiecīgās personas izraudzīšana par mērķi ir nepieciešama un samērīga. Salīdzinājumā ar saturam piemērotajiem vaicājumiem ievērojami vairāk vaicājumu piemēroja sakaru datiem (pat vairāki tūkstoši vienas nedēļas laikā attiecībā uz personām, par kurām bija zināms vai tika uzskatīts, ka tās atrodas Apvienotajā Karalistē), un daudzos gadījumos šīs personas identitāte nebija zināma. Papildus Valdība norādīja, ka saistīto sakaru datu gadījumā bieži vien liela nozīme ir laikam un ka tad, ja šādu datu meklēšana būtu jāatliek, kamēr nav saņemta atsevišķas iestādes piekrišana, izlūkošanas ziņā būtu nopietni apdraudēta šo datu lietderība (skat. iepriekš 296. punktu).

421. Tiesa atzīst, ka saistītie sakaru dati ir būtisks līdzeklis izlūkdienestiem cīņā pret terorismu un smagiem noziegumiem un ka pastāv apstākļi, kuros būtu gan nepieciešams, gan samērīgi meklēt saistītos sakaru datus par personām, par kurām zināms, ka tās atrodas Apvienotajā Karalistē, kā arī šiem datiem piekļūt. Turklāt, lai gan 16. panta 2. punkts paredz svarīgu drošības pasākumu, kas regulē kārtību, kādā pārtverto materiālu atlasa pārbaudei, ir vērts atzīmēt, ka, izvērtējot režīmu, kas regulē satura masveida pārtveršanu, Tiesa daudz lielāku nozīmi piešķīra tam, vai ir pieejams efektīvs mehānisms, lai nodrošinātu, ka selektorus izvēlas atbilstoši Konvencijas prasībām par nepieciešamību un samērīgumu un ka attiecībā uz šo procesu veic gan iekšējo, gan ārējo pārraudzību. Tāpēc, lai gan Tiesa vēlreiz uzsver iepriekš 381. un 382. punktā paustās bažas par selektoru izvēli un pārraudzību, tā neuzskata, ka saistīto sakaru datu izslēgšanai no 16. panta 2. punkta drošības pasākuma piemērošanas jomas jāpiešķir izšķiroša nozīme kopējā izvērtējumā.

422. Pievēršoties uzglabāšanas ilgumam, Valdība apgalvoja, ka attiecībā uz saistītajiem sakaru datiem “bija jāveic analītiskāks darbs ilgākā laika periodā, lai atklātu “vēl nezināmo””. Lai veiktu šādu atklāšanu, atsevišķas nelielas sakaru datu vienības lika kopā, lai izveidotu veselu “kompozīciju”, tādējādi atklājot draudus; šī atklāšana ietvertu arī tādu vienību pārbaudi, par kurām sākumā uzskatīja, ka tām nav izlūkošanas vērtības. Atmetot neatlasītus sakaru datus nekavējoties vai pat pēc dažām dienām, nebūtu iespējams veikt iepriekš minētās darbības (skat. iepriekš 297. punktu).

423. Ņemot vērā iepriekš minēto un to, ka bija noteikts maksimālais datu saglabāšanas periods, kas nepārsniedza “vairākus mēnešus”, kā arī to, ka atšķirīgā apstrāde bija objektīvi un atbilstoši pamatota, Tiesa varētu pieņemt, ka tiesību normas par saistīto sakaru datu uzglabāšanu bija pietiekami skaidras, lai gan tās pēc būtības atšķīrās no saturu regulējošajām tiesību normām. Tomēr šos datu saglabāšanas periodus izpauda vienīgi šajā Tiesā notiekošajā tiesvedībā. Līdz ar to īsākie saglabāšanas periodi nebija acīmredzami ikvienam, kas lasīja *IC* kodeksu, kā arī *IC* kodeksā nebija norāžu par to, ka saistīto sakaru datu saglabāšanas periodi atšķīrās no tiem, kas attiecas uz saturu. Tiesas ieskatā, lai izpildītu 8. pantā noteikto prasību par “paredzamību”, saglabāšanas periodi, kas atklāti šajā Tiesā notiekošajā tiesvedībā, jāiekļauj atbilstošos tiesību aktos un/vai citās vispārīgās normās.

δ) Secinājums

424. Tiesa atzīst, ka masveida pārtveršana līgumslēdzējām valstīm ir ļoti svarīga, lai apzinātu draudus valsts drošībai. To ir atzinusi Venēcijas komisija (skat. iepriekš 196. punktu), un tā bija arī atbildētājas Valdības, kā arī Francijas un Nīderlandes valdības nostāja, iestājoties lietā kā trešā persona (skat. iepriekš 300. un 303. punktu). Tā secināja arī terorisma tiesiskā regulējuma neatkarīgais pārskatītājs, kurš pēc daudzu slēgto materiālu izpētes secināja, ka masveida pārtveršana ir svarīga pilnvara, pirmkārt, tāpēc, ka teroristu, noziedznieku un naidīgo ārvalstu izlūkdienestu rīcība ir kļuvusi daudz rafinētāka, lai tos nevarētu atklāt ar tradicionāliem līdzekļiem, un, otrkārt, tāpēc, ka globālā interneta iezīmju dēļ maršruts, pa kuru konkrētos sakarus pārraida, ir kļuvis ļoti neparedzams. Lai gan viņš un viņa komanda apsvēra masveida pārtveršanas alternatīvas (tostarp mērķētu pārtveršanu, kā arī cilvēkresursu un komerciālo kiberaizsardzības produktu izmantošanu), taču viņi secināja, ka neviena alternatīva vai alternatīvu kombinācija nebūtu pietiekama, lai aizstātu masveida pārtveršanas pilnvaras (skat. iepriekš 166. punktu).

425. Tomēr Tiesa atgādina, ka pastāv ievērojama iespējamība, ka masveida pārtveršanu var izmantot ļaunprātīgi, tādējādi negatīvi ietekmējot personu tiesības uz privātās dzīves neaizskaramību (skat. iepriekš 347. punktu). Tādēļ Tiesa uzskata, ka tiesiskā valstī, kas skaidri norādīts Konvencijas preambulā un ir 8. panta mērķa un nolūka pamatā (skat. iepriekš minētā sprieduma lietā “Romāns Zaharovs” 228. punktu), 8. panta 4. punktā noteiktais režīms, neraugoties uz tajā noteiktajiem drošības pasākumiem, tostarp dažiem īpaši stabiliem drošības pasākumiem, kā norādīts iepriekš (skat., piemēram, iepriekš 412. un 415. punktu), kopumā neparedz pietiekamus “no gala līdz galam” drošības pasākumus, lai nodrošinātu pietiekamas un efektīvas garantijas pret patvaļu un ļaunprātīgas izmantošanas risku. Tā ir konstatējusi būtiskus trūkumus režīmā, proti, neatkarīgas atļaujas neesību, selektoru kategoriju nenorādīšanu pieteikumā ordera izdošanai un faktu, ka attiecībā uz selektoriem, kas attiecas uz personām, nesniedz iepriekšēju iekšējo atļauju (skat. iepriekš 377.–382. punktu). Šīs nepilnības attiecās ne tikai uz sakaru satura, bet arī uz saistīto sakaru datu pārtveršanu (skat. iepriekš 416. punktu). Lai gan *IC* komisārs nodrošināja neatkarīgu un efektīvu režīma pārraudzību un *IPT* piedāvāja stabilu tiesiskās aizsardzības līdzekli ikvienai personai, kurai bija radušās aizdomas, ka izlūkdienesti ir pārtvēruši tās sakarus, šie svarīgie drošības pasākumi nebija pietiekami, lai līdzsvarotu trūkumus, kas uzsvērti iepriekš 377.–382. punktā.

426. Ņemot vērā iepriekš minētos trūkumus, Tiesa atzīst, ka 8. panta 4. punkts neatbilda “tiesību aktu kvalitātes” prasībai, līdz ar to tas nespēja nodrošināt, ka “iejaukšanās” bijusi “nepieciešama demokrātiskā sabiedrībā”.

427. Tādējādi ir noticis Konvencijas 8. panta pārkāpums.

C. Konvencijas 10. panta iespējamais pārkāpums

428. Pieteikuma iesniedzēji gan otrajā, gan trešajā no apvienotajām lietām saskaņā ar Konvencijas 10. pantu sūdzējās par 8. panta 4. punktā noteikto režīmu, apgalvojot, ka aizsardzība, ko 10. pants paredz priviliģētiem sakariem, viņiem kā žurnālistiem un attiecīgi NVO bija ļoti svarīga. Tomēr, tā kā palāta pasludināja pieteikuma iesniedzēju sūdzību trešajā no apvienotajām lietām par nepieņemamu, jo viņi neizmantoja iekšējos tiesiskās aizsardzības līdzekļus, vienīgi sūdzība saistībā ar 10. pantu attiecībā uz žurnālistiem ir Lielajai palātai nodotās lietas ietvaros.

429. Konvencijas 10. pantā ir noteikts:

“1. Ikvienai personai ir tiesības uz vārda brīvību. Šīs tiesības ietver uzskatu brīvību un brīvību saņemt un izplatīt informāciju vai idejas bez valsts iestāžu iejaukšanās un neatkarīgi no valstu robežām. Šis pants neierobežo valstu tiesības noteikt radioraidījumu, televīzijas raidījumu un kino demonstrēšanas licencēšanas režīmu.

2. Tā kā šo brīvību īstenošana ir saistīta ar pienākumiem un atbildību, tā var tikt pakļauta [to var pakļaut] tādām prasībām, nosacījumiem, ierobežojumiem vai sodiem, kas paredzēti likumā un nepieciešami demokrātiskā sabiedrībā, lai aizsargātu valsts drošības, teritoriālās vienotības vai sabiedriskās drošības intereses, nepieļautu nekārtības vai noziedzīgus nodarījumus, aizsargātu veselību vai tikumību, aizsargātu citu cilvēku cieņu vai tiesības, nepieļautu konfidenciālas informācijas izpaušanu vai lai saglabātu tiesu varas autoritāti un objektivitāti.”

1. Palātas spriedums

430. Palāta konstatēja, ka, tā kā uzraudzības pasākumi saskaņā ar 8. panta 4. punktu nebija vērsti uz žurnālistu novērošanu vai žurnālistu avotu atklāšanu, šādu sakaru pārtveršanu pašu par sevi nevar raksturot kā īpaši būtisku iejaukšanos tiesībās uz vārda brīvību. Tomēr tā uzskatīja, ka iejaukšanās būtu būtiskāka, ja šos sakarus atlasītu pārbaudei. Šādā gadījumā iejaukšanos “pamatotu primāra prasība sabiedrības interesēs” vienīgi tad, ja to papildina pietiekami drošības pasākumi. Jo īpaši valsts tiesību aktos būtu pietiekami skaidri jānosaka apstākļi, kādos šādus sakarus varētu apzināti atlasīt pārbaudei, un būtu jāievieš atbilstoši pasākumi, lai nodrošinātu konfidencialitātes aizsardzību, ja šādi sakari ir izvēlēti pārbaudei apzināti vai kā citādi. Tā kā nebija izstrādāta publiski pieejama kārtība, kas ierobežotu izlūkdienestu iespējas meklēt un pārbaudīt konfidenciālu žurnālistikas materiālu, izņemot tad, kad to pamato primāra prasība sabiedrības interesēs, palāta konstatēja, ka noticis arī Konvencijas 10. panta pārkāpums.

2. Pušu argumenti

a) Pieteikuma iesniedzēji

431. Pieteikuma iesniedzēji otrajā no apvienotajām lietām apgalvoja, ka masveida pārtveršanas režīms bija pretrunā ar 10. pantu, jo liela mēroga pārtveršanai un lielu informācijas datubāzu uzturēšanai bija atturoša ietekme uz žurnālistu saziņas brīvību.

432. Ņemot vērā preses brīvības fundamentālo nozīmi, pieteikuma iesniedzēji norādīja, ka tad, kad notikusi jebkāda iejaukšanās žurnālistikas brīvībā un jo īpaši tiesībās saglabāt avotu konfidencialitāti, ir jābūt pieejamiem tiesiskajiem procesuālajiem drošības pasākumiem, kas ir samērīgi ar attiecīgā principa nozīmīgumu. Jo īpaši jēdziens “saskaņā ar likumu” paredzēja, ka tad, kad ar kādu pasākumu bija iespējams identificēt žurnālistikas avotus vai atklāt žurnālistikas materiālu, bija nepieciešama tiesneša vai citas neatkarīgas un objektīvas lēmējstruktūras atļauja, bija jāveic *ex ante* pārskatīšana un atļauju sniedzošajai iestādei bija jāpiešķir pilnvaras noteikt, vai to “pamato primāra prasība sabiedrības interesēs”, un jo īpaši noteikt, vai ar mazāk ierobežojošu pasākumu nebūtu pietiekami, lai ievērotu primārās sabiedrības intereses (skat. 2010. gada 14. septembra spriedumu lietā Nr. 38224/03 ““Sanoma Uitgevers B.V.” pret Nīderlandi” [*GC*]). 8. panta 4. punktā noteiktais režīms neparedz nevienu no šiem drošības pasākumiem.

b) Valdība

433. Valdība vispirms apgalvoja, ka Tiesas judikatūrā nav normu, kas atbalstītu apgalvojumu, ka stratēģiskā pārraudzības režīma darbībai ir nepieciešama iepriekšēja tiesas (vai neatkarīga) atļauja, jo daži žurnālistikas materiāli var tikt pārtverti šā režīma darbības gaitā. Tiesa drīzāk bija krasi nošķīrusi sakaru un/vai sakaru datu stratēģisko pārraudzību, kas varētu netīši “izpaust” dažus žurnālistikas materiālus, no pasākumiem, kas vērsti uz žurnālistikas materiāliem (skat. iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 151. punktu un pretstatīt iepriekš minētajam spriedumam lietā “Sanoma Uitgevers B.V.” un 2012. gada 22. novembra spriedumam lietā Nr. 39315/06 ““Telegraaf Media Nederland Landelijke Media B.V.” un citi pret Nīderlandi”). Prasībai par iepriekšēju tiesas atļauju masveida pārtveršanas kontekstā nebūtu jēgas, jo tiesnesim varētu vienīgi norādīt, ka pastāv iespēja, ka ordera izpildes rezultātā var tikt pārtverts kāds konfidenciāls žurnālistikas materiāls.

434. Līdz ar to Valdība piekrita palātas secinājumam, ka ir jānodrošina papildu aizsardzība brīdī, kad sakarus atlasa pārbaudei. Tādēļ tā apstiprināja, ka *IC* kodekss tika grozīts, lai tas paredzētu, ka “īpaša uzmanība jāpievērš tādu sakaru pārtveršanai un tāda satura atlasīšanai pārbaudei, kas satur informāciju, attiecībā uz kuru personām var pamatoti nākties ievērot augsta līmeņa konfidencialitāti. Tas attiecas uz gadījumiem, kad saziņas aktu saturs ietver juridiski priviliģētu informāciju, konfidenciālu žurnālistikas materiālu vai kad sakari identificē žurnālista avotu”.

c) Trešā persona, kas iestājusies lietā

i) Francijas valdība

435. Francijas valdība apgalvoja, ka žurnālistu uzraudzība ir pieļaujama saskaņā ar Konvencijas 10. pantu, ja tai ir leģitīms mērķis un tā ir nepieciešama un ja pasākums nav vērsts pret žurnālistiem un viņu avotu identificēšanu. Situāciju, kad žurnālistu sakari tikuši pārtverti nejauši, nevar pielīdzināt situācijai, kad ar valsts iestāžu lēmumu žurnālistiem ir pienākums atklāt savus avotus.

ii) Norvēģijas Karalistes valdība

436. Norvēģijas valdība norādīja, ka 8. pantā atļautā plašā rīcības brīvība attiecībā uz lēmumu ieviest masveida pārtveršanas režīmu loģiski bija piemērota arī tad, kad lēmumu izvērtēja no 10. panta aspekta. Masveida pārtveršanas režīma būtība un mērķis būtu apdraudēti, ja Tiesa lēmumu par tā izveidi pārbaudītu, ņemot vērā apstākli par “pamatošanu ar primāru prasību sabiedrības interesēs” tikai tāpēc vien, ka daži no pārtvertajiem sakariem varētu ietvert saskarsmi ar žurnālistiem.

iii) Apvienoto Nāciju īpašais ziņotājs vārda brīvības jautājumos

437. Īpašais ziņotājs apgalvoja, ka ar uzraudzības pasākumiem notika iejaukšanās tiesībās uz vārda brīvību, līdz ar to tiem jāatbilst *ICCPR* 19. panta 3. punktam, kas nosaka, ka vārda brīvības ierobežojumiem ir jābūt “vienīgi tādiem, ko paredz likums un kas ir nepieciešami”, lai aizsargātu citu cilvēku tiesības un cieņu, valsts drošību, sabiedrisko kārtību vai sabiedrības veselību vai tikumību. Masveida uzraudzības programmas radīja būtiskus izaicinājumus attiecībā uz prasību par pieejamiem tiesību aktiem, kam par iemeslu ir uzraudzības tehnoloģiju sarežģītā darbība, neskaidri juridiskie standarti par sakaru pārtveršanu, kā arī sarežģīti un bieži vien konfidenciāli administratīvie regulējumi. Turklāt pastāvēja nopietnas bažas par samērīgumu saistībā ar iejaukšanos žurnālistu darbā un viņu avotu aizsardzību. Tā kā cilvēktiesību normas paredzēja konfidencialitātei augstu aizsardzības līmeni, ierobežojumi jāpiemēro izņēmuma kārtā un jāīsteno vienīgi tiesu iestādēm, turklāt apiešanu, ko tiesu iestādes nav atļāvušas saskaņā ar skaidriem un šauriem tiesību aktiem, nedrīkst izmantot, lai apdraudētu avotu konfidencialitāti. Šajā sakarā, nosakot konfidenciālu sakaru aizsardzības apmēru, bija jāņem vērā plašā izpratne par jēdzienu “žurnālists” saskaņā ar *ICCPR*.

iv) “Article 19”

438. “Article 19” mudināja Tiesu attiecināt uz NVO tādu pašu aizsardzību, kādu parasti attiecina uz žurnālistiem.

v) Helsinku Cilvēktiesību fonds

439. Helsinku fonds norādīja, ka žurnālistu avotu aizsardzību apdraud ne tikai žurnālistu sakaru satura, bet arī saistīto metadatu uzraudzība, kas pati par sevi ļautu identificēt avotus un ziņotājus. Īpaši problemātiski bija tas, ka konfidenciālu informāciju varēja iegūt bez žurnālistu ziņas vai kontroles, tādējādi liedzot viņiem tiesības atsaukties uz konfidencialitāti un liedzot viņu avotiem iespēju paļauties uz konfidencialitātes garantijām.

vi) Plašsaziņas līdzekļu juristu asociācija (turpmāk tekstā – “MLA”)

440. *MLA* pauda bažas, ka masveida uzraudzības režīmi varēja pārtvert žurnālistikas sakarus un sakaru datus, kas varētu identificēt avotus. Tās ieskatā žurnālistikas materiāla pārtveršana vien varētu pārkāpt Konvencijas 10. pantu, pat ja šo materiālu faktiski neanalizētu. Tāpēc ir ļoti svarīgi ieviest atbilstošus drošības pasākumus, lai aizsargātu žurnālistikas avotu konfidencialitāti neatkarīgi no informācijas apkopošanas nolūka. Turklāt režīms, kas ļauj valstīm pārtvert žurnālistu sakarus bez iepriekšējas tiesas atļaujas, visticamāk, ietekmēs žurnālistiku, kas ir sabiedrības interesēs, jo šādu sižetu būtība nozīmēja, ka valsts būtu īpaši ieinteresēta avotu identificēšanā. Risks būtu vēl jo nopietnāks tad, ja avots ir valdības trauksmes cēlējs. Nozīmīga bija atturošā ietekme, ko rada iespējamība, ka šie avoti tiks identificēti. Līdz ar to *MLA* apgalvoja, ka vismaz 10. pants paredz iepriekšēju neatkarīgu tiesas pārraudzību attiecībā uz jebkuru mēģinājumu iegūt žurnālistikas materiālu vai identificēt žurnālistikas avotus un ka tiesas process ir *inter partes*.

vii) Nacionālā Žurnālistu biedrība (turpmāk tekstā – “NUJ”) un Starptautiskā Žurnālistu federācija (turpmāk tekstā – “IFJ”)

441. *NUJ* un *IFJ* apgalvoja, ka avotu konfidencialitāte ir neatņemams preses brīvības elements. Tās arī pauda bažas par iespējamu Apvienotās Karalistes saglabāto datu kopīgošanu ar citām valstīm. Ja konfidenciālu žurnālistikas materiālu kopīgotu ar valsti, kurai drošas apstrādes ziņā nevar uzticēties, tas varētu nonākt tādu cilvēku rokās, kas kaitētu žurnālistam(-ei) vai viņa(-as) avotam. Puses, kas iestājušās lietā, uzskatīja, ka drošības pasākumi atjauninātajā *IC* kodeksā un Sakaru datu iegūšanas prakses kodeksā nebija atbilstoši, jo īpaši tad, kad žurnālists(-e) vai viņa(-as) avota identificēšana nebija uzraudzības pasākuma mērķis.

3. Tiesas vērtējums

a) Žurnālistikas avotu aizsardzības galvenie principi

442. Tā kā vārda brīvība ir viens no būtiskākajiem demokrātiskas sabiedrības pamatiem, Tiesa Konvencijas 10. pantā minētajos gadījumos vienmēr ir rūpīgi izvērtējusi drošības pasākumus saistībā ar brīvību. Uz presi attiecināmajiem drošības pasākumiem ir īpaša nozīme, un žurnālistikas avotu aizsardzība ir viens no preses brīvības stūrakmeņiem. Bez šādas aizsardzības avoti var atturēties sniegt palīdzību presei, kad tā informē sabiedrību par sabiedrības interesēs esošiem jautājumiem. Līdz ar to var tikt apdraudēta preses svarīgā sabiedrības “sargsuņa” loma un negatīvi ietekmēta preses spēja sniegt precīzu un uzticamu informāciju (skat. *inter alia* 1996. gada 27. marta sprieduma lietā Nr. 17488/90 “Gudvina [*Goodwin*] pret Apvienoto Karalisti” 39. punktu, iepriekš minētā sprieduma lietā “Sanoma Uitgevers B.V.” 50. punktu, kā arī iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 143. punktu).

443. Rīkojumi atklāt avotus var negatīvi ietekmēt ne tikai avotu, kura identitāte var tikt atklāta, bet arī laikrakstu vai citu izdevumu, pret kuru rīkojums ir vērsts un kura reputācija šādas informācijas izpaušanas dēļ var tikt negatīvi ietekmēta turpmāko potenciālo avotu acīs, kā arī sabiedrības locekļus, kuri ir ieinteresēti saņemt no anonīmiem avotiem iegūto informāciju. Tomēr pastāv “būtiska atšķirība” starp iestādēm, kas uzliek žurnālistam par pienākumu atklāt viņa avotu identitāti, un iestādēm, kas veic kratīšanu žurnālista mājās un darba vietā, lai atklātu viņa avotus (sal. ar iepriekš minētā sprieduma lietā “Gudvina” 39. punktu un ar sprieduma lietā Nr. 51772/99 “Rēmens [*Roemen*] un Šmita [*Schmit*] pret Luksemburgu” 57. punktu, ECT 2003-IV). Pēdējais no minētajiem, pat ja šāda rīcība nav sniegusi rezultātus, ir drastiskāks pasākums nekā rīkojums izpaust avota identitāti, jo izmeklētājiem, kuri veic kratīšanu žurnālista darba vietā, ir piekļuve visiem žurnālista rīcībā esošajiem dokumentiem (skat. iepriekš minētā sprieduma lietā “Rēmens un Šmita” 57. punktu).

444. Iejaukšanās tiesībās uz žurnālistikas avotu aizsardzību nevar atbilst Konvencijas 10. pantam, ja vien to nepamato kāda absolūta prasība sabiedrības interesēs (skat. iepriekš minētā sprieduma lietā “Sanoma Uitgevers B.V.” 51. punktu, iepriekš minētā sprieduma lietā “Gudvina” 39. punktu, iepriekš minētā sprieduma lietā “Rēmens un Šmita” 46. punktu, kā arī 2007. gada 22. novembra sprieduma lietā Nr. 64752/01 “Voskuils [*Voskuil*] pret Nīderlandi” 65. punktu). Turklāt jebkura iejaukšanās tiesībās uz žurnālistikas avotu aizsardzību ir jāveic, paredzot juridiskus procesuālus drošības pasākumus, kas ir samērīgi ar attiecīgā principa nozīmīgumu (skat. iepriekš minētā sprieduma lietā “Sanoma Uitgevers B.V.” 88.–89. punktu). Vissvarīgākā šo drošības pasākumu kontekstā ir garantija, ka pārskatīšanu veiks tiesnesis vai kāda neatkarīga un objektīva lēmējstruktūra, kas ir pilnvarota noteikt, vai pirms šāda materiāla nodošanas sabiedrības interesēs pastāv prasība, kas ir svarīgāka par žurnālistikas avotu aizsardzības principu, un nepieļaut nevajadzīgu piekļuvi informācijai, kas var atklāt avotu identitāti, ja minētā prasība tāda nav (skat. iepriekš minētā sprieduma lietā “Sanoma Uitgevers B.V.” 88.–90. punktu).

445. Ņemot vērā šādas pārskatīšanas preventīvo veidu, tiesnesim vai citai neatkarīgai un objektīvai struktūrai ir jāspēj izvērtēt šos potenciālos riskus un attiecīgās intereses pirms jebkādas informācijas izpaušanas, atsaucoties uz materiāliem, kurus tā vēlas atklāt, lai var atbilstoši izvērtēt iestāžu argumentus, pamatojoties uz kuriem tās vēlas izpaust informāciju. Uz pieņemamo lēmumu jāattiecina skaidri kritēriji, tostarp izvērtējot, vai ar mazāk ierobežojošu pasākumu var būt pietiekami, lai ievērotu primārās sabiedrības intereses. Tiesnesim vai citai iestādei jābūt iespējai atteikties izdot rīkojumu par informācijas izpaušanu vai izdot ierobežotu vai kvalificētu rīkojumu, lai aizsargātu avotus no atklāšanas neatkarīgi no tā, vai tie ir konkrēti norādīti iegūtajā materiālā, pamatojoties uz to, ka šāda materiāla paziņošana rada nopietnu risku apdraudēt žurnālistu avotu identitāti (skat. iepriekš minētā sprieduma lietā “Sanoma Uitgevers B.V.” 92. punktu, kā arī lēmumu ““Nordisk Film & TV A/S” pret Dāniju” (lēmums), Nr. 40485/02, ECT 2005-XIII). Steidzamās situācijās jābūt ieviestai procedūrai, lai identificētu un izolētu informāciju, ar kuru varētu identificēt avotus, no informācijas, kas nerada šādu risku, pirms iestādes izmanto šo materiālu (skat. *mutatis mutandis* sprieduma lietā Nr. 74336/01 “Vīzers [*Wieser*] un “Bicos Beteiligungen GmbH” pret Austriju” 62.–66. punktu, ECT 2007-XI).

b) 10. pants masveida sakaru pārtveršanas kontekstā

446. Spriedumā lietā “Vēbere un Sarāvija” Tiesa atzina, ka “stratēģiskās pārraudzības” režīms ir iejaucies pirmās pieteikuma iesniedzējas kā žurnālistes tiesībās uz vārda brīvību. Tomēr tā uzskatīja par izšķirošu, ka uzraudzības pasākumi nebija vērsti uz žurnālistu pārraudzību vai žurnālistu avotu atklāšanu. Tādējādi tā konstatēja, ka iejaukšanos pirmās pieteikuma iesniedzējas tiesībās uz vārda brīvību nevar kvalificēt kā īpaši būtisku, un, ņemot vērā ar to saistītos drošības pasākumus, tā atzina viņas sūdzības par nepieņemamām kā acīmredzami nepamatotām (skat. iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 143.–145. un 151. punktu).

c) Šajā lietā izmantojamā pieeja

447. Saskaņā ar 8. panta 4. punktā noteikto režīmu izlūkdienesti varēja piekļūt konfidenciālam žurnālistikas materiālam vai nu apzināti, tieši izmantojot selektorus vai meklēšanas vārdus, kas saistīti ar žurnālistu vai ziņu organizāciju, vai arī netīši – kā masveida pārtveršanas operācijas “piezveju”.

448. Ja izlūkdienestu nolūks ir piekļūt konfidenciālam žurnālistikas materiālam, piemēram, apzināti izmantojot kādu spēcīgu selektoru, kas saistīts ar žurnālistu, vai ja šāda spēcīga selektora izvēles rezultātā pastāv liela varbūtība, ka šādu materiālu atlasīs pārbaudei, Tiesa uzskata, ka iejaukšanās būs samērīga ar kratīšanu žurnālista mājās vai darba vietā; neatkarīgi no tā, vai izlūkdienestu nolūks ir identificēt avotu, izmantot ar žurnālistu saistītus selektorus vai meklēšanas vārdus, visticamāk, tiktu iegūts liels konfidenciāla žurnālistikas materiāla apjoms, kas varētu apdraudēt avotu aizsardzību vēl vairāk nekā rīkojums atklāt avotu (skat. iepriekš minētā sprieduma lietā “Rēmens un Šmita” 57. punktu). Līdz ar to Tiesa uzskata, ka, pirms izlūkdienesti izmanto selektorus vai meklēšanas vārdus, par kuriem zināms, ka tie ir saistīti ar žurnālistu, vai ar kuriem konfidenciālo žurnālistikas materiālu, visticamāk, atlasītu pārbaudei, selektoru vai meklēšanas vārdu izmantošanai ir jāsaņem tiesneša vai kādas tādas neatkarīgas un objektīvas lēmējstruktūras atļauja, kas ir pilnvarota noteikt, vai to “pamato primāra prasība sabiedrības interesēs”, un jo īpaši noteikt, vai ar mazāk ierobežojošu pasākumu nebūtu pietiekami, lai ievērotu primārās sabiedrības intereses (skat. iepriekš minētā sprieduma lietā “Sanoma Uitgevers B.V.” 90.–92. punktu).

449. Pat ja nav nolūka piekļūt konfidenciālam žurnālistikas materiālam un izmantotie selektori un meklēšanas vārdi nav tādi, ar kuriem konfidenciālo žurnālistikas materiālu, visticamāk, atlasītu pārbaudei, tomēr pastāv risks, ka šādu materiālu var pārtvert un pat pārbaudīt kā masveida pārtveršanas operācijas “piezveju”. Tiesas ieskatā šī situācija būtiski atšķiras no mērķētas žurnālista uzraudzības, īstenojot 8. panta 1. punktā vai 8. panta 4. punktā noteiktos režīmus. Tā kā jebkāda žurnālistikas sakaru pārtveršana būtu netīša, iejaukšanās apmēru tiesībās uz žurnālistikas sakaru un/vai avotu aizsardzību sākotnēji nevar paredzēt. Līdz ar to tiesnesis vai cita neatkarīga struktūra atļaujas izsniegšanas posmā nevarētu izvērtēt, vai šādu iejaukšanos “pamato primāra prasība sabiedrības interesēs” un, jo īpaši izvērtēt, vai ar mazāk ierobežojošu pasākumu nebūtu pietiekami, lai ievērotu primārās sabiedrības intereses.

450. Spriedumā lietā “Vēbere un Sarāvija” Tiesa uzskatīja, ka stratēģiskās pārraudzības radīto iejaukšanos tiesībās uz vārda brīvību nevar kvalificēt kā īpaši būtisku, jo tā nebija vērsta uz žurnālistu novērošanu, un iestādes uzzinātu par žurnālista sakaru pārraudzību vienīgi pārtverto telesakaru pārbaudes brīdī vai pat par to neuzzinātu vispār (skat. iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 151. punktu). Tāpēc tā atzina, ka sākotnējā pārtveršana, nepārbaudot pārtverto materiālu, neradīja būtisku iejaukšanos Konvencijas 10. pantā. Tomēr, kā Tiesa jau ir norādījusi, pašreizējā, aizvien digitālākā laikmetā tehnoloģisko iespēju attīstības gaitā ir būtiski palielinājies to sakaru apjoms, kas tiek pārraidīti globālajā internetā, līdz ar to uzraudzība, kas nav tieši vērsta uz personām, var būt ļoti tālejoša gan novērošanas valsts teritorijā, gan ārpus tās (skat. iepriekš 322.–323. punktu). Tā kā, analītiķim pārbaudot žurnālista sakarus vai saistītos sakaru datus, iespējams, varētu tikt identificēts avots, Tiesa uzskata, ka valsts tiesību aktos ir obligāti jāiekļauj stabili drošības pasākumi attiecībā uz šāda konfidenciāla materiāla uzglabāšanu, pārbaudi, izmantošanu, tālāku pārsūtīšanu un iznīcināšanu. Turklāt, pat ja žurnālistikas sakari vai saistītie sakaru dati netiek atlasīti pārbaudei, apzināti izmantojot selektoru vai meklēšanas vārdu, par kuru zināms, ka tas ir saistīts ar žurnālistu, ja un kad kļūst acīmredzams, ka sakari vai saistītie sakaru dati satur konfidenciālu žurnālistikas materiālu, ir jānodrošina, ka analītiķis tos var turpināt uzglabāt un pārbaudīt vienīgi pēc tam, kad ir saņemta atļauja no tiesneša vai kādas citas neatkarīgas un objektīvas lēmējstruktūras, kas ir pilnvarota noteikt, vai turpmāku uzglabāšanu un pārbaudi “pamato primāra prasība sabiedrības interesēs”.

d) Iepriekš minēto kritēriju piemērošana aplūkojamās lietas faktiem

451. Spriedumā lietā “Vēbere un Sarāvija” Tiesa skaidri atzina, ka ar apstrīdēto uzraudzības režīmu bija notikusi iejaukšanās pirmās pieteikuma iesniedzējas kā žurnālistes tiesībās uz vārda brīvību (skat. iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 143.–145. punktu). Šajā lietā Tiesa ir atzinusi, ka ar 8. panta 4. punktā noteiktā režīma darbību notikusi iejaukšanās visās pieteikuma iesniedzēju tiesībās, kas paredzētas Konvencijas 8. pantā (skat. iepriekš 324.–331. punktu). Tā kā pieteikuma iesniedzēji otrajā no apvienotajām lietām bija attiecīgi ziņu vākšanas organizācija un žurnālists, Tiesa varētu pieņemt, ka ar 8. panta 4. punktā noteiktā režīma darbību notikusi iejaukšanās viņu kā žurnālistu tiesībās uz vārda brīvību, kas paredzētas Konvencijas 10. pantā.

452. Kā jau minēts, 8. panta 4. punktā noteiktais režīms ir skaidri reglamentēts valsts tiesību aktos (skat. iepriekš 365. un 366. punktu). Tomēr, izvērtējot paredzamību un nepieciešamību saskaņā ar Konvencijas 8. pantu, Tiesa režīmā un ar to saistītajos drošības pasākumos konstatēja tādus trūkumus kā neatkarīgas atļaujas neesība (skat. iepriekš 377. punktu), selektoru kategoriju nenorādīšana pieteikumā ordera izdošanai (skat. iepriekš 381.–382. punktu) un fakts, ka attiecībā uz selektoriem, kas attiecas uz identificējamu personu, neizsniedz iepriekšēju iekšējo atļauju (skat. iepriekš 382. punktu).

453. Tomēr daži papildu drošības pasākumi attiecībā uz konfidenciālu žurnālistikas materiālu bija noteikti *IC* kodeksa 4.1.–4.3. un 4.26.–4.31. punktā (skat. iepriekš 96. punktu). Saskaņā ar 4.1. punktu jebkurā pieteikumā ordera izdošanai bija jānorāda, vai pārtveršana varētu radīt netiešu iejaukšanos tiesībās uz privātās dzīves neaizskaramību, tostarp gadījumos, kas attiecas uz žurnālistikas sakariem, un, ja iespējams, bija jāprecizē veicamie pasākumi, lai samazinātu netiešās iejaukšanās apmēru. Tomēr saskaņā ar 4.1. punktu valsts sekretāram bija vien jāņem vērā šie apstākļi un pasākumi, izvērtējot pieteikumu 8. panta 1. punktā ordera, proti, mērķētas pārtveršanas ordera, izdošanai. Turklāt 4.2. punkts noteica, ka “īpaša uzmanība jāpievērš arī” gadījumos, kas attiecas uz konfidenciālu žurnālistikas materiālu, savukārt 4.26. punkts paredzēja, ka “īpaša uzmanība” ir jāpievērš tādu sakaru pārtveršanai, kas ietver konfidenciālu žurnālistikas materiālu.

454. Valdība apgalvoja, ka 4.28. punkts attiecas arī uz konfidenciālu žurnālistikas materiālu. Ja nolūks bija iegūt konfidenciālus *personas* datus, 4.28. punktā norādīts, ka ir skaidri jādokumentē šādas rīcības iemesli, kā arī īpašā nepieciešamība un samērīgums. Ja šāda materiāla iegūšana bija iespējama, bet nebija paredzēta, bija jāizvērtē visi iespējamie seku mazināšanas pasākumi un, ja tādi nebija pieejami, jāapsver, vai pārtveršanas aģentūrā ir jāievieš īpaši apstrādes pasākumi (skat. iepriekš 96. punktu). Tiesa tomēr atzīmē, ka *IC* kodeksa 4.26. punktā jēdziens “konfidenciāli personas dati”, šķiet, atšķiras no jēdziena “konfidenciāls žurnālistikas materiāls” (skat. iepriekš 96. punktu).

455. Attiecībā uz konfidenciāla materiāla uzglabāšanu *IC* kodeksa 4.29. punkts noteica, ka šādu materiālu var saglabāt vienīgi tad, ja šāda rīcība ir nepieciešama un samērīga ar kādu no *RIPA* 15. panta 4. punktā atļautajiem nolūkiem, turklāt tas ir droši jāiznīcina, kad tas vairs nav nepieciešams kādam no šiem nolūkiem (skat. iepriekš 96. punktu). Turklāt saskaņā ar 4.30. punktu, ja materiālu saglabā vai izplata kādai ārējai struktūrai, ir jāveic saprātīgi pasākumi, lai informāciju atzīmētu kā konfidenciālu. Ja radās šaubas par paredzētās konfidenciālās informācijas izplatīšanas likumību, pirms jebkādas turpmākas materiāla izplatīšanas bija jāvēršas pie attiecīgās pārtveršanas aģentūras juriskonsulta (skat. iepriekš 96. punktu). Visbeidzot saskaņā ar 4.31. punktu *IC* komisārs ir jāinformē par šāda materiāla saglabāšanu, tiklīdz tas praktiski iespējams, un šim materiālam viņam ir jābūt pieejamam pēc pieprasījuma (skat. iepriekš 96. punktu).

456. Ņemot vērā iepriekš minēto, Tiesa varētu pieņemt, ka *IC* kodeksā paredzētie drošības pasākumi attiecībā uz konfidenciāla žurnālistikas materiāla uzglabāšanu, tālāku pārsūtīšanu un iznīcināšanu bija atbilstoši. Tomēr ar *IC* kodeksā noteiktajiem papildu drošības pasākumiem nav novērstas nepilnības, ko Tiesa konstatēja, izvērtējot režīmu saskaņā ar Konvencijas 8. pantu, kā arī tie neatbilda Tiesas noteiktajām prasībām iepriekš 448.–450. punktā. Proti, nebija noteikta prasība, saskaņā ar kuru selektorus vai meklēšanas vārdus, par kuriem zināms, ka tie ir saistīti ar žurnālistu, varētu izmantot vienīgi tad, ja saņemta tiesneša vai kādas tādas neatkarīgas un objektīvas lēmējstruktūras atļauja, kas ir pilnvarota noteikt, vai to “pamato primāra prasība sabiedrības interesēs” un vai ar mazāk ierobežojošu pasākumu nebūtu bijis pietiekami, lai ievērotu primārās sabiedrības intereses. Gluži pretēji, ja nolūks bija piekļūt konfidenciālam žurnālistikas materiālam vai tas bija ļoti iespējams, ņemot vērā ar žurnālistu saistītu selektoru izmantošanu, bija vienīgi skaidri jānorāda šādas rīcības iemesli, nepieciešamība un samērīgums.

457. Turklāt nebija ieviesti pietiekami drošības pasākumi, lai nodrošinātu, ka, tiklīdz kļūst skaidrs, ka sakari, kas nav atlasīti pārbaudei, apzināti izmantojot selektoru vai meklēšanas vārdu, par kuru zināms, ka tas ir saistīts ar žurnālistu, tomēr satur konfidenciālu žurnālistikas materiālu, analītiķis to turpina glabāt un pārbaudīt vienīgi tad, ja to ir atļāvis tiesnesis vai cita neatkarīga un objektīva lēmējstruktūra, kas ir pilnvarota noteikt, vai turpmāko saglabāšanu un pārbaudi “pamato primāra prasība sabiedrības interesēs”. Tā vietā *IC* kodeksa 4.2. punkts noteica vienīgi to, ka ir jāpievērš “īpaša uzmanība” jebkurai pārtveršanai, kas varētu būt saistīta ar konfidenciāla žurnālistikas materiāla pārtveršanu, tostarp jāapsver jebkuri iespējamie sekas mazinošie pasākumi (skat. iepriekš 96. punktu).

458. Ņemot vērā abus šos trūkumus un tos, ko konstatējusi Tiesa, izskatot sūdzību saskaņā ar Konvencijas 8. pantu, tā konstatē, ka 8. panta 4. punktā noteiktā režīma darbības rezultātā ir noticis arī Konvencijas 10. panta pārkāpums.

III. IZLŪKDATU SAŅEMŠANA NO ĀRVALSTU IZLŪKDIENESTIEM

A. Konvencijas 8. pants

459. Pirmajā no apvienotajām lietām pieteikuma iesniedzēji izvirzīja sūdzību par to, ka Apvienotās Karalistes iestādes saņēma materiālu no ārvalstu izlūkdienestiem. Savukārt trešajā no apvienotajām lietām pieteikuma iesniedzēji izvirzīja konkrētāku sūdzību, apgalvojot, ka atbildētāja valsts saņēma *NSA* pārtverto materiālu, izmantojot programmas “PRISM” un “Upstream”, tādējādi pārkāpjot viņu tiesības, kas paredzētas Konvencijas 8. pantā.

1. Lielajā palātā izskatītās sūdzības būtība

460. “Liberty” tiesvedībā *IPT* norādīja trīs no ārvalstu izlūkošanas partneriem saņemamā materiāla kategorijas: nepieprasītais pārtvertais materiāls, pieprasītais pārtvertais materiāls un nepārtvertais materiāls. Tā kā Valdība informēja palātu, ka pārtvertā materiāla “nepieprasīta” iegūšana bija “maz ticama un reta”, palāta neizvērtēja šajā kategorijā ietilpstošo materiālu (skat. palātas sprieduma 417. punktu). Palāta arī atteicās izvērtēt nepārtvertā materiāla saņemšanu, jo pieteikuma iesniedzēji nebija precizējuši, kādu materiālu ārvalstu izlūkdienesti varētu iegūt ar citām metodēm, izņemot pārtveršanu, un tādēļ tā neuzskatīja, ka pieteikuma iesniedzēji bija pierādījuši, ka ar šā materiāla iegūšanu būtu aizskartas viņu tiesības, kas paredzētas 8. pantā (skat. palātas sprieduma 449. punktu). Pieteikuma iesniedzēji šos secinājumus nav apstrīdējuši.

461. Turklāt, tā kā “Liberty” tiesvedību ierosināja pieteikuma iesniedzēji trešajā no apvienotajām lietām, *IPT* izvērtēja vienīgi no *NSA* saņemtos izlūkdatus. Arī palātā un Lielajā palātā lietas dalībnieki savos argumentos atsaucās uz materiālu, kas saņemts no *NSA*.

462. Tādēļ Lielā palāta izvērtēs sūdzību vienīgi tiktāl, ciktāl tā attiecas uz pieprasīta pārtverta materiāla saņemšanu no *NSA*.

2. Valdības sākotnējais iebildums

463. Valdība apgalvoja, ka pieteikuma iesniedzēji pirmajā un trešajā no apvienotajām lietām nevarēja apgalvot, ka ir cietuši no iespējamā pārkāpuma, jo viņi neatbilda nevienam no diviem spriedumā lietā “Romāns Zaharovs” (minēts iepriekš 171. punktā) izvirzītajiem nosacījumiem (proti, pieteikuma iesniedzējus nevarēja ietekmēt tiesiskais regulējums, kas pieļauj slepenās uzraudzības pasākumus, un valsts līmenī bija pieejami tiesiskās aizsardzības līdzekļi). Proti, tā apgalvoja, ka pieteikuma iesniedzēji nav minējuši tos iemeslus, kas viņiem radīja reālu risku, ka ar programmām “PRISM” vai “Upstream” pārtvers viņu saziņas aktu saturu vai to pieprasīs Apvienotās Karalistes izlūkdienesti. Turklāt tā norādīja, ka pieteikuma iesniedzējiem bija pieejami efektīvi iekšējie tiesiskās aizsardzības līdzekļi, lai noskaidrotu, vai attiecībā uz viņiem notikusi pretlikumīga izlūkdatu apmaiņa.

a) Palātas spriedums

464. Tā kā palāta atzina, ka *IPT* bija nodrošinājusi pieteikuma iesniedzējiem efektīvu tiesiskās aizsardzības līdzekli attiecībā uz sūdzību, ko viņi bija iesnieguši saskaņā ar Konvenciju, tā uzskatīja, ka viņi varēja apgalvot, ka ir “cietušie” tikai izlūkdatu apmaiņas režīma pastāvēšanas dēļ, vienīgi tad, ja viņi varēja pierādīt, ka, iespējams, bija pakļauti riskam, ka Apvienotās Karalistes iestādes varēja iegūt viņu saziņas aktu saturu, to pieprasot no ārvalstu izlūkdienesta (skat. palātas sprieduma 392.–393. punktu saistībā ar iepriekš minētā spriedumā lietā “Romāns Zaharovs” 171. punktu).

465. Pamatojoties uz tai sniegto informāciju, tā atzina, ka pieteikuma iesniedzēji, iespējams, bija pakļauti gan riskam, ka viņu saziņas aktu saturu iegūs ārvalstu izlūkdienests, gan arī riskam, ka Apvienotās Karalistes iestādes to pieprasīs no ārvalstu izlūkdienesta (skat. palātas sprieduma 395. punktu). Lai arī viņu saziņas aktu saturu varēja pieprasīt, vienīgi pamatojoties uz 8. panta 1. vai 4. punktā noteikto orderi, kas attiecās uz pieteikuma iesniedzēju saziņas aktu saturu, no “Liberty” tiesvedības skaidri izrietēja, ka Apvienotās Karalistes izlūkdienesti atbilstoši 8. panta 4. punktā noteiktajam režīmam bija likumīgi pārtvēruši un atlasījuši pārbaudei saziņas aktu saturu, kas attiecās uz vismaz diviem pieteikuma iesniedzējiem trešajā no apvienotajām lietām. Lai gan palātai nebija iemesla uzskatīt, ka izlūkdienestu darbības bija tieši vērstas uz šiem pieteikuma iesniedzējiem, tā norādīja, ka viņu saziņas aktu saturu varēja likumīgi iegūt saskaņā ar 8. panta 4. punktā noteikto režīmu tad, ja viņi, kā paši apgalvoja, sazinājās ar personām, uz kurām šādas darbības bija vērstas. Tāpat viņu saziņas aktu saturu varēja likumīgi pieprasīt no trešās valsts atbilstoši izlūkdatu apmaiņas režīmam, ja viņi sazinājās ar kādu personu, attiecībā uz kuru iesniegts pieprasījums.

466. Tā kā programma “Upstream” darbojās līdzīgi kā 8. panta 4. punktā noteiktais režīms, palāta arī atzina, ka pieteikuma iesniedzēju saziņas aktu saturu, iespējams, varēja iegūt *NSA*.

b) Tiesas vērtējums

467. Pieteikuma iesniedzēji nav apstrīdējuši palātas secinājumu, ka *IPT* nodrošināja efektīvu valsts līmeņa tiesiskās aizsardzības līdzekli attiecībā uz sūdzībām par uzraudzības režīma darbību, kas iesniegtas saskaņā ar Konvenciju, tādēļ, pamatojoties uz iepriekš 413.–415. punktā izklāstītajiem iemesliem, Lielā palāta piekrīt šim secinājumam. Tādēļ, kā palāta norādīja, pieteikuma iesniedzēji varēja apgalvot, ka ir “cietušie” tikai izlūkdatu apmaiņas režīma pastāvēšanas dēļ, vienīgi tad, ja viņi varēja pierādīt, ka, iespējams, bija pakļauti riskam, ka Apvienotās Karalistes iestādes varēja iegūt viņu saziņas aktu saturu, to pieprasot no ārvalstu izlūkdienesta (skat. iepriekš minētā spriedumā lietā “Romāns Zaharovs” 171. punktu). Tas tā būtu vienīgi tad, ja viņi patiešām būtu pakļauti gan riskam, ka ārvalstu izlūkdienesti varēja pārtvert viņu saziņas aktu saturu, gan riskam, ka to bija pieprasījusi *GCHQ*.

468. Pievēršot uzmanību izlūkdatu saņemšanai no Amerikas Savienotajām Valstīm, Valdība apgalvoja, ka pieteikuma iesniedzēji nebija potenciāli pakļauti riskam, ka viņu saziņas aktu saturu varēja pārtvert ar programmu “Upstream”, jo tas bija mērķētas pārtveršanas režīms. Tomēr saskaņā ar *NSA* apgalvojumu līdz 2017. gada aprīlim ar programmu “Upstream” ieguva sakarus “uz” 702. pantā noteikto selektoru (piemēram, e-pasta adresi), “no” šī selektora un “par” to un tikai pēc 2017. gada aprīļa ar to ieguva sakarus “uz” 702. pantā noteikto selektoru un “no” tā (skat. iepriekš 263. punktu). Tā kā 702. pantā noteiktie selektori tika attiecināti uz visiem sakariem, ko pārraidīja pa konkrētiem kabeļiem, šķiet, ka programma “Upstream” nemaz tik ļoti neatšķīrās no 8. panta 4. punktā noteiktā režīma, kura ietvaros arī visus pārtvertos sakarus pārraidīja pa daudziem kabeļiem un filtrēja, izmantojot selektorus. Vienīgā acīmredzamā atšķirība starp abiem režīmiem bija tāda, ka no 2017. gada aprīļa *NSA* varēja meklēt vienīgi sakarus “uz” spēcīgo selektoru un “no” tā, savukārt *GCHQ* joprojām varēja meklēt sakarus ar kompleksiem vaicājumiem.

469. “Liberty” tiesvedībā *IPT* apstiprināja ne tikai to, ka attiecībā uz vismaz diviem pieteikuma iesniedzējiem trešajā no apvienotajām lietām atsevišķi viņu sakari tika pārtverti atbilstoši 8. panta 4. punktā noteiktajam orderim, bet arī to, ka tie tika likumīgi un samērīgi saglabāti atbilstoši šim rīkojumam (skat. iepriekš 58.–60. punktu). Lai tos saglabātu likumīgi, šiem sakariem bija jāatbilst vai nu kādam “spēcīgam selektoram” (kas attiecas uz pieteikuma iesniedzējiem vai kādu citu personu, ar kuru viņi sazinājušies), vai arī “kompleksam vaicājumam”. Tiesa varētu pieņemt, ka tad, ja pieteikuma iesniedzēju atsevišķi sakari atbilst kādam “spēcīgam selektoram”, ko izmanto *GCHQ*, pastāvētu risks, ka tos varētu pārtvert un saglabāt *NSA* programmas “Upstream” ietvaros, pamatojoties uz to, ka tos pārraidīja “uz” 702. pantā noteikto selektoru un “no” tā. Pat ja tie neatbilda kādam spēcīgam selektoram, pieteikuma iesniedzēju atsevišķu saziņas aktu saturam joprojām bija izlūkošanas vērtība. Līdz 2017. gada aprīlim šos sakarus bija iespējams pārtvert un saglabāt ar “Upstream” programmu, ja tie bija “par” 702. pantā noteikto selektoru. Šādā gadījumā *NSA* attiecīgajā brīdī (proti, 2017. gada 7. novembrī) joprojām varēja saglabāt minētos sakarus, jo pēc izmaiņām rīcībpolitikā 2017. gada aprīlī tā vienīgi norādīja, ka tā dzēsīs iepriekš ar programmu “Upstream” iegūtos internetā īstenotos sakarus “pēc iespējas drīzāk” (skat. iepriekš 263. punktu). Līdz ar to *NSA* pirms šā datuma iegūtos sakarus “par” spēcīgu selektoru varēja saglabāt vēl kādu laiku pēc tam.

470. Tādējādi Tiesa varētu pieņemt, ka attiecīgajā brīdī (proti, 2017. gada 7. novembrī) pieteikuma iesniedzēji pirmajā un trešajā no apvienotajām lietām, iespējams, bija pakļauti riskam, ka vismaz atsevišķus viņu sakarus var pārtvert un saglabāt ar programmu “Upstream”.

471. Tomēr pieteikuma iesniedzēji attiecībā uz izlūkdatu apmaiņas režīmu joprojām varēja būt cietušie vienīgi tad, ja viņi, iespējams, bija pakļauti arī riskam, ka viņu saziņas aktu saturu pieprasīja *GCHQ*, ņemot vērā, ka tos varēja pieprasīt vienīgi atbilstoši jau izdotam orderim par meklējamo materiālu. Tomēr, kā Tiesa jau ir norādījusi, apstāklis, ka *GCHQ* bija saglabājusi sakarus attiecībā uz vismaz diviem pieteikuma iesniedzējiem trešajā no apvienotajām lietām, liecina par to, ka 8. panta 4. punktā noteiktais orderis attiecās vismaz uz dažu viņu saziņas aktu saturu. Līdz ar to Tiesa varētu pieņemt, ka pieteikuma iesniedzēji pirmajā un trešajā no apvienotajām lietām, iespējams, bija pakļauti riskam, ka viņu sakarus var pieprasīt arī *GCHQ*.

472. Līdz ar to tā atzīst, ka pieteikuma iesniedzēji pirmajā un trešajā no apvienotajām lietām var apgalvot, ka ir cietušie attiecībā uz viņu sūdzībām par izlūkdatu apmaiņas režīmu. Tādēļ Valdības sākotnējais iebildums ir noraidīts.

3. Lietas būtība

a) Palātas spriedums

473. Izvērtējot, vai režīms par pārtvertā materiāla saņemšanu no ārvalstu izlūkdienestiem, piemēram, *NSA*, atbilst 8. pantam, palāta piemēroja sešu minimālo drošības pasākumu modificēto versiju (skat. 275. punktu). Tā kā pirmās divas prasības nevarēja attiekties uz pārtvertā materiāla pieprasīšanu no ārvalstu valdībām, palāta tā vietā izvērtēja, vai apstākļi, kādos var pieprasīt pārtveršanu, ir pietiekami ierobežoti, lai neļautu valstīm izmantot tiesības apiet attiecīgās valsts tiesību aktus vai savas Konvencijā noteiktās saistības. Pēc tam tā piemēroja pēdējās četras prasības pārtvertā materiāla apstrādei, līdz ko to bija ieguvuši Apvienotās Karalistes izlūkdienesti.

474. Palāta uzskatīja, ka valsts tiesību akti un ar *IC* kodeksā izdarītajiem grozījumiem sniegtie precizējumi pietiekami skaidri noteica kārtību, kādā tiek pieprasīta vai nu pārtveršana, vai arī pārtvertā materiāla nodošana no ārvalstu izlūkdienestiem. Turklāt palāta nekonstatēja nevienu būtisku trūkumu režīma piemērošanā un darbībā. Līdz ar to tā ar balsu vairākumu atzina, ka Konvencijas 8. pants nebija pārkāpts.

b) Lietas dalībnieku argumenti

475. Pieteikuma iesniedzēji apgalvoja, ka ieviestie drošības pasākumi saistībā ar izlūkdatu apmaiņas režīmu bija neatbilstoši. Viņi uzsvēra, ka problēmas, kuru dēļ palāta konstatēja Konvencijas 8. panta pārkāpumu saistībā ar masveida pārtveršanas režīmu (proti, tas, ka netiek pārraudzīta selektoru izmantošana, un neatbilstošie drošības pasākumi attiecībā uz saistītajiem sakaru datiem), ir vienlīdz piemērojamas izlūkdatu apmaiņas režīmam.

476. Savukārt Valdība apgalvoja, ka izlūkdatu apmaiņas režīms bija skaidri pamatots valsts tiesību aktos, to paredzot noteikumā, ko papildina *IC* kodeksa 12. nodaļa, un ka šie tiesību akti bija pieejami. Attiecībā uz paredzamību Valdība apgalvoja, ka tā vietā, lai piemērotu sešu minimālo drošības pasākumu modificēto versiju, palātai bija jāveic vispārīgāks izvērtējums, ko parasti piemēro izlūkdatu apmaiņas gadījumos, kas nav saistīti ar sakaru pārtveršanu, lai noskaidrotu, vai tiesību aktos bija pietiekami skaidri noteikta rīcības brīvība un tās īstenošanas veids, lai nodrošinātu personai atbilstošu aizsardzību pret patvaļīgu iejaukšanos. Jebkurā gadījumā, Valdība apgalvoja, ka izlūkdatu apmaiņas režīms atbilda sešiem minimālajiem drošības pasākumiem. *IC* kodeksā bija skaidri raksturota to nodarījumu būtība, kas ir par pamatu izlūkdatu iegūšanai, šādas izlūkdatu iegūšanas ierobežojumi, iegūto izlūkdatu pārbaudes, izmantošanas un uzglabāšanas process, kā arī apstākļi, kādos izlūkdati ir jādzēš vai jāiznīcina.

477. Visbeidzot, Valdības ieskatā nebija pamatota iemesla nošķirt pārtvertos sakarus un saistītos sakaru datus no cita veida informācijas, ko principā var iegūt no ārvalstu izlūkdienesta, piemēram, izlūkdatus no slepeniem izlūkošanas avotiem vai slepenas audio/video uzraudzības. Proti, daudzos gadījumos izlūkdienestiem pat, iespējams, nemaz nav zināms, vai sakari, ko tiem sniedza ārvalsts izlūkdienests, bija iegūti pārtveršanas ceļā.

c) Trešo personu argumenti

i) Francijas valdība

478. Francijas valdība norādīja, ka izlūkdatu apmaiņa starp izlūkošanas partneriem neatkarīgi no tā, vai tā notiek pēc *ad hoc* principa vai arī regulāri, bija ļoti svarīga, jo īpaši cīņā pret pieaugošajiem pārrobežu un plašas izplatības draudiem, kuri valstīm bija jānovērš, galvenokārt identificējot aizdomās turamos pirms to darbības. Šī cīņa attaisnoja izlūkošanas kopienas izveidi, jo bez tās izlūkdienesti ar to ierobežotajām pilnvarām ārvalstīs nevarētu izpildīt tiem uzticēto uzdevumu.

479. Francijas valdība arī apgalvoja, ka izlūkdatu apmaiņas kontekstā iejaukšanās nenotika ar pārtveršanu, bet gan drīzāk ar informācijas iegūšanu, pat ja materiāls bija pārtverts pēc saņēmējas valsts pieprasījuma. Tā atsaucās uz palātas izmantoto pieeju, analizējot Apvienotās Karalistes izlūkdatu apmaiņas režīmu, un lūdza Lielo palātu izmantot tādu pašu pieeju.

480. Valdības ieskatā saņēmēja dienesta konfidencialitāte bija viens no galvenajiem kritērijiem, uz ko sūtītāja valsts balstīja savu lēmumu par datu apmaiņu, līdz ar to saņēmējai valstij bija jāgarantē stingra konfidencialitāte attiecībā uz tai paziņoto informāciju. Tādēļ garantijām, kas nepieciešamas, lai apstrādātu ar izlūkošanas partneri īstenotās datu apmaiņas ceļā apkopotos izlūkdatus, bija jāatbilst “trešās personas principam”, kas liedza aģentūrai, kura bija saņēmusi informāciju no ārvalsts partnera, to koplietot ar trešo personu bez informācijas nosūtītāja piekrišanas. Bez šādas garantijas valstis varētu atteikties pārsūtīt informāciju.

ii) Apvienoto Nāciju īpašais ziņotājs vārda brīvības jautājumos

481. Īpašais ziņotājs apgalvoja, ka datu iegūšanai no ārvalstu izlūkdienestiem jāpiemēro tie paši standarti, ko piemēro tad, kad pašas valsts iestādes iegūst datus. Pretēja nostāja varētu radīt situāciju, kad valsts iestādes *de facto* uztic uzraudzības darbības ārpakalpojumu sniedzējiem, apejot *ICCPR* paredzētos aizsardzības mehānismus.

iii) “Access Now”

482. “Access Now” apgalvoja, ka, lai gan starptautiskās tiesiskās palīdzības līgumi (turpmāk tekstā – “STPL”) paredz pārredzamu un formālu procesu, kas ļauj vienai valstij pieprasīt izlūkdatus no kādas citas valsts, slepenās sakaru izlūkdatu programmas (piemēram, “Five Eyes” izlūkdatu apmaiņas tīkls, kam pievienojušās Amerikas Savienotās Valstis, Austrālija, Kanāda un Jaunzēlande) nebija pārskatāmas un tās aizliedza starptautiskie cilvēktiesību standarti. Šī organizācija norādīja, ka šādas slepenas programmas nav nepieciešamas, jo attiecīgos izlūkdatus varēja iegūt STPL ietvaros.

iv) Koalīcija “Nīderlandes pilsoņi pret Plasterku [Plasterk]” (“Burgers tegen Plasterk”)

483. “Nīderlandes pilsoņi pret Plasterku”, proti, koalīcija, ko veidoja piecas personas un četras asociācijas, bija pieteikuma iesniedzēji lietā pret Nīderlandi, kurā viņi mēģināja apstrīdēt datu apmaiņu starp Nīderlandes iestādēm un to ārvalstu izlūkošanas partneriem (tostarp Amerikas Savienotajām Valstīm un Apvienoto Karalisti).

484. Iestājoties šajā Tiesā izskatāmajā lietā kā trešā persona, tā apgalvoja, ka izlūkdatu apmaiņa jāatļauj vienīgi tad, ja tiek paredzēti atbilstoši drošības pasākumi un ārvalstu iestādei ir stabils juridiskais pamats materiāla iegūšanai. Pretējā gadījumā varētu tikt apieti Konvencijas 8. pantā paredzētie aizsardzības mehānismi. Valstīm nedrīkst ļaut iegūt no ārvalstu iestādēm materiālu, kuru tās pašas nav varējušas likumīgi iegūt.

v) “Center for Democracy and Technology” (“CDT”) un “Pen American Center” (“PEN America”)

485. *CDT* un “PEN America” apgalvoja, ka apstākļos, kādos notiek starptautiskā sadarbība masveida datu un sakaru uzraudzībā, ir jānodrošina atbilstība trim nosacījumiem: valstis aktīvi izvērtē un pārliecinās, vai to ārvalstu partneru tiesiskais un administratīvais regulējums, kas regulē pārtveršanu, ir atbilstošs, un ietver šos atbilstības pasākumus valsts tiesību aktos; ir saņemta neatkarīga, uz pamatotām aizdomām balstīta atļauja, vēlams no tiesas, izmantot uz konkrētām personām attiecināmus selektorus, lai pieprasītu no ārvalstu partneriem iegūtu informāciju, kā arī ir noteikta prasība par uzraudzīto subjektu turpmāku informēšanu.

486. *CDT* un “PEN America” norādīja, ka *NSA* izmantotie pārtveršanas režīmi, jo īpaši saskaņā ar *FISA* 702. pantu un izpildrīkojumu Nr. 12333, neatbilda ne Konvencijas 8. pantā noteiktajai prasībai par pārtveršanu “saskaņā ar likumu”, ne prasībai par tās “samērīgumu” un ka šie trūkumi ietekmēja Apvienotās Karalistes izlūkdatu apmaiņas režīma likumību.

vi) Eiropas Nacionālo cilvēktiesību institūciju tīkls (“ENNHRI”)

487. *ENNHRI* minēja piemērus par dalībvalstīm, kurās, tā ieskatā, bija būtiski mainījusies starptautiskās izlūkdatu apmaiņas būtība, kā rezultātā bija kļuvis grūti atšķirt “pieprasītos” un “nepieprasītos” datus. Tas norādīja, ka vēsturiski starptautiskā izlūkdatu apmaiņa ietvēra izvērtēto datu vai pabeigto izlūkdatu pārsūtīšanu. Tomēr jaunu tehnoloģiju rašanās bija par pamatu aizvien pieaugošai neizvērtēto “neapstrādāto” datu apmaiņai. Pat tad, kad bija noslēgta vienošanās par divpusējo vai daudzpusējo izlūkošanas sadarbību, automatizācijas un lielo datu rašanās kontekstā bija daudz grūtāk izvērtēt, ko viena puse saņēma no otras, tostarp to, vai informācija atbilda sākotnējā pieprasījuma parametriem. Līdz ar to bija nepieciešama stabila un neatkarīga starptautiskās izlūkdatu apmaiņas pārraudzība, nenošķirot pieprasītos datus no nepieprasītajiem datiem. Pārraudzības iestādēm jābūt juridiski pilnvarotām pārraudzīt visus to izlūkdienestu starptautisko sadarbību skarošos jautājumus, sadarboties ar neatkarīgām pārraudzības iestādēm no trešām valstīm izlūkdatu apmaiņas jomā un piesaistīt neatkarīgus speciālistus ar pieredzi moderno informācijas un komunikāciju tehnoloģiju jomā, ja tas nepieciešams.

vii) “Human Rights Watch” (“HRW”)

488. Lai gan šie pieteikumi attiecās uz ārvalstu izlūkdatu saņemšanu no Amerikas Savienotajām Valstīm, *HRW* uzskatīja, ka to valstu tīkls, ar kurām tika koplietoti sakaru izlūkdati, bija ievērojami plašāks. Piemēram, “Five Eyes Alliance” veidoja Apvienotā Karaliste, Amerikas Savienotās Valstis, Austrālija, Kanāda un Jaunzēlande, turklāt tika uzskatīts, ka pastāv citas, daudz ierobežotākas izlūkdatu apmaiņas koalīcijas (piemēram, “Nine Eyes”, kurā papildus ietilpst arī Dānija, Francija, Nīderlande un Norvēģija, “Fourteen Eyes”, kurā papildus ietilpst arī Vācija, Beļģija, Itālija, Spānija un Zviedrija, un “Forty-One Eyes”, kurā papildus ietilpst arī citas sabiedrotās koalīcijas Afganistānā).

viii) “Open Society Justice Initiative” (“OSJI”)

489. *OSJI* apgalvoja, ka valstīm nav jāsaņem vai jāpieprasa dati no trešām personām tādā veidā, ka tiek apietas 8. pantā noteiktās personu tiesības. Lai tas nenotiktu, materiāla sākotnējās apkopošanas brīdī bija jāveic drošības pasākumi, tostarp iepriekš jāpārbauda attiecīgās ārvalsts atbilstība cilvēktiesībām un tās pārtveršanas tiesību akti un prakse, kā arī neatkarīga, vēlams tiesas noteikta, apmaiņas pasākumu *a posteriori* pārraudzība, lai nodrošinātu, ka ir ieviesti un īstenoti drošības pasākumi.

ix) Elektroniskā privātuma informācijas centrs (“EPIC”)

490. *EPIC* apgalvoja, ka Amerikas Savienoto Valstu tiesību akti pieļāva neselektīvi masveidā uzraudzīt personas, kuras nav ASV pilsoņi. Tas norādīja, ka uzraudzība notika saskaņā ar *FISA* 702. pantu un izpildrīkojumu Nr. 12333. Uzraudzība saskaņā ar 702. pantu Amerikas Savienotajās Valstīs notika ar pakalpojumu sniedzēju palīdzību piespiedu kārtā, un tā bija vērsta uz personām, kuras nav ASV pilsoņi un par kurām pamatoti uzskatīja, ka tās atrodas ārpus Amerikas Savienotajām Valstīm. Uzraudzības darbība netika iepriekš pārskatīta tiesā, nebija nepieciešams atsaukties uz pamatotām aizdomām, un nebija tiesību aktos noteikta pienākuma informēt uzraudzības subjektus. Vienīgā prasība bija tāda, ka *FISC* katru gadu ir jāpārskata novērojamo personu noteikšanas un izlūkdatu un ar to saistīto darbību samazināšanas procedūras, kuru mērķis ir ierobežot ASV pilsoņu vai Amerikas Savienotajās Valstīs esošu personu saziņas aktu satura iegūšanu.

491. Tas arī norādīja, ka saskaņā ar izpildrīkojumu Nr. 12333 *NSA* bija pilnvarota iegūt ārvalstu izlūkošanas un pretizlūkošanas datus. Rīkojums paredzēja plašas pilnvaras veikt sakaru izlūkdatu uzraudzību no dažādiem avotiem, tostarp optiskās šķiedras kabeļu tīkliem. Datus apkopoja ārpus Amerikas Savienoto Valstu teritorijas. Nebija pieejami ziņojumi vai oficiāla informācija par uzraudzības apmēru atbilstoši rīkojumam, ko tiesai nebija jāpārrauga.

492. *EPIC* ieskatā ar *NSA* veikto uzraudzību tiktu pārkāpts Konvencijas 8. pants, pamatojoties uz to, ka nav ierobežots uzraudzības apjoms un ilgums un nav nodrošināta atbilstoša pārraudzība, informēšana un tiesiskās aizsardzības līdzekļi.

x) Starptautiskā Juristu komisija (“ICJ”)

493. *ICJ* Tiesā atsaucās uz Starptautisko tiesību komitejas noteikumu par valsts atbildību (turpmāk tekstā – “*ILC* noteikumi”) 15. un 16. pantu. Tā apgalvoja, ka saskaņā ar 15. pantu līgumslēdzēja valsts varētu būt atbildīga par masveida uzraudzību, ko veikusi valsts, kas nav līgumslēdzēja valsts, ja tās īstenotu organizētas un strukturētas sadarbības formas, un ka saskaņā ar 16. pantu līgumslēdzēja valsts varētu būt atbildīga par masveida uzraudzību, ko veic kāda valsts, kas nav līgumslēdzēja valsts, ja tā sniegtu ieguldījumu novērošanas programmā un tās rīcībā būtu faktiska vai konstruktīva informācija par sistēmā saistošo starptautisko cilvēktiesību ievērošanas pienākumu pārkāpumiem. *ICJ* arī norādīja, ka līgumslēdzējām valstīm, kuras piedalās vai sniedz ieguldījumu masveida uzraudzības programmā, bija pienākums izveidot drošības pasākumu sistēmu 8. pantā noteikto tiesību aizsardzībai un aizsargāt to jurisdikcijā esošās personas pret 8. pantā noteikto tiesību pārkāpumiem, kuru pamatā bija masveida uzraudzības programmas.

xi) Anglijas un Velsas Juridiskā biedrība

494. Juridiskā biedrība apgalvoja, ka 8. panta 4. punktā noteiktais režīms un saistītie kodeksi neparedzēja stabilus vai pārskatāmus drošības pasākumus attiecībā uz juridiski priviliģētu materiālu. Tā kā tie paši drošības pasākumi attiecās uz priviliģētu materiālu, ko ieguva ārvalstis un kas tika izpausts Apvienotās Karalistes izlūkdienestiem, tie paši trūkumi ietekmēja arī šo režīmu.

d) Tiesas vērtējums

i) Veicamais izvērtējums

495. Palāta uzskata, ka sakaru pārtveršana, ko veic ārvalstu izlūkdienesti, nevarēja ietilpt saņēmējas valsts atbildības jomā vai tās jurisdikcijā Konvencijas 1. panta izpratnē, pat ja pārtveršana veikta pēc šīs valsts pieprasījuma (skat. palātas sprieduma 420. punktu). Pirmkārt, ciktāl dažas trešās personas bija atsaukušās uz *ILC* noteikumiem, palāta uzskatīja, ka tiem būtu nozīme vienīgi tad, ja ārvalstu izlūkdienesti ir nodoti saņēmējas valsts rīcībā un rīkojas, īstenojot šīs valsts pārvaldības pilnvaru elementus (6. pants), ja saņēmēja valsts sniedz ārvalstu izlūkdienestiem palīdzību vai atbalstu sakaru pārtveršanā tad, kad tas kvalificējams kā starptautiska prettiesiska rīcība attiecībā uz valsti, kura ir atbildīga par pakalpojumiem, saņēmēja valsts apzinājās starptautiskās prettiesiskās rīcības apstākļus un šī rīcība būtu bijusi starptautiski prettiesiska, ja to pieļautu saņēmēja valsts (16. pants), vai vienīgi tad, ja saņēmēja valsts vada vai kontrolē ārvalsts valdību (17. pants). Otrkārt, no Tiesas judikatūras izriet, ka sakaru pārtveršana, ko veic ārvalstu izlūkdienesti, varēja ietilpt saņēmējas valsts jurisdikcijā vienīgi tad, ja valsts īstenoja pilnvaras vai kontroli pār ārvalstu izlūkdienestiem (skat., piemēram, sprieduma lietā Nr. 55721/07 “Al Skeini [*Al-Skeini*] un citi pret Apvienoto Karalisti” [*GC*] 130.–139. punktu, ECT 2011, un sprieduma lietā Nr. 47708/08 “Jalouds [*Jaloud*] pret Nīderlandi” [*GC*] 139. un 151. punktu, ECT 2014).

496. Lielā palāta ir vienisprātis ar palātu, ka izvērtējamajā situācijā nebija saskatāms neviens no šiem elementiem, turklāt pieteikuma iesniedzēji savos argumentu izklāstos Lielajā palātā uz tiem nav atsaukušies. Tādēļ jebkurš Konvencijas 8. pantā noteikto tiesību aizskārums varētu izrietēt vienīgi no sākotnējā pieprasījuma un turpmākas pārtvertā materiāla saņemšanas, pēc kuras to tālāk uzglabāja, pārbaudīja un izmantoja saņēmējas valsts izlūkdienesti.

497. Konvencijā paredzētie aizsardzības mehānismi būtu neefektīvi, ja valstis varētu apiet savus Konvencijā noteiktos pienākumus, pieprasot to, lai valstis, kuras nav līgumslēdzējas valstis, pārtvertu sakarus, vai arī pārtverto sakaru nodošanu no šīm valstīm vai pat iegūstot šos sakarus, tieši piekļūstot šo valstu datubāzēm, lai gan tas šajās lietās nav tieši izvērtēts. Tādēļ Tiesa uzskata, ka tad, kad valstij, kura nav līgumslēdzēja valsts, tiek iesniegts pieprasījums par materiāla pārtveršanu, šim pieprasījumam ir jābūt pamatotam ar valsts tiesību aktiem, kuriem jābūt pieejamiem attiecīgajai personai un paredzamiem attiecībā uz to sekām (skat. iepriekš minētā spriedumā lietā “Romāns Zaharovs” 228. punktu). Tāpat būs jānodrošina skaidri un detalizēti noteikumi, kuri ļauj pilsoņiem gūt atbilstošu priekšstatu par apstākļiem un nosacījumiem, kādos iestādes ir pilnvarotas iesniegt šādu pieprasījumu (skat. iepriekš minētā spriedumā lietā “Romāns Zaharovs” 229. punktu, iepriekš minētā sprieduma lietā “Malons” 67. punktu, iepriekš minētā sprieduma lietā “Leanders” 51. punktu, iepriekš minētā sprieduma lietā “Huvigs” 29. punktu, iepriekš minētā sprieduma lietā “Krulēns” 30. punktu, iepriekš minētā sprieduma lietā “Valensvela Kontrerass” 46. punktu, iepriekš minētā sprieduma lietā “Rotaru” 55. punktu, iepriekš minētā sprieduma lietā “Vēbere un Sarāvija” 93. punktu, kā arī iepriekš minētā sprieduma lietā “Eiropas integrācijas un cilvēktiesību asociācija un Ekimdžijevs” 75. punktu), un paredz efektīvas garantijas pret šo pilnvaru īstenošanu, lai apietu valsts tiesību aktus un/vai valstu pienākumus, kas noteikti Konvencijā.

498. Tiesa uzskata, ka pārtvertā materiāla saņemšanas brīdī saņēmējā valstī ir jābūt ieviestiem atbilstošiem drošības pasākumiem pārtvertā materiāla pārbaudei, izmantošanai un uzglabāšanai, kā arī tā turpmākai pārsūtīšanai, dzēšanai un iznīcināšanai. Šie drošības pasākumi, ko sākotnēji ieviesa Tiesa savā judikatūrā par līgumslēdzēju valstu veikto sakaru pārtveršanu, vienlīdz attiecas uz pieprasīto pārtverto materiālu, ko līgumslēdzēja valsts saņem no ārvalstu izlūkdienesta. Ja valstīm, kā to apgalvo Valdība, ne vienmēr ir zināms, vai no izlūkdienestiem saņemtais materiāls ir pārtveršanas rezultāts, Tiesa uzskata, ka tādi paši standarti ir jāpiemēro visam materiālam, kas saņemts no izlūkdienestiem un varētu būt pārtveršanas rezultāts.

499. Visbeidzot, Tiesa uzskata, ka attiecībā uz jebkuru režīmu, kas ļauj izlūkdienestiem pieprasīt materiāla pārtveršanu vai pārtverto materiālu no valstīm, kuras nav līgumslēdzējas valstis, vai arī ļauj tiešu piekļuvi šim materiālam, ir jāīsteno neatkarīga pārraudzība, kā arī jāparedz iespēja veikt neatkarīgu *ex post facto* pārskatīšanu.

ii) Šā izvērtējuma piemērošana izskatāmajā lietā

500. 1946. gada 5. marta Lielbritānijas–ASV līgums par sakaru izlūkošanu konkrēti noteica, ka ir pieļaujama materiāla apmaiņa starp Amerikas Savienotajām Valstīm un Apvienoto Karalisti (skat. iepriekš 103. punktu). Tomēr sīkāku informāciju par izlūkdienestu iekšējiem (jeb iekšēji regulētajiem) noteikumiem izpauda vienīgi “Liberty” tiesvedībā (skat. iepriekš 33.–36. punktu). Šī jaunā informācija pēc tam tika iekļauta *IC* kodeksa 12. nodaļā (skat. iepriekš 116. punktu), kas, kā norādīts iepriekš, bija publisks dokuments, kuru apstiprināja abas parlamenta palātas, un kas bija jāņem vērā gan pārtveršanas pienākumus pildošajām iestādēm, gan tiesām un tribunāliem (skat. iepriekš 93.–94. punktu). Tiesa ir atzinusi, ka *IC* kodeksa noteikumus var ņemt vērā, izvērtējot *RIPA* noteiktā režīma paredzamību (skat. iepriekš minētā sprieduma lietā “Kenedijs” 157. punktu un iepriekš 366. punktu), un ka tam pašam jāattiecas uz izlūkdatu apmaiņas režīmu.

501. Līdz ar to Tiesa uzskata, ka režīms, kas reglamentē izlūkdatu pieprasīšanu un saņemšanu no valstīm, kuras nav līgumslēdzējas valstis, bija skaidri pamatots attiecīgās valsts tiesību aktos, kuri pēc grozījumu izdarīšanas *IC* kodeksā bija atbilstoši pieejami. Tā kā šā režīma leģitīmie mērķi, bez šaubām, bija aizsargāt valsts drošību, novērst nekārtības un noziedzību un aizsargāt citu personu tiesības un brīvības, Tiesa turpmāk kopīgi izvērtēs izlūkdatu apmaiņas režīmu atbilstoši tās ierastajai metodoloģijai (skat. iepriekš 334. punktu).

502. *IC* kodeksa 12. nodaļa (skat. iepriekš 116. punktu) paredz tādu pašu pieeju kā pieņemtais valsts tiesiskais regulējums saistībā ar masveida pārtveršanu. Saskaņā ar 12. nodaļu izlūkdienesti varēja iesniegt ārvalsts valdībai pieprasījumu par neanalizētiem pārtvertiem sakariem un/vai saistītiem sakaru datiem vienīgi tad, ja valsts sekretārs jau bija izdevis pārtveršanas orderi saskaņā ar *RIPA*, ja konkrētu sakaru iegūšanai bija nepieciešama ārvalsts valdības palīdzība, jo tos nebija iespējams iegūt atbilstoši esošajam orderim (skat. *IC* kodeksa 12.2. punktu iepriekš 116. punktā), un ja šo sakaru iegūšana pārtveršanas aģentūrai bija nepieciešama un samērīga. Šajā nolūkā attiecīgais *RIPA* noteiktais pārtveršanas orderis bija vai nu 8. panta 1. punktā noteiktais orderis saistībā ar izvērtējamo jautājumu, 8. panta 4. punktā noteiktais orderis un tam pievienotais apliecinājums, kurā iekļauts viens vai vairāki “pārtvertā materiāla apraksti” saistībā ar subjekta saziņas aktu saturu, vai arī tad, kad par subjektu bija zināms, ka tas atrodas Britu salās, 8. panta 4. punktā noteiktais orderis un tam pievienotais apliecinājums, kurā iekļauts viens vai vairāki “pārtvertā materiāla apraksti” saistībā ar subjekta saziņas aktu saturu, kopā ar atbilstošajām 16. panta 3. punktā veiktajām izmaiņām.

503. Izņēmuma apstākļos, kad nebija izdots *RIPA* noteiktais pārtveršanas rīkojums, pieprasījumu attiecībā uz sakariem varēja iesniegt vienīgi tad, ja tas nebija kvalificējams kā apzināta *RIPA* apiešana vai tas nekā citādi neietekmēja tā mērķus (piemēram, tādēļ, ka sakaru iegūšana atbilstoši *RIPA* nebija tehniski iespējama) un ja pārtveršanas aģentūrai šo sakaru pārtveršana bija nepieciešama un samērīga. Šādā gadījumā valsts sekretāram šis pieprasījums bija jāizvērtē un jāizlemj personīgi un saskaņā ar pārskatīto *IC* kodeksu par to jāinformē *IC* komisārs. Saskaņā ar informāciju, kas tika izpausta “Liberty” tiesvedībā un apstiprināta Valdības argumentos gan palātā, gan Lielajā palātā, nebija iesniegts neviens pieprasījums par materiāla pārtveršanu apstākļos, kad nebija izdots *RIPA* noteiktais orderis (skat. iepriekš 42. punktu).

504. Ņemot vērā iepriekš minēto, Tiesa uzskata, ka valsts tiesību aktos bija noteiktas skaidras tiesību normas, kas ļauj pilsoņiem gūt atbilstošu priekšstatu par apstākļiem un nosacījumiem, kādos iestādes var pieprasīt ārvalstij pārtverto materiālu.

505. Ja bija izdots 8. panta 1. punktā vai 8. panta 4. punktā noteiktais orderis, tas bija jāapstiprina valsts sekretāram. Proti, no *IC* kodeksa 12.5. punkta, to lasot kopā ar attiecīgo zemsvītras piezīmi, izriet, ka tad, kad pieprasījums balstīts uz kādu esošu orderi, šim pieprasījumam ir jābūt vērstam “uz” konkrētiem selektoriem, “no” tiem jāizriet un jābūt “par” tiem (proti, saistībā ar kādu konkrētu personu vai personām) un valsts sekretārs jau būtu apstiprinājis pieprasījumu par šo personu saziņas aktu saturu. Lai gan izņēmuma apstākļos pieprasījumu varēja iesniegt tad, ja nebija izdots attiecīgais rīkojums, valsts sekretāram bija personīgi jāapstiprina šis pieprasījums un, ja tas bija balstīts uz konkrētiem selektoriem, personīgi jāizvērtē un jāapstiprina šo saziņas aktu satura pārbaude, atsaucoties uz šādiem faktoriem (skat. iepriekš 116. punktu).

506. Tā kā valsts tiesību akti saistībā ar pieprasījumiem par izlūkdatu apmaiņu paredzēja tādu pašu pieeju kā masveida pārtveršanai un valsts tiesību akti konkrēti aizliedza tiesību normu apiešanu, Tiesa nesaskata nepieciešamību atsevišķi izvērtēt atļaujas izsniegšanas procedūru.

507. Attiecībā uz drošības pasākumiem pieprasītā pārtvertā materiāla pārbaudei, izmantošanai, uzglabāšanai, turpmākai pārraidīšanai, dzēšanai un iznīcināšanai no *IC* kodeksa 12.6. punkta skaidri izrietēja, ka pārtvertajam saturam vai saistītajiem sakaru datiem, ko Apvienotās Karalistes izlūkdienesti ieguva no citas valsts, bija piemērojami tie paši iekšējie noteikumi un drošības pasākumi, ko piemēroja tās pašas kategorijas saturam vai datiem, kad pārtveršanas aģentūras tos tieši ieguva pārtveršanas ceļā saskaņā ar *RIPA*. Līdz ar to drošības pasākumi, kuri noteikti *RIPA* 15. un 16. pantā, ko papildina *IC* kodekss, attiecās vienādi uz pārtvertajiem sakariem un sakaru datiem, kas iegūti no ārvalstu izlūkdienestiem, ar nosacījumu, ka materiāls “pats par sevi liecina par to, ka tas ticis pārtverts”.

508. Tiesa ir izvērtējusi 15. un 16. punktā noteiktos drošības pasākumus saistībā ar masveida pārtveršanas režīmu, un tā guva pārliecību, ka procedūras par iegūtā materiāla uzglabāšanu, piekļuvi, pārbaudi un izmantošanu, materiāla izpaušanu citām pusēm un iegūtā materiāla dzēšanu un iznīcināšanu bija pietiekami skaidras un paredzēja atbilstošu aizsardzību pret pilnvaru ļaunprātīgu izmantošanu (skat. iepriekš 384.–405. punktu). Ņemot vērā iepriekš 498. punktā izklāstītos Tiesas secinājumus, Tiesa norāda, ka *IC* kodeksa 12.6. punkts neparedz ar *IC* kodeksu papildinātā *RIPA* 15. un 16. pantā noteikto drošības pasākumu attiecināšanu uz visu no ārvalstu izlūkdienestiem saņemto materiālu, kas varētu būt pārtverts, paredzot to attiecināšanu vienīgi uz materiālu, kas pats par sevi liecina par pārtveršanu, tomēr Tiesa neuzskata, ka no šā apstākļa vien būtu atkarīga izlūkdatu apmaiņas režīma atbilstība 8. pantam.

509. 8. panta 4. punktā noteiktā režīma kontekstā Tiesai radās bažas par to, ka uz saistītajiem sakaru datiem neattiecas 16. pantā noteiktie drošības pasākumi. Tomēr 8. panta 4. punktā noteiktā režīma ietvaros valsts varēja pārtvert, uzglabāt un meklēt visas to sakaru paketes, ko pārraida konkrēti nesēji. Tādējādi tas, ka uz saistītajiem sakaru datiem vispārīgi neattiecās 16. pantā noteiktie drošības pasākumi, nozīmēja, ka izlūkdienesti acīmredzot bez jebkādiem ierobežojumiem bija varējuši meklēt visus šos datus neatkarīgi no tā, vai tiem bija izlūkošanas vērtība. Tomēr saskaņā ar *IC* kodeksa 12. nodaļu izlūkdienesti masveidā nepieprasīja saturu un saistītos sakaru datus. No *IC* kodeksa 12.5. punkta, to lasot kopā ar attiecīgo zemsvītras piezīmi, izriet, ka tad, ja pieprasījums balstīts uz kādu esošu orderi, šim pieprasījumam ir jābūt vērstam “uz” konkrētiem selektoriem, “no” tiem jāizriet un jābūt “par” tiem (proti, konkrētām personām) un valsts sekretārs jau būtu apstiprinājis pieprasījumu par šo personu saziņas aktu saturu. Lai gan izņēmuma apstākļos pieprasījumu varēja iesniegt tad, ja rīkojums nebija izdots, valsts sekretāram bija personīgi jāapstiprina šis pieprasījums un, ja tas bija balstīts uz konkrētiem selektoriem, personīgi jāizvērtē un jāapstiprina šo sakaru pārbaude, atsaucoties uz minētajiem faktoriem. Ja pieprasījums neattiecās uz konkrētiem selektoriem, jebkurus turpmāk iegūtos sakarus nevarēja pārbaudīt atbilstoši faktoram, kas attiecināms uz kādu personu, par kuru zināms, ka tā atradās Britu salās, ja vien valsts sekretārs nebija apstiprinājis šo sakaru pārbaudi (skat. iepriekš 116. punktu). Citiem vārdiem, izlūkdienesti pieprasīja izlūkdatus par kādu personu, attiecībā uz kuru valsts sekretārs tās saziņas aktu satura iegūšanu jau bija atzinis par nepieciešamu un samērīgu, vai arī iegūtajam materiālam tika piemērots 16. pantā noteiktais drošības pasākums. Tā kā iepriekš vēl nav iesniegts neviens pieprasījums apstākļos, kad nav izdots orderis, šķiet, ka līdz šim visi pieprasījumi ir ietilpuši pirmajā kategorijā.

510. Līdz ar to Tiesa uzskata, ka Apvienotajā Karalistē bija ieviesti atbilstoši drošības pasākumi no izlūkošanas partneriem saņemtā satura un sakaru datu pārbaudei, izmantošanai un uzglabāšanai, šā materiāla turpmākai pārraidīšanai, kā arī tā dzēšanai un iznīcināšanai.

511. Visbeidzot, Tiesa norāda, ka *IC* komisārs un *IPT* bija nodrošinājuši papildu aizsardzības līmeni (skat. iepriekš 41. punktu). *IC* komisārs bija pārraudzījis izlūkdatu apmaiņas režīmu, proti, *IC* kodeksa 12.7. punkts (skat. iepriekš 116. punktu) noteica, ka viņš ir jāinformē par visiem pieprasījumiem, kas iesniegti apstākļos, kad nav izdots rīkojums, turklāt viņš jau uzraudzīja rīkojumu piešķiršanu un to, kā izlūkdienesti uzglabā materiālu.

512. Līdzās *IC* komisāra veiktajai pārraudzībai *IPT* veica izlūkdatu apmaiņas režīma *ex post facto* pārskatīšanu. Kā izriet no “Liberty” tiesvedības, *IPT* varēja vērsties ikviens, kurš vēlējās iesniegt konkrētu vai vispārīgu sūdzību par izlūkdatu apmaiņas režīmu, savukārt *IPT* varēja pārbaudīt gan ārēji, gan iekšēji regulētos noteikumus, lai izvērtētu režīma atbilstību Konvencijai.

513. Līdz ar to Tiesa uzskata, ka pārtvertā materiāla pieprasīšanas un saņemšanas režīms atbilda Konvencijas 8. pantam. Bija ieviesti skaidri un detalizēti noteikumi, kas sniedza pilsoņiem atbilstošu priekšstatu par apstākļiem un nosacījumiem, kādos iestādes bija pilnvarotas iesniegt pieprasījumu ārvalstu izlūkdienestam; valsts tiesību akti paredzēja efektīvas garantijas pret šādu pieprasījumu izmantošanu, lai apietu valsts tiesību aktus un/vai Apvienotās Karalistes pienākumus saskaņā ar Konvenciju; Apvienotajā Karalistē bija ieviesti atbilstoši drošības pasākumi materiāla pārbaudei, izmantošanai, uzglabāšanai, turpmākai pārraidīšanai, dzēšanai un iznīcināšanai, savukārt *IC* komisārs attiecībā uz režīmu veica neatkarīgu pārraudzību, kā arī bija paredzēta iespēja, ka *IPT* veic *ex post facto* pārskatīšanu.

514. Līdz ar to nav pārkāpts Konvencijas 8. pants.

B. Konvencijas 10. pants

515. Pieteikuma iesniedzēji trešajā no apvienotajām lietām arī bija izvirzījuši sūdzību par to, ka izlūkdatu apmaiņas režīma izmantošanas rezultātā tika pārkāptas viņu tiesības, kas paredzētas Konvencijas 10. pantā. Ciktāl šī sūdzība attiecās uz viņu kā NVO darbību, palāta to atzina par nepieņemamu, pamatojoties uz to, ka pieteikuma iesniedzēji nebija izsmēluši iekšējos tiesiskās aizsardzības līdzekļus, jo viņi sūdzību valsts tiesvedībā bija izvirzījuši pārāk vēlu, lai to varētu izskatīt (skat. palātas sprieduma 473. punktu). Tādējādi šis sūdzības aspekts ir ārpus Lielās palātas pārbaudes kompetences.

516. Pieteikuma iesniedzēji trešajā no apvienotajām lietām izvirzīja arī vispārīgāku sūdzību par izlūkdatu apmaiņas režīma atbilstību 10. pantam. Lai gan šis arguments *IPT* tika izvirzīts savlaicīgi, Tiesa piekrīt palātai, ka šis arguments nav iemesls, lai to aplūkotu kā atsevišķu jautājumu papildus tam, kas izriet no Konvencijas 8. panta. Līdz ar to tā uzskata, ka arī šajā jautājumā nav pārkāpts Konvencijas 10. pants.

IV. SAKARU DATU IEGŪŠANA NO SAKARU PAKALPOJUMU SNIEDZĒJIEM

A. Konvencijas 8. pants

517. Pieteikuma iesniedzēji otrajā no apvienotajām lietām izvirzīja sūdzību, ka režīms, kas paredz sakaru datu iegūšanu saskaņā ar *RIPA* II nodaļu, neatbilda viņu tiesībām, kas paredzētas Konvencijas 8. pantā.

1. Palātas spriedums

518. Dienā, kad palāta izskatīja lietu, Apvienotās Karalistes valdība īstenoja atbilstošo procesu, lai aizstātu pašreizējo tiesisko režīmu, kas reglamentē slepenās uzraudzības veikšanu, ar jauno *IPA*. “Liberty” valsts tiesvedībā apstrīdēja tiesību normas jaunajā tiesiskajā regulējumā, kas noteica kārtību, kādā SPS saglabā sakaru datus. Šajā tiesvedībā Valdība atzina, ka attiecīgā tiesību norma bija pretrunā ar ES tiesību aktu prasībām. Līdz ar to Augstā tiesa atzina 4. daļu par tādu, kas nav saderīga ar ES pamattiesībām, jo krimināltiesību jomā iestādes nepiekļuva saglabātajiem datiem vienīgi “smaga nozieguma” apkarošanas nolūkā, turklāt piekļuvi saglabātajiem datiem iepriekš nepārskatīja tiesa vai kāda neatkarīga pārvaldes struktūra.

519. Ņemot vērā gan ES tiesību aktu pārākumu pār Apvienotās Karalistes tiesību aktiem, gan Valdības piekāpšanos valsts tiesvedībā tam, ka *IPA* tiesību normas, kas noteica kārtību, kādā SPS saglabā sakaru datus, nebija saderīgas ar ES tiesību aktiem, palātas ieskatā bija “skaidrs”, ka valsts tiesību akti paredzēja, ka jebkuru režīmu, kas ļauj iestādēm piekļūt SPS saglabātajiem datiem, atļauts izmantot vienīgi “smaga nozieguma” apkarošanas nolūkā un ka šāda piekļuve iepriekš ir jāpārskata tiesai vai kādai neatkarīgai pārvaldes struktūrai. Tā kā iepriekšējam režīmam bija raksturīgi tādi paši “trūkumi” kā pēc tam ieviestajam režīmam, palāta atzina, ka to Konvencijas 8. panta nozīmē nevarēja uzskatīt par tādu, kas darbojas saskaņā ar likumu (skat. palātas sprieduma 465.–468. punktu).

2. Lietas dalībnieku argumenti

520. Lietas dalībnieki Lielajā palātā saistībā ar šo sūdzību neizvirzīja citus argumentus.

3. Tiesas vērtējums

521. Valdība Lielajā palātā neapstrīdēja palātas secinājumus. Turklāt Lielā palāta nesaskata iemeslu, kādēļ nepiekrist palātas secinājumiem.

522. Līdz ar to Tiesa uzskata, ka izskatāmajā lietā tika pārkāpts Konvencijas 8. pants, pamatojoties uz to, ka režīms atbilstoši *RIPA* II nodaļai nebija īstenots “saskaņā ar likumu”.

B. Konvencijas 10. pants

523. Pieteikuma iesniedzēji otrajā no apvienotajām lietām arīdzan izvirzīja sūdzību saskaņā ar Konvencijas 10. pantu saistībā ar režīmu, kas paredz sakaru datu iegūšanu no SPS.

1. Palātas spriedums

524. Palāta atzina, ka II nodaļā noteiktais režīms paredzēja labākus aizsardzības mehānismus tad, ja datus pieprasīja žurnālista avota identificēšanas nolūkā. Proti, Sakaru datu ieguves prakses kodeksa 3.77. punkts paredzēja, ka tad, ja pieteikuma mērķis bija noteikt žurnālistikas informācijas avotu, tam bija jāatbilst primārajai prasībai par rīcību sabiedrības interesēs, turklāt šim pieteikumam bija jāpiemēro 1984. gada Likumā par policiju un pierādījumiem krimināllietās [*Police and Criminal Evidence Act 1984*] (turpmāk tekstā – “*PACE*”) noteiktā kārtība, lai lūgtu tiesu izdot uzrādīšanas rīkojumu šo datu iegūšanai. Saskaņā ar *PACE* 1. papildinājumu pieteikumu uzrādīšanas rīkojuma izdošanai iesniedza tiesnesim, un tad, ja pieteikums attiecās uz materiālu, ko veido žurnālistikas materiāls vai kas šādu materiālu ietver, pieteikums bija jāiesniedz *inter partes*. Iekšēju atļauju varēja izmantot vienīgi tad, kad tika uzskatīts, ka pastāvēja tūlītējs risks cilvēka dzīvībai un ka tiesas atļaujas izsniegšanas procesam raksturīgā kavēšanās varēja apdraudēt personas dzīvību (skat. palātas sprieduma 498. punktu).

525. Tomēr šīs tiesību normas piemēroja vienīgi tad, kad pieteikuma mērķis bija avota noteikšana; tās nebija piemērojamas visos gadījumos, kad tika pieprasīti žurnālista sakaru dati vai bija iespējama netieša iejaukšanās. Turklāt gadījumos, kad tika pieprasīta piekļuve žurnālista sakaru datiem, nebija noteiktas īpašas tiesību normas, kas ļautu tiem piekļūt vienīgi “smaga nozieguma” apkarošanas nolūkā. Līdz ar to palāta uzskatīja, ka attiecībā uz sūdzību, kas izvirzīta saskaņā ar 10. pantu, režīms nebija īstenots “saskaņā ar likumu” (skat. palātas sprieduma 496.–499. punktu).

2. Lietas dalībnieku argumenti

526. Lietas dalībnieki Lielajā palātā saistībā ar šo sūdzību neizvirzīja citus argumentus.

3. Tiesas vērtējums

527. Valdība Lielajā palātā neapstrīdēja palātas secinājumus. Turklāt Lielā palāta nesaskata iemeslu, kādēļ nepiekrist palātas secinājumiem.

528. Līdz ar to Tiesa uzskata, ka izskatāmajā lietā tika pārkāpts arī Konvencijas 10. pants, pamatojoties uz to, ka režīms atbilstoši *RIPA* II nodaļai nebija īstenots “saskaņā ar likumu”.

V. KONVENCIJAS 41. PANTA PIEMĒROŠANA

529. Konvencijas 41. pantā ir noteikts:

“Ja Tiesa konstatē, ka ir noticis Konvencijas un tās protokolu pārkāpums, un ja attiecīgās Augstās Līgumslēdzējas puses iekšējā likumdošana pieļauj, ka tiek veikta tikai daļēja šā pārkāpuma seku labošana, Tiesa, ja nepieciešams, cietušajai pusei piedāvā taisnīgu kompensāciju.”

A. Kaitējums

530. Pieteikuma iesniedzēji neiesniedza prasību saistībā ar naudas izteiksmē novērtēto vai morālo kaitējumu. Līdz ar to Tiesa uzskata, ka šajā ziņā nav pamata piešķirt viņiem jebkādas naudas summas.

B. Izmaksas un izdevumi

531. Pieteikuma iesniedzēji pirmajā no apvienotajām lietām palātā bija pieprasījuši 208 958,55 GBP saistībā ar viņu izmaksām un izdevumiem, savukārt pieteikuma iesniedzēji otrajā no apvienotajām lietām bija pieprasījuši 45 127,89 GBP. Pieteikuma iesniedzēji trešajā no apvienotajām lietām nebija iesnieguši prasību saistībā ar izmaksām un izdevumiem.

532. Palāta piešķīra pieteikuma iesniedzējiem pirmajā no apvienotajām lietām 150 000 EUR saistībā ar tiesvedību, savukārt pieteikuma iesniedzējiem otrajā no apvienotajām lietām – 35 000 EUR saistībā ar tiesvedību.

533. Pieteikuma iesniedzēji pirmajā no apvienotajām lietām Lielajā palātā bija papildus pieprasījuši 138 036,66 GBP, pieteikuma iesniedzēji otrajā no apvienotajām lietām bija papildus pieprasījuši 69 200,20 GBP, savukārt pieteikuma iesniedzēji trešajā no apvienotajām lietām bija pieprasījuši 44 993,60 GBP.

534. Valdība apstrīdēja pieprasītās naudas summas.

535. Saskaņā ar Tiesas judikatūru pieteikuma iesniedzējs ir tiesīgs saņemt kompensāciju par izmaksām un izdevumiem vienīgi tad, ja ir pierādīts, ka šādas izmaksas un izdevumi faktiski bija radušies, kā arī bija nepieciešami un apjoma ziņā samērīgi. Šajā lietā, ņemot vērā Tiesas rīcībā esošos dokumentus un iepriekš minētos kritērijus, Tiesa uzskata, ka ir pamats piešķirt turpmāk minētās naudas summas, lai segtu visas palātā notikušās tiesvedības ietvaros radušās izmaksas: pieteikuma iesniedzējiem pirmajā no apvienotajām lietām – naudas summu 150 000 EUR apmērā, savukārt pieteikuma iesniedzējiem otrajā no apvienotajām lietām – naudas summu 35 000 EUR apmērā. Tā arī uzskata, ka ir pamats piešķirt turpmāk minētās naudas summas, lai segtu visas Lielajā palātā notikušās tiesvedības ietvaros radušās izmaksas: pieteikuma iesniedzējiem pirmajā no apvienotajām lietām – naudas summu 77 500 EUR apmērā, pieteikuma iesniedzējiem otrajā no apvienotajām lietām – naudas summu 55 000 EUR apmērā, savukārt pieteikuma iesniedzējiem trešajā no apvienotajām lietām – naudas summu 36 000 EUR apmērā.

C. Nokavējuma procenti

536. Tiesa uzskata, ka nokavējuma procentu likmei ir jābūt balstītai uz Eiropas Centrālās bankas aizdevuma uz nakti procentu likmi, kam jāpieskaita trīs procentpunkti.

1. ŠO IEMESLU DĒĻ TIESA

1.vienprātīgi *nospriež*, ka ir ticis pārkāpts Konvencijas 8. pants attiecībā uz 8. panta 4. punktā noteikto režīmu;

2.vienprātīgi *nospriež*, ka ir ticis pārkāpts Konvencijas 8. pants attiecībā uz II nodaļā noteikto režīmu;

3.ar divpadsmit balsīm par un piecām balsīm pret *nospriež*, ka nav ticis pārkāpts Konvencijas 8. pants attiecībā uz izlūkdatu saņemšanu no ārvalstu izlūkdienestiem;

4.vienprātīgi *nospriež*, ka, ciktāl to izvirzīja pieteikuma iesniedzēji otrajā no apvienotajām lietām, ir ticis pārkāpts Konvencijas 10. pants attiecībā uz 8. panta 4. punktā un II nodaļā noteikto režīmu;

5.ar divpadsmit balsīm par un piecām balsīm pret *nospriež*, ka nav ticis pārkāpts Konvencijas 10. pants attiecībā uz izlūkdatu saņemšanu no ārvalstu izlūkdienestiem;

6.vienprātīgi *nospriež*, ka:

a) atbildētājai valstij trīs mēnešu laikā ir jāsamaksā pieteikuma iesniedzējiem šādas summas, kas konvertējamas atbildētājas valsts valūtā atbilstoši maksājuma dienā spēkā esošajam kursam:

i) pieteikuma iesniedzējiem pirmajā no apvienotajām lietām: 227 500 EUR (divi simti divdesmit septiņi tūkstoši pieci simti *euro*), kā arī visi nodokļi, kas var būt piemērojami pieteikuma iesniedzējiem attiecībā uz izmaksām un izdevumiem;

ii) pieteikuma iesniedzējiem otrajā no apvienotajām lietām: 90 000 EUR (deviņdesmit tūkstoši *euro*), kā arī visi nodokļi, kas var būt piemērojami pieteikuma iesniedzējiem attiecībā uz izmaksām un izdevumiem;

iii) pieteikuma iesniedzējiem trešajā no apvienotajām lietām: 36 000 EUR (trīsdesmit seši tūkstoši *euro*), kā arī visi nodokļi, kas var būt piemērojami pieteikuma iesniedzējiem attiecībā uz izmaksām un izdevumiem;

b) no dienas, kad pagājuši minētie trīs mēneši, līdz maksājuma veikšanai šīm summām pieskaitāmi procenti pēc vienkāršas likmes, kas vienāda ar Eiropas Centrālās bankas aizdevuma uz nakti procentu likmi kavējuma periodā, pieskaitot trīs procentpunktus;

7.vienprātīgi *noraida* pieteikuma iesniedzēju prasību pārējā daļā par taisnīgu atlīdzību.

Sagatavots angļu un franču valodā un paziņots 2021. gada 25. maija sēdē saskaņā ar Tiesas reglamenta 77. panta 2. un 3. punktu.

|  |  |
| --- | --- |
| Sorens PrebensensSekretāra palīgs | Roberts SpanoPriekšsēdētājs |

Saskaņā ar Konvencijas 45. panta 2. punktu un Tiesas reglamenta 74. panta 2. punktu šim spriedumam ir pievienoti šādi atsevišķi viedokļi:

a) tiesnešu Lemensa, Vehaboviča un Bošņaka kopīgais daļēji piekrītošais viedoklis;

b) tiesneša Pinto de Albukerkes daļēji piekrītošais un daļēji nepiekrītošais viedoklis;

c) tiesnešu Lemensa, Vehaboviča, Ranconi un Bošņaka kopīgais daļēji nepiekrītošais viedoklis.

R. S. O.
S. C. P.

TIESNEŠU LEMENSA, VEHABOVIČA UN BOŠŅAKA KOPĪGAIS DAĻĒJI PIEKRĪTOŠAIS VIEDOKLIS

1. Šajā lietā mēs piekrītam vairākumam visos sprieduma rezolutīvās daļas aspektos, izņemot attiecībā uz 3. punktu (nav pārkāpts Konvencijas 8. pants attiecībā uz izlūkdatu saņemšanu no ārvalstu izlūkdienestiem) un 5. punktu (nav pārkāpts Konvencijas 10. pants saistībā ar izlūkdatu saņemšanu no ārvalstu izlūkdienestiem). Lai pamatotu punktus, kuros mēs nepiekrītam lietas iznākumam, mēs iesniedzam nepiekrītošo viedokli kopā ar mūsu kolēģi, tiesnesi Ranconi. Turklāt mēs iesniedzam šo piekrītošo viedokli, lai uzsvērtu, ka, lai gan šis spriedums kopumā ir veiksmīgi strukturēts un satura ziņā lielākoties skaidri formulēts, tajā nav izmantota iespēja pilnībā uzsvērt to, cik nozīmīga ir privātās dzīves un korespondences neaizskaramība, kad iejaukšanās pieļauta masveida uzraudzības rezultātā.

I. SĀKOTNĒJĀS PIEZĪMES

2. Šī lieta ir saistīta ar līdzsvara panākšanu starp līgumslēdzēju valstu leģitīmajām interesēm un cilvēktiesībām un pamatbrīvībām, ko īpaši aizsargā Konvencijas 8. pants. Izvērtējuma sākumā (sprieduma 322. un 323. punktā) Lielā palāta izvērsti raksturo to moderno draudu būtību, ar kuriem saskaras līgumslēdzējas puses, un atzīst, cik vērtīga var būt masveida pārtveršana, identificējot un novēršot šos draudus. Turklāt spriedumā uzsvērta darbību slepenības nepieciešamība šajā jomā, ko Lielā palāta atzīst par pamatotu, proti, sabiedrībai būs pieejams ļoti neliels daudzums informācijas par attiecīgo režīmu vai šāda informācija nebūs pieejama vispār. Zināmā mērā var piekrist tam, kā ir raksturotas leģitīmās intereses saistībā ar masveida pārtveršanas režīma izmantošanu, tomēr jānorāda, ka tajās pašās sākotnējās piezīmēs nav tikpat spēcīgi uzsvērta privātuma vai jebkuru citu privāto interešu nozīme. Lai gan tas tieši neietekmē konkrētās masveida pārtveršanas sistēmas izvērtējumu, mēs šajā izvērtējumā būtu devuši priekšroku daudz līdzsvarotākam ievadam.

3. Pirms izvērtēt šā sprieduma, mūsuprāt, vājās puses, vēlamies atgādināt, ka privātās dzīves neaizskaramība ir ne tikai dažādu individuālu pamatinterešu, bet arī demokrātiskas sabiedrības pastāvēšanas priekšnoteikums. Tā būtiski ietekmē cilvēka labsajūtu, autonomiju, personīgo attīstību un spēju veidot jēgpilnas attiecības ar citām personām. Tā arī ir svarīgs priekšnoteikums, lai personas varētu īstenot savas pilsoniskās tiesības un līdz ar to arī izmantot brīva un vienlīdzīga demokrātiskas sabiedrības locekļa statusu. Privātās dzīves aizskaršana ne tikai mazina personas autonomiju un pasliktina tās garīgo un fizisko veselību, bet arī apgrūtina demokrātisku pašpārvaldi.

4. Pirmkārt, privātās dzīves neaizskaramība ir svarīga personas garīgajai un fiziskajai veselībai.Tikai sajūta vien, ka citas personas tevi pastāvīgi novēro un vērtē, var nopietni ietekmēt cilvēka garīgo un fizisko labsajūtu. Tādējādi tiek pārāk ierobežota cilvēku sociālā uzvedība, liekot viņiem justies vainīgiem vai kaunēties par savām jūtām vai domām, vēlmēm vai rīcību, ko viņi nevēlētos paust publiski. Šāda spriedze starp viņu iekšējās pasaules vajadzībām un pašapliecināšanās radīto spiedienu var radīt nopietnas veselības problēmas.

5. Otrkārt, ārējie novērojumi un pašapliecināšanās radītais spiediens kavē “brīvības, autonomijas, patības un cilvēku savstarpējo attiecību sekmēšanu un brīvas sabiedrības pastāvēšanu”.[[3]](#footnote-3) Uzraudzība rada kavējošu iedarbību, jo tā samazina apmēru, kādā mēs varam spontāni un patiesi sazināties ar citiem cilvēkiem un iesaistīties zināmās darbībās. Privātās dzīves neaizskaramības trūkums radītu bremzējošu ietekmi uz mūsu iekšējo pasauli, mūsu savstarpējām attiecībām un līdz ar to arī mūsu autonomiju. “Tādējādi tiks zaudēts (..) iekšējais personīgais kodols, kas ir mūsu paražu kritikas, radošuma, pretošanās un atjaunošanās avots.”[[4]](#footnote-4)

6. Treškārt, privātās dzīves neaizskaramība ir svarīga demokrātiskai pašpārvaldei. Masveida uzraudzība rada ārēju un iekšēju spiedienu, liekot indivīdiem pielāgoties un padarot viņus pakļāvīgus un godbijīgus. Lai izvairītos no tiešas apspiešanas un piešķirtu sev leģitimitātes akcentu, pastāv risks, ka valsts veiks uzraudzību, lai panāktu atbilstību un pakļāvību. Kā Džordžs Orvels [*George Orwell*] izklāstīja savā romānā “1984” [*“Nineteen Eighty-Four”*]:

“Protams, nebija iespējams pateikt, vai attiecīgajā brīdī jūs novēro vai ne. Cik bieži vai pēc kādas metodes domu policija pieslēdzas katram atsevišķam vadam, to varēja tikai minēt. Bija pat iespējams, ka tā nemitīgi novēro visus. Lai būtu kā būdams, bija skaidrs, ka tā var pieslēgties katram vadam, kad vien vēlas. Bija jādzīvo, un aiz ieraduma, kas bija pārvērties instinktā, ikviens arī dzīvoja pārliecībā, ka jebkuru skaņu un vārdu kaut kur dzird un, izņemot tumsas brīžus, ik kustību novēro.”[[5]](#footnote-5)

7. Nodrošinot nenovērotas darbības vidi, privātās dzīves neaizskaramība veicina un sekmē pilsoņu morālo autonomiju, kas ir galvenā pašpārvaldes prasība demokrātiskā sabiedrībā.[[6]](#footnote-6) Vienīgi autonomas personas var patiesi pārvaldīt sevi un īstenot visas pilsoniskās tiesības, piemēram, tiesības balsot, biedrošanās brīvību, tiesības piedalīties pilsoniskās sabiedrības dzīvē, kā arī domu un apziņas, vārda un izpausmes, un reliģijas brīvību, kas ir būtiski aspekti pašpārvaldē. Nevar apgalvot, ka mēs pilnībā īstenojam brīvības, kuras šīm tiesībām ir jāgarantē, ja tiek apdraudēta mūsu iekšējā brīvība.

8. Tomēr uzraudzība nerada vienīgi iekšējo spiedienu uz brīvību. Ciktāl pilsoņi saglabā savu autonomiju, tā rada arī ārējo spiedienu uz viņu brīvību īstenot savas pilsoniskās tiesības. Gluži kā pastāvīgas sociālās kontroles ietekmē ir mazāk ticams, ka mēs bailēs no atstumtības rīkosimies savu jūtu un domu vadīti, dzīvošana pastāvīgā valdības uzraudzībā var likt pilsoņiem būt nedaudz piesardzīgākiem, paužot savu politisko pārliecību, nedaudz mazāk brīvi biedroties, nedaudz mazāk brīvi izteikties, nedaudz mazāk paust pretēju viedokli un ne tik aktīvi kandidēt uz valsts amatiem. Bieži vien šķietami nebūtisku traucēkļu kopums var nomākt to, ko reiz dēvējām par brīvu sabiedrību, vēl jo vairāk tādēļ, ka cilvēki uzaug vidē, kurai raksturīgs izteikts konformisms un morālais gļēvums. ASV Augstākās tiesas tiesnesis Viljams O. Duglass [*William O. Douglas*], formulējot savu nepiekrītošo viedokli, bija pārsteidzoši raksturojis draudus, kurus masveida uzraudzība rada mūsu demokrātiskajām brīvībām:

“(..) Var pienākt brīdis, kad neviens vairs nevarēs būt drošs par to, vai viņa sacītais tiek ierakstīts, lai to kādā brīdī izmantotu nākotnē, kad ikviens baidīsies, ka viņa slēptākās domas vairs nepiederēs viņam vien, bet gan valdībai, kad visdedzīgākie un ziņkārākie vienmēr būs gatavi noklausīties mūsu konfidenciālākās un intīmākās sarunas. Ja tāds brīdis pienāks, privātās dzīves neaizskaramība un līdz ar to arī brīvība beigs pastāvēt. Ja var aizskart cilvēka tiesības uz privātās dzīves neaizskaramību, kurš var apgalvot, ka ir brīvs? Ja tiek fiksēts un izvērtēts ikviens vārds vai rodas bažas, ka tas varētu notikt, kurš var apgalvot, ka bauda tiesības uz vārda brīvību? Ja ir zināma un tiek fiksēta ikviena saistība ar kādu biedrību un ja tiek pārtvertas sarunas ar biedriem, kurš var apgalvot, ka bauda biedrošanās brīvību? Šādos apstākļos mūsu pilsoņi baidīsies paust savas domas, izsakot vienīgi visdrošākos un pieņemamākos uzskatus, un biedroties ar citiem, tā vietā biedrojoties vienīgi ar vispieņemamākajām personām. Brīvība, kādu mēs to uztveram Konstitūcijas izpratnē, izzudīs.”[[7]](#footnote-7)

9. Visbeidzot, ņemot vērā jauno tehnoloģiju attīstību, kas ļauj veikt masveida uzraudzību un efektīvāk izmantot apkopoto informāciju, ir pieauguši draudi privātās dzīves neaizskaramībai, kā arī personas datu ļaunprātīgas izmantošanas risks. Mēs nevēlamies apgalvot, ka šie draudi un riski jau ir īstenojušies plašā mērogā vai radījuši iepriekš apspriestās sekas. Tomēr mums ir jāapzinās, ka tie pastāv, kad mēs izstrādājam sistēmu, kas ļauj novērst, atklāt un sodīt jebkuru iespējamu ļaunprātīgu rīcību.

10. Mūsuprāt, Tiesai, ņemot vērā šos apsvērumus, bija jāpiešķir ievērojami lielāka nozīme privātajai dzīvei kopumā un īpaši korespondences konfidencialitātei, mēģinot panākt līdzsvaru starp šiem aspektiem un atbildētājas valsts leģitīmajām interesēm, izmantojot masveida pārtveršanas režīmu. Līdz ar to Lielajai palātai bija: a) jāprecizē un pienācīgi jāuzsver iejaukšanās tiesībās uz privātās dzīves un korespondences neaizskaramību, b) jāparedz skaidri minimālie drošības pasākumi, lai aizsargātu indivīdus pret patvaļīgu vai pārmērīgu iejaukšanos, un līdz ar to c) stingrāk jāizvērtē apstrīdētais masveida pārtveršanas režīms.

II. IEJAUKŠANĀS TIESĪBĀS UZ PRIVĀTĀS DZĪVES UN KORESPONDENCES NEAIZSKARAMĪBU

11. Sprieduma 325. punktā vairākums raksturo masveida pārtveršanas sistēmas posmus. Tas uzskata, ka sākotnējais posms, kas raksturots kā sakaru un saistīto sakaru datu pārtveršana un sākotnēja saglabāšana, pēc kura sakaru daļas tiek nekavējoties atmestas, “nerada būtisku iejaukšanos” (sprieduma 330. punkts). Visu cieņu, taču mēs nepiekrītam. Mēs uzskatām, ka iejaukšanās ir būtiska jau šajā posmā. Pirmkārt, satura pārtveršanas un sākotnējās saglabāšanas rezultātā visi kādas personas sakari, kas plūst cauri atlasītajiem nesējiem, un visi saistītie sakaru dati nonāk valsts iestāžu rokās. Otrkārt, lai gan tiesa, ka šajā posmā šo sakaru saturs vēl nav analizēts vai darīts zināms lēmumu pieņēmējiem un līdz ar to pret attiecīgo indivīdu vēl nevar vērst nekādas darbības, pirmais posms ir *sine qua non* jebkuram turpmākajam posmam. Nav zināms precīzs apmērs, kādā izlūkdienesti apkopo sakarus un ar tiem saistītos datus. Tomēr pastāv vairāki iemesli uzskatīt, ka regulāri tiek pārtverta liela daļa no miljoniem personu sakariem. Šo situāciju saasina fakts, ka attiecīgajām personām parasti par šādu iejaukšanos nav ne jausmas. Šādā situācijā, kad cilvēki nevar zināt, vai viņu sakarus paredzēts pārtvert, bet viņi apzinās, ka šāda iespējamība ir ļoti liela, rodas iejaukšanās trešais elements, proti, cilvēki var pielāgot savu rīcību, bieži radot nopietnas sekas, kā norādīts šā atsevišķā viedokļa 3.–8. punktā.

12. Saskaņā ar sprieduma 330. punktu daļa pārtverto sakaru tiek nekavējoties atmesta. Tiesas rīcībā nav informācijas par šo “atmešanas” kārtību. Var pamatoti pieņemt, ka tas netiek veikts nejauši bez jebkādas iekšējas loģikas un ka šajā procesā izlūkdienesti piemēro noteiktus kritērijus, ar kuriem nederīgais materiāls tiek nošķirts no potenciāli lietderīgā materiāla. Fakts vien, ka šo procesu veic slepenībā un ar nezināmu pamatojumu, mūsuprāt, rada nopietnu pamatu bažām. Ir maz ticams, ka šāds pārskatāmības trūkums atbildīs prasībai par paredzamību, kas savukārt ir viens no priekšnoteikumiem tam, lai iejaukšanās ar Konvencijas 8. pantu aizsargātajās tiesībās būtu likumīga. Neraugoties uz to, vairākums vispār nav pievērsies šim konkrētajam masveida pārtveršanas procesa posmam. Mūsuprāt, tas ir būtisks šā sprieduma trūkums.

III. MINIMĀLIE DROŠĪBAS PASĀKUMI PERSONU AIZSARDZĪBAI PRET PATVAĻĪGU VAI PĀRMĒRĪGU IEJAUKŠANOS

13. Sprieduma 335. punktā ir izklāstīta Tiesas judikatūra par sešām minimālajām prasībām, kas jānorāda valsts tiesību aktos, lai novērstu pilnvaru ļaunprātīgu izmantošanu gadījumos, kad sakari tiek pārtverti kriminālizmeklēšanas nolūkos. Tajā arī ir paskaidrots, ka spriedumā lietā “Romāns Zaharovs pret Krieviju” ([*GC*], Nr. 47143/06, ECT 2015) Tiesa atzina, ka tie paši minimālie drošības pasākumi piemērojami gadījumos, kad pārtveršana notiek valsts drošības apsvērumu dēļ. Pēc tam Lielā palāta min nepieciešamību izstrādāt šīs prasības un tās pielāgot masveida pārtveršanas īpatnībām un noslēgumā uzskaita astoņus kritērijus, kas valsts tiesiskajā regulējumā ir skaidri jādefinē, lai nodrošinātu atbilstību Konvencijas 8. pantam (sprieduma 361. punkts).

14. Šis uzskaitījums ir lieliski pamatots ar argumentiem, un to pavisam noteikti var izmantot, lai nodrošinātu aizsardzību pret patvaļību un pilnvaru ļaunprātīgu izmantošanu. Tomēr uzskaitītie kritēriji:

a) nav viennozīmīgi uzskatāmi par autonomiem minimālajiem drošības pasākumiem, jo jebkura neatbilstība kādam no šiem standartiem šķiet “labojama”, veicot visaptverošu novērtējumu;

b) ir jāīsteno, skaidri definējot attiecīgos drošības pasākumus valsts tiesību aktos, taču tie paši par sevi nenosaka nekādus minimālos drošības pasākumus, un

c) neparedz skaidru indivīda pamata aizsardzību pret nesamērīgu iejaukšanos, jo īpaši posmā, kad apkopotajam materiālam tiek piemēroti spēcīgie selektori, turklāt arī ar šiem kritērijiem paredzētā procesuālā aizsardzība ir nepietiekama.

15. Attiecībā uz a) apakšpunktu vēlamies vērst uzmanību uz sprieduma 360. punktu, kurā pausta nepieciešamība veikt visaptverošu konkrētā masveida pārtveršanas režīma novērtēšanu. Lai gan tas izklausās pievilcīgi, tas pavisam noteikti mazina katra drošības pasākuma nozīmīgumu. Tomēr, mūsuprāt, nevienu drošības pasākumu, ko uzskata par minimālu, nekad nevar kompensēt ar jebkādiem līdzsvarojošiem faktoriem attiecībā uz citiem kritērijiem. Citiem vārdiem, konstatējot neatbilstību šādam minimālam drošības pasākumam, automātiski jāuzskata, ka pārkāpts Konvencijas 8. pants neatkarīgi no tā, vai visaptverošs vērtējums varētu liecināt par pozitīvāku rezultātu. Diemžēl vairākums, šķiet, nav izvēlējies šādu pieeju. Jāpiebilst, ka pieeja, kas nosaka minimālos standartus kā absolūtas robežas, proti, biezas sarkanās līnijas, kuras nedrīkst šķērsot, nodrošinātu stingrāku un paredzamāku aizsardzību, kas ir ārkārtīgi svarīgi jomā, kurā valsts iestāžu darbība tiek turēta stingrā slepenībā, kā rezultātā atbilstoši šajā spriedumā minētajam (skat. 322. punktu) ir pieejams maz informācijas par režīma darbību vai šāda informācija nav pieejama vispār, turklāt pieejamā informācija var būt formulēta, izmantojot neskaidru terminoloģiju.

16. Attiecībā uz b) apakšpunktu vairākums ir norādījis, ka astoņi 361. punktā minētie kritēriji ir skaidri jādefinē valsts tiesiskajā regulējumā. Lai gan šī prasība ir apsveicama, jo īpaši no tiesību akta paredzamības viedokļa, šie kritēriji paši par sevi nenosaka minimālās prasības attiecībā uz materiālajiem vai procesuālajiem nosacījumiem, kas jāievēro, lai izmantotu masveida pārtveršanas režīmu un pārietu no tā sākotnējā posma uz posmiem, kas ir ierobežojošāki. Šo trūkumu daļēji kompensē fakts, ka konkrēti (bet ne visi) sprieduma 348.–360. punktā aplūkotie elementi ir izklāstīti ne tikai aprakstošās daļās, kurās ietverta atsauce uz pastāvošo judikatūru, bet arī preskriptīvajā formulējumā, kas nosaka konkrētas prasības, jo īpaši attiecībā uz atļauju veikt masveida pārtveršanu tās konkrētajos posmos. Taču mēs uzskatām, ka vairākuma izvirzītās prasības nav pietiekamas, lai aizsargātu personu pret patvaļīgu, pārmērīgu vai ļaunprātīgu iejaukšanos viņa vai viņas tiesībās uz privātās dzīves neaizskaramību un korespondenci.

17. Līdz ar to nonākam pie c) apakšpunkta. Mērķētas pārtveršanas kontekstā, galvenokārt noziedzīgu darbību atklāšanas un izmeklēšanas nolūkos, Tiesa ir atsaukusies uz noteiktiem būtiskiem drošības pasākumiem pret pilnvaru ļaunprātīgu izmantošanu. Tādējādi Tiesa ir noteikusi, ka ir jādefinē to noziedzīgo nodarījumu būtība, kas var būt par pamatu pārtveršanas rīkojumam, kā arī to personu kategorijas, kuru sakari var tikt pārtverti. Turklāt Tiesa vairākkārt ir atsaukusies uz prasību par pamatotām aizdomām. Vairākums vienkārši uzskata, ka šie drošības pasākumi nav viegli piemērojami masveida pārtveršanai. Lai gan mēs varam piekrist, ka tos nevar tieši transponēt, joprojām ir jāizstrādā stabila pamataizsardzība, lai drošības pasākumi, kas izstrādāti saistībā ar mērķētu pārtveršanu noziedzības apkarošanas nolūkā, var būt kā lielisks iedvesmas avots, kā mēs to centīsimies paskaidrot turpmāk.

18. Pirmkārt, atšķirībā no mērķētas pārtveršanas noziedzības novēršanā masveida pārtveršanu lielākoties veic valsts drošības nolūkos. Ir grūti saprast, kādēļ nav jārēķinās ar to, ka valsts tiesiskais regulējums skaidri definē iespējamos draudus valsts drošībai un apstākļus, kādos šie draudi var būt par pamatu masveida pārtveršanai.

19. Attiecībā uz otro pamatprasību, kas saistīta ar mērķētu pārtveršanu, proti, to personu kategoriju definēšanu, kuru sakari var tikt pārtverti, var atzīt, ka līdzīgai prasībai būtu maz jēgas masveida pārtveršanas pirmajā posmā, kad neselektīvi tiek pārtverti visi sakari, kas plūst cauri konkrētiem nesējiem. Tomēr iejaukšanās apmērs nav jāattaisno, lai atteiktos no noteikta drošības pasākuma. Turklāt masveida pārtveršanas vēlākos posmos, jo īpaši tad, ja tiek izmantoti spēcīgi selektori nolūkā atlasīt un analizēt kādas identificētas personas saziņas aktu saturu, situācija ir lielā mērā pielīdzināma mērķētai pārtveršanai. Rēķināšanās ar to, ka tiesiskais regulējums definē to personu kategorijas, uz kurām var attiecināt spēcīgos selektorus, nebūtu pārmērīga, bet gan pilnībā atbilstoša prasība.

20. Treškārt, prasība par pamatotām aizdomām ir svarīgs aizsardzības mehānisms pret patvaļīgu un nesamērīgu iejaukšanos vairākās Konvencijā garantētajās tiesībās. Tā attiecas uz iespējamību, ka ir ticis vai tiks izdarīts noziedzīgs nodarījums, kas izraisa iejaukšanos. Lai gan masveida pārtveršana nav jāveic noziegumu izmeklēšanā, bet gan drīzāk valsts drošības nolūkos, mēs uzskatām, ka standartam, kas līdzinās prasībai par pamatotām aizdomām, jāattiecas uz pamatu, atbilstoši kuram var atļaut veikt masveida pārtveršanu. Tas jo īpaši attiecas uz gadījumiem, kad masveida pārtveršana ir vērsta uz kādu identificētu personu, piemērojot spēcīgus selektorus. Skaidrības labad jānorāda, ka demokrātiskā sabiedrībā izlūkdienesti var pārbaudīt kādas personas saziņas aktu saturu un saistītos sakaru datus vienīgi tad, ja tie objektīvam novērotājam var pierādīt, ka attiecīgā persona var būt iesaistīta vai iesaistīsies darbībās, ar kurām tiek aizskartas konkrētas valsts drošības intereses, vai tā ir persona, kura uztur vai var uzturēt kontaktu ar personām, kas ir iesaistītas vai iesaistīsies šādās darbībās. Vairākums šajā spriedumā šādu vai līdzīgu prasību nav apsvēruši.

21. Šo trīs drošības pasākumu vietā vairākums ir noteicis pārāk plašu pamatprasību, proti, ka valsts tiesiskajā regulējumā ir skaidri jādefinē pamatojums, atbilstoši kuram var atļaut veikt masveida pārtveršanu, un apstākļi, kādos var pārtvert personas sakarus. Diemžēl atsauce uz “pamatojumu” un “apstākļiem” ir diezgan neskaidra, jo īpaši tad, ja nav atsauces uz to, kāds šis pamatojums un apstākļi var būt vai nebūt. Turklāt saskaņā ar sprieduma 361. punktā lietoto valodu konkrētā prasība attiecībā uz pamatojumu attiecas vienīgi uz masveida pārtveršanas atļaujas sniegšanas posmu, nevis uz jebkuru turpmāku posmu, tādējādi nesniedzot norādes par to, vai ir noteikta jebkāda pamatprasība, piemēram, attiecībā uz spēcīgo selektoru piemērošanu kādas identificētas personas sakaru pārtveršanai.

22. Atbilstošas pamataizsardzības trūkums būtiski ietekmē procesuālās aizsardzības efektivitāti. Procesuālās aizsardzības galvenais elements ir prasība par iepriekšēju atļauju, ko ar šo spriedumu paredz gan masveida pārtveršanas pirmajā posmā, gan pirms spēcīgo selektoru piemērošanas. Jebkuras iepriekšējās atļaujas izšķirošais aspekts ir pārliecināties, vai paredzētā iejaukšanās atbilst tai noteiktajiem pamatkritērijiem. Tomēr, ja šie pamatkritēriji ir neskaidri, pārāk plaši vai pat tādi nav noteikti, ar prasību par iepriekšēju atļauju ne vienmēr būs nodrošināta pietiekami efektīva aizsardzība pret patvaļību vai pilnvaru ļaunprātīgu izmantošanu.

23. Attiecībā uz prasību par iepriekšēju atļauju spriedumā ir norādīts, ka šī atļauja sākotnējā posmā ir jāizmanto struktūrai, kura ir neatkarīga no izpildvaras. Mēs varam piekrist. Lai gan mēs cienām šādu nostāju, mēs stingri iebilstam pret to, ka pietiek ar to vien, ka attiecībā uz spēcīgo selektoru piemērošanu identificējamām personām tiek sniegta vienīgi iepriekšēja *iekšēja* atļauja. Proti, mēs uzskatām, ka šajā posmā būtu nepieciešama iepriekšēja tiesas kontrole. Lai gan Tiesas pašreizējā judikatūra neparedz prasību par tiesas atļauju personu sakaru mērķētai pārtveršanai, mēs uzskatām, ka ir pamatoti iemesli stiprināt aizsardzības standartu gadījumos, kad masveida pārtveršanā piemēro spēcīgos selektorus. Šie iemesli ir šādi:

a) masveida pārtveršana pretēji mērķētai pārtveršanai nav vērsta vienīgi uz kādu konkrētu personu kategoriju, līdz ar to iespējams pārbaudīt daudz lielāku sakaru apjomu nekā mērķētu sakaru gadījumā;

b) turklāt, piemērojot kādu spēcīgu selektoru, kas attiecināms uz kādu identificētu personu, var tikt pavērta iespēja pārtvert daudz lielāku sakaru apjomu, proti, jebkur, kur konkrētā persona pieminēta, pat ja tā pati nav iesaistījusies šajā saziņā (pretēji saziņai ar saziņas līdzekļiem, ko tā personīgi izmanto);

c) veicot mērķētu pārtveršanu tiesībaizsardzības nolūkos, kādā konkrētā brīdī procesa gaitā parasti tiks īstenota tiesas kontrole. Piemēram, tad, kad pierādījumus iegūst ar mērķētas pārtveršanas palīdzību, to aplūko turpmākajā kriminālprocesā, lai šo procesu īstenojošā tiesa varētu pārliecināties, vai mērķētā pārtveršana attiecīgajā lietā atbilda likumā noteiktajām prasībām. Šāda turpmāka tiesas kontrole parasti netiks veikta masveida pārtveršanas gadījumos, kad tiek piemēroti spēcīgie selektori.

24. Gluži pretēji šim uzskatam vairākums uzskata, ka pietiek vien ar iepriekšēju iekšēju atļauju. Mūsuprāt, iekšēja atļauja nevar nodrošināt tāda līmeņa aizsardzību pret patvaļību un pilnvaru ļaunprātīgu izmantošanu, kādu nodrošina neatkarīga pārbaude. Turklāt ir grūti iedomāties, kā persona, kura uztur organizatorisku un, iespējams, koleģiālu saikni ar pieprasījuma iesniedzēju iestādi, varētu izvērtēt pieprasījumu taisnīgi un nesavtīgi. Iespējams, ka prasības par atļaujas saņemšanu netiks pilnībā izpildītas, līdz ar to netiks sasniegts šā drošības pasākuma mērķis. Tas ir vēl jo vairāk iespējams to augsto līgumslēdzēju pušu valstīs, kurās nav iedibinātas izlūkdienestu demokrātiskas pārraudzības tradīcijas.

25. Jāpiebilst, ka Apvienotās Karalistes un Nīderlandes valdība ir norādījušas, ka jebkura prasība precizēt vai pamatot selektorus vai meklēšanas kritērijus nopietni ierobežotu masveida pārtveršanas efektivitāti (sprieduma 353. punkts) un ka vairākums šim argumentam ir zināmā mērā piekritis (sprieduma 354. punkts). Mēs šim argumentam nevaram piekrist. Mēs uzskatām, ka demokrātiskā sabiedrībā identificētas personas sakarus un saistītos sakaru datus nevar atlasīt un pārbaudīt bez šīs personas piekrišanas, ja vien nav pārliecinošu iemeslu šādi rīkoties. Ja izlūkdienests vai kāda cita iestāde nespēj minēt šādus iemeslus un tos pamatot kādai neatkarīgai iestādei, tas nozīmē vien to, ka šim izlūkdienestam vai iestādei nevajadzētu piekļūt šiem sakariem. Mēs atzīstam, ka var rasties situācija, kad ierastais atļaujas sniegšanas process ir pārāk apgrūtinošs, lai efektīvi neitralizētu draudus valsts drošībai, un ka šajā ziņā jārod citi risinājumi. Tomēr, ja stabila atļaujas sniegšanas sistēma, kas izstrādāta, lai atbilstoši aizsargātu cilvēktiesības, tiek uztverta kā lieks šķērslis, demokrātiskas sabiedrības uzmanība ir jāvērš uz šo apstākli.

IV. APLŪKOJAMĀ MASVEIDA PĀRTVERŠANAS REŽĪMA IZVĒRTĒJUMS

26. Mēs piekrītam pārējo Lielās palātas locekļu secinājumiem sprieduma rezolutīvās daļas 1., 2. un 4. punktā. Līdz ar to mēs uzskatām, ka atsevišķu apstrīdētā režīma iezīmju novērtējums nav pietiekami detalizēts un neļauj pienācīgi apzināt dažus tā trūkumus.

27. Piemēram, mēs vēlamies pievērst lasītāja uzmanību pamatojumam, atbilstoši kuram masveida pārtveršanu var atļaut veikt saskaņā ar Apvienotās Karalistes sistēmu (sprieduma 368.–371. punkts). Masveida pārtveršanas orderi varēja izdot, ja tas bija nepieciešams: a) valsts drošības interesēs, b) smaga nozieguma novēršanai vai atklāšanai vai c) Apvienotās Karalistes ekonomiskās labklājības nodrošināšanai, ciktāl šīs intereses sasaucās ar valsts drošības interesēm.

28. a) un c) apakšpunktā minētie nolūki sasaucās ar valsts drošības interesēm. Šķiet, ka nekur nebija definēta ne valsts drošība, ne valsts intereses. Lai gan mēs atsaucamies uz tiesneša norādi par *IC* komisāra skaidrojumu saistībā ar to, kā praksē uztvēra terminu “valsts drošība” (sprieduma 369. punkts), mēs uzskatām, ka prasības par paredzamību kontekstā šis precizējums joprojām ir nepietiekams. Turklāt mēs apšaubām, vai *IC* komisāra precizējumu var pielīdzināt pastāvīgajai tiesu praksei, kas saskaņā ar Tiesas praksi pieļauj nenoteiktības kompensēšanu tiesību aktos. Tā kā nav skaidras definīcijas, persona nevarēja būt droša par precīzu pamatojumu, kādēļ izlūkdienesti varēja pārtvert un analizēt tās sakarus, pat ja šī persona ir vērsusies pie profesionāla konsultanta.

29. Nolūkam, kas minēts b) apakšpunktā, nebija a) un c) apakšpunktā minētajiem nolūkiem raksturīgo trūkumu. Smags noziegums bija definēts kā nodarījums, par kuru personai (kura sasniegusi divdesmit viena gada vecumu un kurai nav iepriekšējas sodāmības) pamatoti varētu piespriest brīvības atņemšanu uz trim gadiem vai ilgāk, vai ja rīcība izpaužas kā vardarbība, tās rezultātā tiek gūts būtisks finansiāls labums vai arī rīcība ir attiecināma uz lielu skaitu personu, kas rīkojušās kopēja mērķa sasniegšanai (skat. sprieduma 369. punktu). Šāda definīcija aptver ļoti plašu rīcību spektru, kas rada nopietnas šaubas par šā pamatojuma samērīgumu. Turklāt demokrātiskā sabiedrībā izlūkdienestiem nav jābūt pilnvarotiem apkarot noziedzību, ja vien noziedzīgās darbības neapdraud valsts drošību.[[8]](#footnote-8) Valdības skaidrojums, proti, ka masveida pārtveršanas ceļā iegūto informāciju nevar izmantot noziedzīga nodarījuma izmeklēšanā, mūsuprāt, nav pārliecinošs. Šķiet, ka, pamatojoties uz šādi iegūto informāciju, tiesībsargājošās iestādes varētu rīkoties, piemēram, veicot ar izmeklēšanu saistītus pasākumus vai pat noteikt arestus, kas savukārt kļūtu kā pierādījums kriminālvajāšanas nolūkā. Iespējams, ka ne tik tālā nākotnē, izpētot tuvāk šo konkrēto jomu, noziegumu izmeklēšana varētu pāriet no mērķētas uzraudzības uz masveida datu pārtveršanu.

V. SECINĀJUMI

30. Retos gadījumos Tiesa izskata lietu, kas veido mūsu sabiedrības nākotni. Šis ir viens no šādiem gadījumiem. Lielā palāta ir daļēji izmantojusi iespēju, lai visaptveroši izklāstītu principus, kuru mērķis ir aizsargāt cilvēktiesības un pamatbrīvības, jo īpaši tās, kas noteiktas Konvencijas 8. un 10. pantā. Tomēr šajā atsevišķajā viedoklī paskaidroto iemeslu dēļ, veicot iepriekš minēto līdzsvarošanu, vairākums nav pietiekami uzsvēris privātās dzīves un korespondences neaizskaramību, kam vairākos aspektos netiek nodrošināta pietiekama aizsardzība, kad iejaukšanās notikusi masveida pārtveršanas rezultātā. Atliek vien cerēt, ka turpmāk lietās saistībā ar konkrētu iejaukšanos noteiktu personu tiesībās Tiesa interpretēs un turpinās attīstīt principus tā, kā tas pienākas demokrātiskā sabiedrībā un atbilstoši tās vērtībā

TIESNEŠA PINTO DE ALBUKERKES DAĻĒJI PIEKRĪTOŠAIS UN DAĻĒJI NEPIEKRĪTOŠAIS VIEDOKLIS

**I. Ievads (1. punkts)**

**II. Tiesas *pro autoritate* masveida pārtveršanas režīma kritisks izvērtējums (2.–18. punkts)**

A. Neskaidra valoda (2.–3. punkts)

B. Neobjektīva metodoloģija (4.–12. punkts)

C. Nepilnīgs drošības pasākumu režīms (13.–15. punkts)

D. Sākotnējais secinājums (16.–18. punkts)

**III. *Pro persona* masveida pārtveršanas režīma izvērtējums (19.–34. punkts)**

A. Sakaru masveida pārtveršana (19.–29. punkts)

B. Pārtverto datu apmaiņa ar ārvalstu izlūkdienestiem (30.–31. punkts)

C. Saistīto sakaru datu masveida pārtveršana (32. punkts)

D. Sākotnējais secinājums (33.–34. punkts)

**IV. Apstrīdētā Apvienotās Karalistes pārtveršanas režīma kritika (35.–58. punkts)**

A. Sakaru masveida pārtveršana saskaņā ar *RIPA* (35.–49. punkts)

B. Pārtverto datu apmaiņa ar ārvalstu izlūkdienestiem saskaņā ar *IC* kodeksa 12. nodaļu (50.–54. punkts)

C. Saistīto sakaru datu masveida pārtveršana saskaņā ar *RIPA* (55.–57. punkts)

D. Sākotnējais secinājums (58. punkts)

**V. Secinājums (59.–60. punkts)**

I. IEVADS

1. Es balsoju ar vairākumu, izņemot secinājumu par to, ka nav pārkāpts Konvencijas 8. un 10. punkts saistībā ar pārtvertā materiāla saņemšanu no ārvalstu izlūkdienestiem, proti, attiecībā uz masveida materiālu, ko Amerikas Savienoto Valstu Nacionālās drošības aģentūra (*NSA*) pārtvēra, izmantojot programmas “PRISM” un “Upstream”. Turklāt es nepiekrītu vairākuma pamata argumentācijai saistībā ar secinājumu par 8. un 10. panta pārkāpumu. Šā viedokļa mērķis ir norādīt mana nepiekrītošā viedokļa iemeslus.[[9]](#footnote-9)

II. TIESAS *PRO AUTORITATE* MASVEIDA PĀRTVERŠANAS REŽĪMA KRITISKS IZVĒRTĒJUMS

A. Neskaidra valoda

2. Diemžēl jau iesākumā jānorāda, ka Tiesas lietotā valoda ir nepieņemami neskaidra, kas tiks paskaidrots turpmāk šā viedokļa izklāstā. Lai gan dažkārt lietotā valoda atspoguļo Tiesas apzinātu nodomu piešķirt atbildētājai valstij rīcības brīvību šā sprieduma izpildē, citos gadījumos tā liecina par tiesnešu vilcināšanos viņu tiesas spriešanas funkcijas izpildē. Līdz ar to tiek ne tikai vājināta Tiesas autoritāte, bet arī mazināta šā sprieduma vērtība standartu izvirzīšanas ziņā.

3. Tā kā Eiropas cilvēktiesību juridiskie jēdzieni ir autonomi tādējādi, ka tie nav absolūti atkarīgi no attiecīgo valstu juridisko jēdzienu nozīmes un piemērošanas jomas, un ņemot vērā juridisko jautājumu novatorismu Lielajā palātā aplūkotajā lietā, Tiesai bija jādefinē kā “melns uz balta” juridiskie pamatjēdzieni, ko tā izmanto šajā spriedumā,[[10]](#footnote-10) neatkarīgi no tā, kā tie ir definēti 2000. gada Likumā par izmeklēšanas pilnvaru regulējumu (*RIPA*), Sakaru pārtveršanas prakses kodeksā (*IC* kodekss) vai jebkuros iekšēji regulētos noteikumos. Skaidrības labad jānorāda, ka izmantošu turpmāk uzskaitītos terminus, kas definēti šādi:

**a) “pārtveršanas subjekts”** ir fiziskas un juridiskas personas, tostarp valsts dienesti, privātas sabiedrības, NVO un jebkuras pilsoniskās sabiedrības organizācijas, kuru elektroniskie sakari var tikt vai ir tikuši pārtverti;[[11]](#footnote-11)

**b) “pārtvertais materiāls” vai “masveida materiāls”** ir elektronisko sakaru saturs vai saistīto sakaru datu saturs, kas apkopots masveida pārtveršanas veidā;[[12]](#footnote-12)

**c) “saistītie sakaru dati”** ir dati, kas nepieciešami, lai noteiktu elektronisko sakaru avota atrašanās vietu un to galamērķi, kā arī sakaru datumu, laiku, ilgumu un veidu, identificētu izmantoto sakaru ierīci, kā arī noteiktu galiekārtas atrašanās vietu un sakarus, datus, kas *inter alia* ietver lietotāja vārdu un adresi, zvanītāja un zvanu saņemošās personas tālruņa numurus, kā arī IP adresi attiecībā uz interneta pakalpojumiem;[[13]](#footnote-13)

**d) “masveida pārtveršana”** ir elektronisko sakaru (un saistīto sakaru datu), kas cirkulē cauri nesējiem, mērķēta un nemērķēta pārtveršana ar spēcīgajiem selektoriem un selektoriem;

**e) “nesēji”** ir elektronisko sakaru nesēji (galvenokārt zemūdens optiskās šķiedras kabeļi);

**f) “spēcīgie selektori”** ir specifiski (uz personu attiecināmi) identifikatori, kas saistīti ar kādu identificētu vai identificējamu mērķi un ļauj iegūt elektroniskos sakarus, ko pārraida uz šo mērķi, no tā vai par to;

**g) “selektori”** ir nemērķēti (uz personu neattiecināmi) identifikatori;

**h) “uz” vai “no” sakari** ir elektroniski sakari, kuru nosūtītājs vai saņēmējs ir izmantotā selektora lietotājs;

**i) “par” sakari** ir tādi, kuros izmantotais selektors ir minēts iegūtajos elektroniskajos sakaros, bet mērķis ne vienmēr ir saziņas dalībnieks;

**j) “ārējie sakari”** ir sakari, ko pārraida vai saņem ārpus valsts teritorijas;[[14]](#footnote-14)

**k) “sakari”** ir “jebkas, kas ietver sacīto, mūziku, skaņas, vizuālus attēlus vai jebkāda apraksta datus un signālus, kas paredzēti vai nu kaut kā izplatīšanai starp personām, starp personu un lietu vai starp lietām, vai jebkuras ierīces iedarbināšanai vai kontrolei”;[[15]](#footnote-15)

**l) “iekšēji regulēti noteikumi”** ir slepeni iekšēji pārtveršanas iestādes noteikumi un rīcība.

B. Neobjektīva metodoloģija

4. Tiesas metodoloģiskā pieeja šajā lietā ir neatbilstoša divu galveno iemeslu dēļ. Pirmkārt, Tiesa bija gatava izlemt tik svarīgu lietu, “pamatojoties uz ierobežotu informāciju par šo [līgumslēdzēju valstu masveida pārtveršanas] režīmu darbības veidu”.[[16]](#footnote-16) Piemēram, Valdība nenorādīja izmantoto selektoru skaitu vai precizitātes pakāpi, pārtverto nesēju skaitu vai to, kā tieši šie nesēji tika atlasīti, vai sagatavoto izlūkošanas ziņojumu veidu attiecībā uz saistītajiem sakaru datiem, tomēr Tiesa neuzstāja uz šīs svarīgās informācijas iegūšanu. Izmeklēšanas pilnvaru tiesa (*IPT*) izvērtēja iekšēji regulētos noteikumus,[[17]](#footnote-17) komisāram sakaru pārtveršanas jautājumos (*IC* komisārs) bija piekļuve “konfidenciālam materiālam”,[[18]](#footnote-18) un pat neatkarīgais terorisma apkarošanas tiesiskā regulējuma pārskatītājs izvērtēja “lielu daudzumu konfidenciālā materiāla”,[[19]](#footnote-19) taču Tiesa šādi nerīkojās un nespēja rīkoties. Tiesai acīmredzami trūka detalizēta materiāla, kas nepieciešams, lai veiktu pilnīgu strukturālo analīzi un izvērtētu masveida pārtveršanu Apvienotajā Karalistē. Ir sarūgtinoši, ka šā sprieduma priekšmeta sensitivitāte, ko Tiesa vairākkārt uzsvēra, derēja vienīgi tam, lai uzsvērtu nepieciešamību pēc masveida pārtveršanas sistēmas “efektivitātes”[[20]](#footnote-20) un “elastīguma”,[[21]](#footnote-21) nevis tam, lai apkopotu visus atbilstošos pierādījumus, kas nepieciešami ar faktiem pamatotam Tiesas spriedumam. Šis pašas Tiesas noteiktais ierobežojums tās pilnvarām apkopot pierādījumus liecina par to, ka Strasbūras tiesneši neuzskata Tiesu par īstu tiesu iestādi, kas ir pilnvarota uzlikt lietas dalībniekiem par pienākumu nodrošināt neierobežotu un beznosacījuma piekļuvi pierādījumiem attiecībā uz lietas priekšmetu. Tā rezultātā Tiesa izteica “gudrus minējumus” par apmēru, kādā notikusi iejaukšanās personas tiesībās dažādos pārtveršanas procesa posmos. Problēma ar reglamentējošo standartu izstrādi, pamatojoties uz “gudriem minējumiem”, ir tāda, ka tie atspoguļo reglamentējošās institūcijas pieņēmumus un aizspriedumus. Turklāt tie skaidri izpaužas arī šajā lietā. Valdības nostājas pamatā ir vienkāršs priekšlikums, proti, “uzticieties mums”. Vairākums bija gatavs pieņemt šo nostāju, riskējot kļūdīties un pieļaujot pārmērīgu izlūkdatu apkopošanu. Es nepieņemu. Kā norādījusi Amerikas Savienoto Valstu Prezidenta kanceleja, “Amerikas pilsoņi nedrīkst pieļaut kļūdu, uzticoties amatpersonām”.[[22]](#footnote-22) To pašu es teiktu eiropiešiem.

5. Otrkārt, iepriekš minētais pašas Tiesas noteiktais acīmredzamais un tiesas spriešanas spējas ietekmējošais ierobežojums liek Tiesai pieņemt to, ka masveida pārtveršana ir neizbēgama, un pat to, ka tikpat neizbēgams ir vispārīgs, nemērķēts, uz aizdomām balstīts pārtveršanas režīms, kā to norādījusi atbildētāja valsts un trešās personas šajā lietā un spriedumā lietā ““Centrum för rättvisa” pret Zviedriju”.[[23]](#footnote-23) Pamatojoties uz cirkulāru argumentāciju, Valdība apstiprināja, ka masveida pārtveršana neatbilda prasībai par pamatotām aizdomām, jo tā bija nemērķēta, pamatojoties uz tās definīciju un to, ka nebija jāievēro prasība par pamatotām aizdomām.[[24]](#footnote-24) Tiesa sekoja šim piemēram un to formulēja aksiomātiski:

“prasība par “pamatotām aizdomām”, kas paredzēta Tiesas judikatūrā par mērķētu pārtveršanu kriminālizmeklēšanas kontekstā, ir mazāk raksturīga masveida pārtveršanas kontekstā, kuras nolūks principā ir preventīvs, nevis konkrēta mērķa un/vai identificējama noziedzīga nodarījuma izmeklēšanai”.[[25]](#footnote-25)

No šīs jaunās paradigmas izriet, ka Tiesa ir atkāpusies no pastāvīgās judikatūras, saskaņā ar kuru tā “neuzskata, ka ir pamats piemērot atšķirīgus principus par tādu noteikumu pieejamību un skaidrību, kas reglamentē, no vienas puses, atsevišķu sakaru pārtveršanu un, no otras puses, vispārīgākas uzraudzības programmas”.[[26]](#footnote-26) Tiesa ir izvērtējusi gan Vācijas, gan Lielbritānijas masveida pārtveršanas sistēmas, piemērojot tos pašus kritērijus, ko piemēro mērķētai pārtveršanai. Es atsaucos uz vispārīgu stratēģisku uzraudzību saskaņā ar spriedumā lietā “Vēbere un Sarāvija pret Vāciju”[[27]](#footnote-27) aplūkoto Vācijas federālā likuma 10. pantu [G-10], kā arī neselektīvu ārpus Britu salām nosūtītu vai saņemtu telekomunikāciju apkopošanu saskaņā ar spriedumā lietā ““Liberty” un citi pret Apvienoto Karalisti”[[28]](#footnote-28) aplūkoto 1985. gada Likumu par sakaru pārtveršanu un liela apjoma iekšējo sakaru pārtveršanu saskaņā ar spriedumā lietā “Kenedijs pret Apvienoto Karalisti”[[29]](#footnote-29) aplūkoto 2000. gada Izmeklēšanas pilnvaru likumu. Tiesa ir atkāpusies no šīs judikatūras pamatprincipiem bez pamatota iemesla, ko es paskaidrošu turpmāk.

6. Turklāt Tiesa pietiekami neuzsvēra to, ka tā bija atjaunojusi un efektīvi piemērojusi līdzšinējo judikatūru trīs nesen izskatītās lietās, kuru priekšmets bija sakaru nemērķēta pārtveršana – vienā no lietām netieši, savukārt abās pārējās lietās – konkrēti. Es atsaucos uz spriedumiem lietās “Romāns Zaharovs pret Krieviju”,[[30]](#footnote-30) “Zabo un Visija pret Ungāriju”[[31]](#footnote-31) un “Mustafa Sezgins Tanrikulu [*Mustafa Sezgin Tanrıkulu*] pret Turciju”[[32]](#footnote-32).Jānorāda, ka arī spriedumā lietā “Romāns Zaharovs pret Krieviju”[[33]](#footnote-33) lietoja spriedumā lietā “Vēbere un Sarāvija” noteiktos kritērijus, izvērtējot operatīvās meklēšanas darbības, tostarp iejaukšanos pasta, telegrāfa un cita veida sakaros, kas varēja ietekmēt “jebkuru personu, kura izmanto šos mobilā tālruņa pakalpojumus”[[34]](#footnote-34) valsts, militārās, ekonomiskās vai ekoloģiskās drošības nolūkā[[35]](#footnote-35). Lielā palāta minētajā lietā nonāca tik tālu, ka tā nosodīja praksi attiecībā uz “pārtveršanas atļaujām, kurās nav minēta konkrēta persona vai tālruņa numurs, kas jānoklausās, bet kuras ļauj pārtvert visus tālruņu sakarus teritorijā, kurā izdarīts noziedzīgs nodarījums”.[[36]](#footnote-36) Spriedumā lietā “Zabo un Visija pret Ungāriju”[[37]](#footnote-37) Tiesa pat vēl vairāk nosodīja “liela pilsoņu skaita neierobežotu uzraudzību”[[38]](#footnote-38) terorisma apkarošanas un ārvalstīs nelaimē nonākušu Ungārijas pilsoņu glābšanas nolūkā[[39]](#footnote-39). Lai gan Tiesa atzina, ka masveida pārtveršana ir nepieciešama cīņā ar iekšējiem un ārējiem draudiem, tā noteica prasību par “pamatotām aizdomām”[[40]](#footnote-40) attiecībā uz ikvienu uzraudzības pasākumu, ņemot vērā spriedumā lietā “Vēbere un Sarāvija” noteiktos kritērijus[[41]](#footnote-41). Savukārt spriedumā lietā “Mustafa Sezgins Tanrikulu pret Turciju”[[42]](#footnote-42) Tiesa nosodīja valsts tiesas lēmumu ļaut pārtvert jebkuras Turcijā esošas personas tālruņa un elektroniskos sakarus nolūkā novērst teroristu organizāciju draudus pēc tam, kad tā bija atsaukusi un apstiprinājusi judikatūru lietās “Vēbere un Sarāvija”, “Romāns Zaharovs” un “Zabo un Visija”.

7. Papildus apgalvojumam, ka “abas lietas [““Liberty” un citi” un “Vēbere un Sarāvija”] tika izskatītas vairāk nekā pirms desmit gadiem” un ka minētajās lietās aplūkotās uzraudzības darbības apjoms bija “daudz šaurāks”,[[43]](#footnote-43) Tiesa minēja trīs iemeslus, lai atkāptos no līdzšinējās judikatūras,[[44]](#footnote-44) kas visi faktiski bija nepamatoti.

8. Pirmais arguments ir tāds, ka masveida pārtveršanas “norādītais nolūks” “daudzos gadījumos” ir uzraudzīt to personu sakarus, kuras atrodas ārpus valsts teritoriālās jurisdikcijas, “kuru nevarētu pārraudzīt ar citiem uzraudzības veidiem”.[[45]](#footnote-45) Tiesa nesniedza un nevarēja sniegt nekādus pierādījumus tam, ka “daudzos gadījumos” masveida pārtveršana “norādītā nolūka” un vēl jo mazāk reālās prakses ziņā attiecās uz personām ārpus valsts teritoriālās jurisdikcijas. Gluži pretēji, visi pieejamie nozīmīgie dokumenti par masveida pārtveršanu, kurus Tiesa izvēlējās ignorēt, vēsta par ko citu. Nav saprotams, kādēļ, ņemot vērā atbildētājas Valdības sniegto pierādījumu trūkumu, Tiesa ir ignorējusi Eiropas Padomes un Eiropas Savienības faktu vērtējumus, kas bija publiski pieejami daudzos nozīmīgos dokumentos par masveida pārtveršanu un publicēti pēc Snoudena skandāla izcelšanās, piemēram, Eiropas Padomes Parlamentārās asamblejas (turpmāk tekstā – “*PACE*”) rezolūcijas 1954 (2013) un 2045 (2015) un rekomendāciju 2067 (2015), 2013. gada 11. jūnija Ministru komitejas deklarāciju un tās atbildi uz *PACE* rekomendāciju 2067 (2015), Eiropas Komisijas pret rasismu un neiecietību Vispārēji politisko rekomendāciju Nr. 11, Cilvēktiesību komisāra 2013. gada 24. oktobra komentārus, viņa 2014. gada 8. decembra un 2015. gada maija dokumentus un viņa 2015. gada 1. oktobra Ziņojumu par trūkumiem Vācijas izlūkošanas un drošības dienestu pārraudzībā [*Report on the shortcomings in the oversight of German intelligence and security services*], Eiropas Parlamenta 2014. gada 12. marta rezolūciju un 2015. gada 29. oktobra rezolūciju, Eiropas datu aizsardzības uzraudzītāja 2014. gada 20. februāra atzinumu un Darba grupas atzinuma Nr. 4/2014 29. pantu. Tā arī nebija ņēmusi vērā Apvienoto Nāciju Organizācijas Ģenerālās asamblejas 2013. gada 18. decembra Rezolūciju Nr. 68/167, Apvienoto Nāciju Organizācijas Cilvēktiesību komitejas (turpmāk tekstā – “*HRC*”) noslēguma apsvērumus par ASV 2014. gada 26. marta ceturto ziņojumu, kā arī Apvienoto Nāciju Organizācijas īpašā ziņotāja un Amerikas Cilvēktiesību komisijas īpašā ziņotāja vārda brīvības jautājumos 2013. gada 21. jūnija kopīgo deklarāciju.[[46]](#footnote-46) Pārsteidzošākais ir tas, ka vairākums pat nav ņēmis vērā pieejamos starptautiskos nozīmīgos dokumentus par Lielbritānijas masveida pārtveršanas režīmu, piemēram, *HRC* noslēguma apsvērumus par Apvienotās Karalistes 2015. gada 17. augusta septīto periodisko ziņojumu[[47]](#footnote-47) un Eiropas Padomes cilvēktiesību komisāra 2016. gada maija Memorandu par uzraudzības un pārraudzības mehānismiem Apvienotajā Karalistē [*Memorandum on Surveillance and Oversight Mechanisms in the United Kingdom*][[48]](#footnote-48).

9. Visi šie dokumenti, kā arī šīs Tiesas nesenie spriedumi lietās “Zabo un Visija”[[49]](#footnote-49) un “Mustafa Sezgins Tanrikulu pret Turciju”[[50]](#footnote-50) un Eiropas Savienības Tiesas (turpmāk tekstā – “EST”) attiecīgā judikatūra[[51]](#footnote-51) ir pretrunā ar iespējamo ārpus valsts teritoriālās jurisdikcijas esošo personu novērošanas izplatību. Šīs iestādes, gluži pretēji, apstiprina, ka masveida uzraudzība ir galvenokārt vērsta uz personām, kuras atrodas valsts teritoriālajā jurisdikcijā.[[52]](#footnote-52) Pati Valdība ir atzinusi, ka vaicājumu skaits saistībā ar saistītajiem sakaru datiem saskaņā ar *RIPA* 8. panta 4. punktu attiecībā uz personām, par kurām zināms, ka tās atrodas Apvienotajā Karalistē – tātad kā iekšējās uzraudzības līdzeklis – sasniedz vairākus tūkstošus nedēļā.[[53]](#footnote-53)

10. Otrais arguments, kas neatbilst līdzšinējai judikatūrai, ir fakts, ka Eiropas Padomes dalībvalstis, “šķiet, veic”[[54]](#footnote-54) masveida pārtveršanu nevis noziegumu izmeklēšanai, bet gan citos nolūkos. Šķiet, ka no Tiesas argumentācijas izriet, ka, tā kā mērķēta pārtveršana “lielākoties”[[55]](#footnote-55) tiek veikta masveida pārtveršanas ietvaros noziegumu atklāšanas un izmeklēšanas nolūkos, bet masveida pārtveršanu var veikt arī ārvalstu izlūkdatu iegūšanai tad, kad var nebūt noteikts ne konkrēts mērķis, ne identificējams nodarījums, uz masveida pārtveršanu neattiecas (un nav jāatiecina) tie paši standarti kā uz mērķētu uzraudzību.[[56]](#footnote-56) Šis ir vēl viens arguments, ko Tiesa nav pierādījusi, jo tā nolēma pieņemt lēmumu, pamatojoties uz šķietamību, nevis faktiem.

11. Patiesībā nemērķēta masveida pārtveršana ir tieši vai netieši aizliegta divdesmit trīs Eiropas valstīs.[[57]](#footnote-57) Kā pārliecinoši pierādīja *PACE*[[58]](#footnote-58) un Eiropas Padomes cilvēktiesību komisārs,[[59]](#footnote-59) neselektīva masveida sakaru uzraudzība ir izrādījusies neefektīva terorisma novēršanā, tāpēc ir ne tikai drauds cilvēktiesību aizsardzībai, bet arī resursu izšķērdēšana. Tādējādi, ja Eiropā ir vienprātība par nemērķētu masveida pārtveršanu, jāņem vērā kopējā nostāja, ka tā ir jāaizliedz, taču Tiesa to ir ignorējusi. Tikai septiņas Eiropas Padomes dalībvalstis izmanto šādus režīmus,[[60]](#footnote-60) un lielākoties tās šādi rīkojas, lai novērstu, atklātu un izmeklētu tādus noziegumus kā terorisms, spiegošana, kiberuzbrukumi un vispārīgākā nozīmē “smagus noziegumus”,[[61]](#footnote-61) kā norādīts iepriekš minētajos nozīmīgajos Eiropas Padomes un Eiropas Savienības dokumentos, šīs Tiesas spriedumā lietās “Zabo un Visija” un “Mustafa Sezgins Tanrikulu”, kā arī attiecīgajā EST judikatūrā. Ārvalstu izlūkdatu vākšana ir tikai viens no daudziem nolūkiem, un Tiesas rīcībā nav statistikas vai citu pierādījumu minimālā elementa par to, kā šī rīcība šajā nolūkā tiek īstenota, neatkarīgi no tā, vai tas ir balstīts uz konkrētu mērķu uzraudzību vai kā citādi. Pat ja izvērtēšanas nolūkos varētu pieņemt, ka ārvalstu izlūkdatu vākšana lielākoties tiek veikta nemērķētas masveida pārtveršanas veidā, tas ne vienmēr nozīmē, ka jebkādai masveida pārtveršanai, tostarp masveida pārtveršanai noziegumu atklāšanas un izmeklēšanas nolūkā, ir jābūt nemērķētai. Pretējā gadījumā masveida pārtveršana kļūst par nepilnību, ko izmanto, lai apietu drošības mehānismus attiecībā uz atsevišķu orderi apstākļos, kad šāds orderis būtu lieliski piemērots attiecīgo sakaru iegūšanai. Tomēr nekas neizslēdz iespēju, ka pašu ārvalstu izlūkdatu vākšanu var veikt masveida pārtveršanas veidā, pamatojoties uz prasību par pamatotām aizdomām par novērojamās personas vai personu grupas līdzdalību valsts drošībai kaitīgās darbībās, pat ja tās nav kvalificējamas kā noziedzīgi nodarījumi.[[62]](#footnote-62)

12. Trešais arguments attiecas tieši uz šo trauslo robežu starp vecmodīgo mērķēto pārtveršanu un jaunajiem masveida pārtveršanas veidiem, ko izmanto, lai izraudzītu noteiktas personas, un tas ir vājākais Tiesas arguments. Attiecībā uz gadījumiem, kad pārtveršanu veic, izmantojot spēcīgos selektorus, Tiesa apgalvo, ka “izraudzīto personu ierīces netiek pārraudzītas”,[[63]](#footnote-63) līdz ar to attiecībā uz masveida pārtveršanu nav jānodrošina tādas pašas garantijas kā parastai mērķētai pārtveršanai. Šis apgalvojums nav pārliecinošs. Automātiska datu vākšana un apstrāde, izmantojot spēcīgos selektorus, kas ļauj iegūt elektroniskos sakarus uz mērķi, no tā vai par to, izmantojot izlūkdienestu izvēlētos datu nesējus, var radīt daudz nopietnāku iejaukšanos 8. pantā noteiktajās tiesībās nekā vienīgi izraudzīto personu ierīču pārraudzība.[[64]](#footnote-64) Līdz ar to ir maldinoši apgalvot, ka tiks pārtvertas “vienīgi” (346. punkts) izraudzīto personu sakaru paketes, radot iespaidu, ka masveida pārtveršana, pamatojoties uz spēcīgajiem selektoriem, ir mazāk nopietna nekā ierastā personas ierīču pārraudzība.

C. Nepilnīgs drošības pasākumu režīms

13. No šīs faktiski nepamatotās argumentācijas Tiesa izdarīja divus juridiskus secinājumus par “pieeju, kas jāievēro masveida pārtveršanas lietās”[[65]](#footnote-65), proti, valsts tiesību aktos nav jāidentificē to noziedzīgo nodarījumu būtība, kas var būt par pamatu pārtveršanas rīkojumam, un personu kategorijas, kuru sakarus var pārtvert, un, lai pamatotu šādu pārtveršanas rīkojumu, nav vajadzīgas nekādas pamatotas aizdomas.[[66]](#footnote-66) Vadoties pēc Tiesas loģikas, tā kā “[masveida pārtveršanas] nolūks principā ir preventīvs, nevis konkrēta mērķa un/vai identificējama noziedzīga nodarījuma izmeklēšana”[[67]](#footnote-67), valsts tiesību aktos nav jāparedz neviens no iepriekš minētajiem drošības pasākumiem, pat ja masveida pārtveršana ir vērsta uz kādu konkrētu personu, kas iesaistīta identificējamā noziedzīgā nodarījumā. Līdz ar to masveida pārtveršanas uzsākšanai kopumā nepieciešams vien uz aizdomām nebalstīts pārtveršanas rīkojums neatkarīgi no tā, vai pārtveršana veicama nozieguma atklāšanas un izmeklēšanas vai citos nolūkos.

14. Šāda Tiesas nostāja atstāj neatbildētus daudzus jautājumus. Kāds ir masveida pārtveršanas pieļaujamais pamatojums? Piemēram, vai “nopietnu noziedzīgu nodarījumu” izmeklēšana bez jebkāda papildu precizējuma ir pieļaujams pamatojums? Kādai ir jābūt izmeklējamā nozieguma smaguma pakāpei? Vai naudas maka un mobilā tālruņa zādzības izmeklēšana ir pieļaujams pamatojums?[[68]](#footnote-68) Vai ekonomiskās un rūpnieciskās spiegošanas veicināšana pārtverošās valsts ekonomiskās labklājības un valsts drošības nolūkos ir pieļaujams pamatojums?[[69]](#footnote-69) Kādi ir pieņemamie “apstākļi”, kādos personas sakarus var pārtvert? Cik nopietnās interesēs veicama personas sakaru pārtveršana masveida pārtveršanas rīkojumā minētajos nolūkos, lai attaisnotu personas sakaru masveida pārtveršanu? Vai ir jāpiemēro spriedumā lietā “Zabo un Visija”[[70]](#footnote-70) noteiktais standarts par atsevišķām aizdomām vai arī spriedumā lietā “Romāns Zaharovs”[[71]](#footnote-71) noteiktie pamatoto aizdomu kritēriji? Kā Tiesa var pieprasīt, lai valsts tiesību aktos “pietiekami skaidri”[[72]](#footnote-72) būtu noteikts pamatojums, atbilstoši kuram var atļaut veikt masveida pārtveršanu, un apstākļi, kādos var pārtvert personas sakarus, ja Tiesai pašai nav pietiekami skaidrs, uz kādu “pamatojumu” un “apstākļiem” tā atsaucas?

15. Tā kā 8. pants attiecas uz visiem masveida pārtveršanas posmiem, tostarp sākotnējo sakaru un saistīto sakaru datu saglabāšanu,[[73]](#footnote-73) Tiesa ir pareizi noteikusi “no gala līdz galam drošības pasākumus”[[74]](#footnote-74). Problēma ir tāda, ka Tiesai nav skaidrības par šo “no gala līdz galam drošības pasākumu” juridisko būtību. No vienas puses, tā ir lietojusi pavēles izteiksmi (“jāīsteno”[[75]](#footnote-75), “jāpakļauj”[[76]](#footnote-76), “jāatļauj”[[77]](#footnote-77), “jāinformē”[[78]](#footnote-78), “jāpamato”[[79]](#footnote-79), “rūpīgi jāfiksē”[[80]](#footnote-80), “arī jāpakļauj”[[81]](#footnote-81), “ir svarīgi, lai tiesiskās aizsardzības līdzeklis būtu”[[82]](#footnote-82)) un tos atzinusi par “fundamentāliem drošības pasākumiem”[[83]](#footnote-83) un pat “minimālajiem drošības pasākumiem”[[84]](#footnote-84). No otras puses, tā ir mazinājusi šo drošības pasākumu efektivitāti, veicot “visaptverošu režīma darbības izvērtējumu”[[85]](#footnote-85), līdz ar to ļaujot panākt kompromisu starp drošības pasākumiem[[86]](#footnote-86). Šķiet, ka galu galā neviens no drošības pasākumiem nav obligāts, un Tiesas lietotā preskriptīvā valoda īsti neatbilst valsts tiesību sistēmas neapspriežamajām iezīmēm. Dažos Eiropas nostūros dedzīgiem slepenajiem dienestiem šķitīs vilinoši izmantot Tiesas izteikti brīvo juridisko standartu formulējumu, un nevainīgi cilvēki agrāk vai vēlāk no tā cietīs.

D. Sākotnējais secinājums

16. Tiesas ieskatā neatkarīgai iestādei,[[87]](#footnote-87) t. i., no izpildvaras neatkarīgai iestādei, jau sākotnēji ir jāizvērtē pārtveršanas nolūks, datu nesēju atlase[[88]](#footnote-88) un selektoru kategorijas,[[89]](#footnote-89) ņemot vērā nepieciešamības un proporcionalitātes principu. Īpaši problemātiska ir ar identificējamām personām saistītu spēcīgu selektoru atlase, jo, lai atlasītu un “izmantotu katru spēcīgo selektoru”,[[90]](#footnote-90) nav nepieciešama iepriekšēja neatkarīga atļauja. Tiesa uzskata, ka šajā lietā pietiek vien ar iekšējo atļauju kopā ar garantijām, ka pieprasījums par spēcīgo selektoru izmantošanu ir pamatots un iekšējais process ir “rūpīgi” fiksēts.[[91]](#footnote-91)

17. Turklāt no izpildvaras neatkarīgai iestādei ir jāuzrauga masveida pārtveršanas rīkojuma izpilde, tostarp jebkura tā turpmāka atjaunošana, iegūto datu izmantošana, uzglabāšana, turpmāka pārraidīšana un dzēšana, detalizēti fiksējot procesu katrā pārtveršanas posmā, lai atvieglotu šo pārraudzību.[[92]](#footnote-92)

18. Visbeidzot, no izpildvaras neatkarīgai iestādei ir jāveic visa procesa *ex post facto* pārskatīšana, nodrošinot taisnīgu, uz argumentu apmaiņu vērstu procedūru un īstenojot saistošas pilnvaras pārtraukt prettiesisku pārtveršanu un noteikt iznīcināt prettiesiski iegūtus vai uzglabātus datus, kā arī novecojušus, neprecīzus un nesamērīgus datus.[[93]](#footnote-93)

III. *PRO PERSONA* MASVEIDA PĀRTVERŠANAS REŽĪMA IZVĒRTĒJUMS

A. Sakaru masveida pārtveršana

19. Man šķiet, ka iepriekš minētais režīms nav pielīdzināms pietiekamam garantiju kopumam, ko paredz no 8. un 10. panta izrietošās tiesības. Manuprāt, ir pienācis laiks atteikties no tiesas atļaujas, pārraudzības un *ex post facto* pārskatīšanas pamata garantijām masveida pārtveršanas jomā.[[94]](#footnote-94) Principā masveida pārtveršanas “no gala līdz galam” tiesas īstenotu pārraudzību nodrošina šā procesa ārkārtīgi ierobežojošais veids. Es nesaskatu iemeslu, kādēļ tiesiskai valstij nebūtu jāuzticas saviem tiesnešiem, galu galā – saviem gados vecākiem un pieredzējušākiem tiesnešiem, lai lemtu par šādiem jautājumiem. Ja vien Tiesa neuzskata, ka tiesu iestādēm līdzīgas struktūras ir neatkarīgākas nekā parastās tiesas... Manuprāt, tiesu iestādēm līdzīgu struktūru neatkarība nav pašsaprotama. Turklāt, ja parastajām tiesām ir kompetence atļaut, uzraudzīt un pārskatīt sakaru pārtveršanu ļoti sarežģītos kriminālprocesos, piemēram, organizētās noziedzības un terorisma izmeklēšanā, es nesaskatu iemeslu, kādēļ tām nav jābūt kompetentām pildīt tieši tādu pašu funkciju attiecībā uz masveida pārtveršanas procesa darbību. Tādējādi nav jāapšauba ne parasto tiesu neatkarība, ne kompetence, lai izveidotu Konvencijai atbilstošu drošības pasākumu sistēmu attiecībā uz masveida pārtveršanas režīmu. Valstij, kura uzskata, ka tās tiesu vara nav piemērota šo funkciju veikšanai, ir nopietna problēma ar tiesiskumu.

20. Protams, tiesas iejaukšanās nedrīkst būt panaceja.[[95]](#footnote-95) Ir acīmredzams, ka tiesas īstenota visa procesa pārraudzība būtu bezjēdzīga, ja uzraugāmo noziedzīgo nodarījumu un darbību kategorijas un pārtveršanas subjekti nebūtu noteikti valsts tiesību aktos ar nepieciešamo skaidrības un precizitātes pakāpi. Līdz ar to tiesas kontrolei ir jāietver konkrētu nesēju un spēcīgu selektoru atlase. Ar vārdu “konkrēts” es domāju atsevišķus nesējus un spēcīgus selektorus, nevis nesēju vai selektoru “šķiras” vai “kategorijas”, kas garantētu pārtveršanas iestādei absolūtu rīcības brīvību, lai rīkotos pēc savas patikas.

21. Dubultas drošības sistēmas gadījumā, kad tiesnesis izskata politiķa vai administratīvās amatpersonas iepriekš pieņemtos orderus, tiesas īstenotā pārraudzība nedrīkst paredzēt vienīgi iespēju atcelt administratīvo lēmumu, ja tiesnesis uzskata, ka politiķis vai administratīvā amatpersona ir rīkojusies nesaprātīgi. Tā nebūtu īsti tiesas atļauja, jo Konvencijā noteiktais nepieciešamības un proporcionalitātes izvērtējums ir stingrāks nekā vienkāršs saprātīguma izvērtējums.

22. Kā esmu norādījis spriedumā lietā “Zabo un Visija”, Konvencija nepieļauj “datu piezveju” vai “pētnieciskas” ekspedīcijas nemērķētas uzraudzības veidā, pamatojoties uz nemērķētiem selektoriem, vai tādas uzraudzības veidā, kas balstīta uz spēcīgajiem selektoriem un vērsta uz sakariem par izraudzīto pārtveršanas subjektu.[[96]](#footnote-96) Nav pieļaujams arī paplašināt pārtveršanas subjektu tīklu, izmantojot neskaidrākus meklēšanas vārdus. Vēlos atgādināt galveno iemeslu, kāpēc esmu nonācis pie šāda secinājuma. Atļaujot veikt nemērķētu masveida pārtveršanu, būtiski tiek mainīts veids, kā mēs uztveram izmeklēšanu un izlūkdatu vākšanu Eiropā, sākot ar identificējama aizdomās turamā izraudzīšanu līdz ikvienas personas uzskatīšanai par potenciālo aizdomās turamo, kura dati ir jāuzglabā, jāanalizē un jāprofilē.[[97]](#footnote-97) Protams, šādu izmaiņu ietekmi uz nevainīgām personām, galu galā, varētu mazināt vairāk vai mazāk elastīgu tiesnešu un reglamentējošu iestāžu grupa, kā arī vairāk vai mazāk izdevīgu likumu un prakses kodeksu kopums, taču uz šādiem pamatiem balstīta sabiedrība vairāk līdzinātos policijas kontrolētai valstij, nevis demokrātiskai sabiedrībai. Tas būtu pretrunā ar to, ko Eiropai vēlēja dibinātāji, 1950. gadā parakstot Konvenciju.

23. Tādējādi jebkuram uzraudzības mērķim vienmēr jābūt iepriekš identificētam vai identificējamam, balstoties uz pamatotām aizdomām. Skaidrības labad jānorāda, ka masveida pārtveršanai jābūt pieļaujamai, vienīgi pamatojoties uz spēcīgiem selektoriem, kas vērsti uz sakariem no izraudzītā pārtveršanas subjekta un uz to, ja radušās pamatotas aizdomas, ka tas ir iesaistīts tādu juridiski noteiktu kategoriju smagos nodarījumos vai darbībās, kas kaitē valsts drošībai, taču ne vienmēr ir noziedzīgi.[[98]](#footnote-98)

24. Kārtībai, kādā izdod tiesu orderus, jāattiecas arī uz atļauju uzraudzīt sakarus vai saistītos sakaru datus, tostarp slepenus un konfidenciālus datus, izņemot steidzamus gadījumus, kad kompetentais tiesnesis nav uzreiz pieejams, jo tad atļauju var dot prokurors, bet kompetentais tiesnesis to apstiprina vēlāk.

25. Valsts tiesību aktiem ir jāparedz konkrēts režīms, lai aizsargātu priviliģētu profesionālu saziņas aktu saturu attiecībā uz parlamenta deputātiem, ārstiem, advokātiem un žurnālistiem.[[99]](#footnote-99) Tā kā neselektīva, uz aizdomām nebalstīta sakaru masveida apkopošana varētu traucēt ar likumu aizsargātas un konfidenciālas informācijas aizsardzību, to var efektīvi garantēt vienīgi ar tiesas atļauju pārtvert šādus sakarus, ja tiek iesniegti pierādījumi, kas apstiprina pamatotas aizdomas par šo speciālistu izdarītajiem smagiem nodarījumiem vai rīcību, kas kaitē valsts drošībai.[[100]](#footnote-100) Turklāt ir nekavējoties jāiznīcina jebkādi šīm kategorijām pieskaitāmo speciālistu sakari, uz ko attiecas viņu profesionālais noslēpums, ja tie pārtverti nejauši. Valsts tiesību aktiem jāparedz arī absolūts aizliegums pārtvert sakarus, uz ko attiecas reliģisks noslēpums.

26. Tiesas īstenotajai pārraudzībai nav jāapstājas pārtveršanas darbības sākumā. Ja tiesneši nevarētu pārraudzīt pārtveršanas sistēmas darbību, tiesneša sākotnējo iejaukšanos varētu viegli ietekmēt un tā zaudētu efektivitāti, kļūstot par faktiski virtuālu, maldinošu drošības pasākumu. Gluži pretēji, tiesnesim ir jāpiedalās visā procesā, regulāri un uzmanīgi pārbaudot pārtveršanas rīkojuma nepieciešamību un samērīgumu, ņemot vērā iegūtos pārtveršanas datus. Ja vien tiesnesis nesaņem pastāvīgu atgriezenisko saiti no pārtverošās iestādes, pilnvarotais tiesnesis nezinās, kā šī atļauja faktiski tiek izmantota. Pārtveršanas rīkojuma neievērošanas gadījumā tiesnesim jābūt iespējai nekavējoties pārtraukt tā izmantošanu un noteikt pretlikumīgi iegūto datu iznīcināšanu. Tas pats jāattiecina uz gadījumiem, kad operācija vairs nav jāturpina, piemēram, tāpēc, ka uz iegūtajiem datiem neattiecas pārtveršanas rīkojumā minētie nolūki. Tikai tiesnesis, kuram ir tiesības pieņemt šādus saistošus lēmumus, var sniegt efektīvu garantiju par glabājamā materiāla likumību. Kopumā jānorāda, ka tiesnesim jāspēj regulāri pārskatīt sistēmas darbību, tostarp visus pārtveršanas un konfidenciālo pavaddokumentu reģistrus,[[101]](#footnote-101) lai izvairītos no liekas un nesamērīgas iejaukšanās 8. un 10. pantā noteiktajās tiesībās.

27. Visbeidzot, pārtveršanas rīkojuma izmantošanas *ex post* pārskatīšana jāveic, arī informējot personu, uz kuru pārtveršana ir vērsta. Ja nav nekādu šķēršļu, lai informētu personu, kuras sakari ir pārtverti, tas ļautu viņam vai viņai taisnīgā un uz argumentu apmaiņu vērstā procedūrā apstrīdēt šādas pārtveršanas pamatojumu.[[102]](#footnote-102) Tāpēc, maigi izsakoties, ir ļoti apšaubāmi cerēt, ka sistēma, kas nav atkarīga no pārtveršanas subjekta informēšanas, “var sniegt labākas garantijas atbilstošai procedūras norisei nekā sistēma, kuras pamatā ir informēšana”[[103]](#footnote-103). Nevienam pārtveršanas subjekta intereses nerūp vairāk kā pašam subjektam.

28. Ja kāda iemesla, piemēram, valsts drošības interešu, dēļ nav iespējams informēt personu, kuras sakari ir pārtverti, personai reāli nav iespējas uzzināt par uzraudzības pasākumu, kas attiecībā uz viņu ir veikts. Šajā gadījumā kompetentajam tiesnesim obligāti ir jānosaka pienākums pēc savas iniciatīvas (*ex proprio motu*) vai pēc trešās personas (piemēram, prokurora) iniciatīvas izvērtēt veidu, kādā pārtveršanas rīkojums bija izpildīts, lai noteiktu, vai attiecīgie dati bija apkopoti likumīgi un vai tie ir jāsaglabā vai jāiznīcina; pārtveršanas subjekts tad jāpārstāv advokātam, kurš specializējies privātās dzīves neaizskaramības jomā.

29. Turklāt, kas nav mazsvarīgi, cilvēku un finanšu pārraudzības resursiem un iespējām ir jāatbilst pārraudzīto darbību apjomam, citādi visa sistēma būs tikai fasāde, kas aptvers pārtverošo iestāžu diskrecionāro administratīvo procesu.

B. Pārtverto datu apmaiņa ar ārvalstu izlūkdienestiem

30. Tiesa ir noteikusi zemāku aizsardzības standartu masveida pārtveršanas veidā iegūtu datu pārsūtīšanai ārvalstu izlūkdienestiem. Pirmkārt, pārsūtošajai valstij nav pienākuma pārbaudīt, vai saņēmējā valstī ir nodrošināts līdzvērtīgs aizsardzības līmenis. Turklāt pirms katras pārsūtīšanas nav jāpieprasa garantijas, ka saņēmēja valsts, nododot datus, ievēros drošības pasākumus, kas spēj novērst pilnvaru ļaunprātīgu izmantošanu un nesamērīgu iejaukšanos.[[104]](#footnote-104) Tādējādi Tiesa nav izslēgusi iespēju, ka dati pastāvīgi masveidā ir pārsūtīti ārvalstu izlūkdienestam tikai vienā konkrētā nolūkā. Ņemot vērā šo sistēmu, kurai raksturīga izteikta rīcības brīvība, nav skaidrs, kas ir Tiesas pieprasītās “neatkarīgās kontroles” pamatā.[[105]](#footnote-105) Kāds ir neatkarīgas kontroles nolūks, ja nav nepieciešams izvērtēt saņēmējas valsts ieviestos drošības pasākumus (ņemot vērā, ka tie “garantēs materiāla drošu uzglabāšanu un ierobežos tā tālāku izpaušanu”[[106]](#footnote-106)) pirms katras datu pārsūtīšanas reizes? Vai neatkarīga kontrole attiecas vienīgi uz gadījumiem, kad “ir skaidrs, ka tiek pārsūtīts materiāls, attiecībā uz kuru jāievēro īpaša konfidencialitāte, piemēram, žurnālistikas materiāls”[[107]](#footnote-107)? Kam par to jābūt skaidrībai – datus pārsūtošajam izlūkdienestam vai tiesnesim? Vai ir jebkāda atšķirība starp neatkarīgu kontroli un neatkarīgu atļauju? Lietojot tik neskaidru valodu, Tiesa, šķiet, apzināti mazina uz datu pārsūtīšanu attiecināmo drošības pasākumu efektivitāti.

31. Es nesaskatu iemeslu šādai Konvencijā paredzētā aizsardzības mehānisma efektivitātes mazināšanai gadījumos, kad tiek koplietoti masveida dati, un šādu iemeslu nemin arī Tiesa. Saskaņā ar konsolidētajiem Eiropas Padomes un Eiropas Savienības standartiem personas datu apmaiņa ir jāīsteno vienīgi ar trešām valstīm, kas nodrošina aizsardzības līmeni, kurš būtībā ir līdzvērtīgs tam, kas tiek garantēts attiecīgi Eiropas Padomē un Eiropas Savienībā.[[108]](#footnote-108) Tiesas īstenotajai pārraudzībai šeit jābūt tikpat stingrai kā jebkurā citā gadījumā. Šī rūpīgā tiesas īstenotā pārraudzība ir īpaši pamatota, ja Eiropas Padomes dalībvalsts pārsūta datus uz valsti, kas nav dalībvalsts, tāda acīmredzama iemesla dēļ, ka šo datu turpmāka izmantošana valstī, kas nav dalībvalsts, neietilpst Tiesas jurisdikcijā. Šādu tiesas īstenotu pārraudzību nav jāierobežo ar “trešās personas principu”, kas liedz izlūkošanas aģentūrai, kura saņēma informāciju no ārvalstu izlūkdienesta, to koplietot ar trešo personu bez informācijas nosūtītāja piekrišanas.[[109]](#footnote-109)

C. Saistīto sakaru datu masveida pārtveršana

32. Visbeidzot, Tiesa ir atzinusi, ka saistīto sakaru datu masveida pārtveršana var radīt ļoti nopietnu iejaukšanos personas tiesībās,[[110]](#footnote-110) taču šajā lietā tā nav noteikusi tāda paša apmēra aizsardzību.[[111]](#footnote-111) No vienas puses, tā uzliek par pienākumu nodrošināt, lai “būtu ieviesti iepriekš minētie drošības pasākumi”, atsaucoties uz tiem, kas norādīti šā sprieduma 361. punktā, taču, no otras puses, tā atzīst, ka dalībvalstīm ir rīcības brīvība izvēlēties, kādus konkrētus drošības pasākumus ieviest valsts tiesību aktos, jo “tiesību normām, kas reglamentē [saistīto sakaru datu] apstrādi, ne vienmēr visos aspektos jābūt identiskām satura apstrādi regulējošajām tiesību normām”.[[112]](#footnote-112) Tiesas neskaidrais arguments ir tik vispārīgs, ka tas nesniedz norādes par valstīm, kurām “iepriekš minētie drošības pasākumi” attiecībā uz saistīto sakaru datu masveida pārtveršanu ir obligāti, ja tādi vispār noteikti. Līdz ar to Tiesas vilcināšanās nemazina risku, ka tiks analizēta visa personas sociālā dzīve, ko pati Tiesa ir konstatējusi.

D. Sākotnējais secinājums

33. Es nepiekrītu tam, ka “valstīm ir plaša rīcības brīvība, lemjot par to, kāda veida pārtveršanas režīms ir nepieciešams šiem nolūkiem [valsts drošības un citu svarīgu valsts interešu aizsardzībai pret nopietniem ārējiem draudiem], [bet] izmantojot šādu sistēmu, tām piešķirtajai rīcības brīvībai ir jābūt šaurākai”[[113]](#footnote-113). Ja valsts rīcības brīvības robežas ir plašas, pat visstingrākā to kārtības nodrošināšana garantē vienīgi minimālu aizsardzību pret pilnvaru ļaunprātīgu izmantošanu. Rīcības brīvībai jābūt vienādai gan sistēmas izstrādē, gan tās izmantošanā, un šī rīcības brīvība ir neliela, ņemot vērā attiecīgo valsts uzraudzības pilnvaru īpašo nopietnību, šo pilnvaru ļaunprātīgas izmantošanas augsta līmeņa risku un, ko nevajadzētu piemirst, Eiropas kopējo nostāju attiecībā uz nemērķētas masveida pārtveršanas aizliegumu. Šo risku vēl jo vairāk palielina dažu valstu valdības, kuras pārmērīgi nodarbojas ar drošības jautājumu risināšanu un nerimstoši vēlas iegūt datus, attiecībā uz kuriem tagad ir pieejami tehnoloģiski līdzekļi digitālo sakaru kontrolēšanai visā pasaulē.

34. Kopumā jānorāda, ka valsts tiesību aktiem ir jābūt pietiekami skaidriem, lai tie sniegtu fiziskām un juridiskām personām[[114]](#footnote-114) atbilstošu priekšstatu par obligātajiem nosacījumiem un kompleksajām procedūrām, saskaņā ar kurām iestādes ir pilnvarotas veikt masveida pārtveršanu; šajos nosacījumos un procedūrās ietver turpmāk minēto[[115]](#footnote-115):

a) tāda pamatojuma definīciju, kas var attaisnot pārtveršanas rīkojuma pieņemšanu, piemēram, tādu darbību atklāšana, kas apdraud valsts drošību, vai nopietnu noziegumu novēršana, atklāšana vai izmeklēšana, kad nodarījumiem, kas var būt par pamatu pārtveršanas veikšanai, jāatbilst vai nu uzskaitītajiem konkrētajiem smagajiem nodarījumiem, vai arī vispārīgi nodarījumiem, par kuriem paredzēts sods ar brīvības atņemšanu uz četriem vai vairāk gadiem;[[116]](#footnote-116)

b) pārtveršanas subjektu, citiem vārdiem, personu vai iestāžu, kuru sakarus var pārtvert, definīcija:

i) stingrs aizliegums veikt datu piezveju vai pētnieciskas ekspedīcijas, lai atklātu “vēl nezināmo”, tostarp jebkāda veida nemērķētu uzraudzību, balstoties uz nespecifiskajiem selektoriem;

ii) stingrs aizliegums izmantot spēcīgos selektorus, kas vērsti uz sakariem par izraudzīto pārtveršanas subjektu;

iii) atļauja izmantot spēcīgos selektorus, kas vērsti uz sakariem no izraudzītā pārtveršanas subjekta un uz to, ja radušās aizdomas, ka pārtveršanas subjekts ir iesaistīts iepriekš minētajos nodarījumos vai darbībās;

c) to elektronisko sakaru veidu katalogu, ko var pārtvert, piemēram, tālrunis, telefakss, fakss, e-pasts, informācijas meklēšana “Google”, interneta pārlūkošana, sociālie tīkli un mākoņkrātuve;

d) prasību par nepieciešamības principa ievērošanu, kas nosaka, ka:

i) iejaukšanās pārtveršanas subjektu tiesībās ir pienācīgi jāveic izvirzītajos nolūkos un nepārsniedz šo mērķu sasniegšanai nepieciešamo;

ii) pārtveršana ir jāpamato vienīgi kā galējais līdzeklis, proti, ja nav pieejami citi līdzekļi pierādījumu vai informācijas iegūšanai, jo citu mazāk ierobežojošu metožu izmantošana ir izrādījusies neveiksmīga vai, izņēmuma kārtā, ja citas mazāk ierobežojošas metodes tiek uzskatītas par mazāk veiksmīgām;

iii) pārtveršanai jābūt pielāgotai tā, lai pēc iespējas izvairītos no tādu personu vai iestāžu iesaistīšanas, kas nav atbildīgas par iepriekš minētajiem nodarījumiem vai darbībām, un

iv) pārtveršana nekavējoties jāpārtrauc, kad tā vairs neatbilst izvirzītajiem nolūkiem;

e) prasību par samērīguma principa ievērošanu, kas nosaka, ka:

i) ir jāatrod taisnīgs līdzsvars starp pārtveršanas subjektu konkurējošām tiesībām un izvirzītajiem nolūkiem saskaņā ar principu – jo smagāki ir iepriekš minētie nodarījumi vai darbības un to pagātnes vai nākotnes sekas, jo nopietnāka un apjomīgāka pārtveršana var tikt veikta, un

ii) jebkurā gadījumā pārtveršanai ir jānodrošina, ka tiek ievērota pārtveršanas subjektu tiesību būtība (vai minimālā būtība), piemēram, fizisko personu tiesības uz intīmās privātās dzīves neaizskaramību. Pārtveršana ir jāpārtrauc, tiklīdz kļūst skaidrs, ka tā aizskar privātās dzīves neaizskaramības būtību;

f) pārtveršanas rīkojuma ilguma ierobežojumu, ko var pagarināt vienu vai vairākas reizes pēc operācijas rezultātu novērtējuma, bet jebkurā gadījumā ar maksimālo laika ierobežojumu, kas noteikts visai operācijai;

g) tiesas pārraudzību “no gala līdz galam”, kurai jāietver:

i) pārtveršanas atļauja, tostarp konkrētie pārtveramie nesēji un izmantojamie spēcīgie selektori;

ii) regulāra pārtveršanas rīkojuma izpildes kontrole pietiekami īsos intervālos, tostarp pārtveršanas rīkojuma termiņa pagarināšana un iegūto datu pārsūtīšana trešām personām, un

iii) pārtveršanas procesa un pārtverto datu *ex post facto* pārskatīšana;

h) steidzamos gadījumos prokurors var izdot īpašu pārtveršanas rīkojumu, taču tas īsā laikposmā jāapstiprina tiesnesim;

i) procedūru, kas jāievēro, pārbaudot, izmantojot, uzglabājot un iznīcinot iegūtos datus, ar detalizētu aprakstu par tiesas īstenotās pārraudzības apmēru pārtveršanas laikā un pēc tās beigām un ar dokumentāciju par datu dzēšanas galvenajiem posmiem, ciktāl tas nepieciešams tiesas īstenotajai pārraudzībai;

j) izpildāmos nosacījumus un veicamos piesardzības pasākumus, apmainoties ar pārtvertajiem datiem ar ārvalstu izlūkdienestiem, proti:

i) absolūts aizliegums izmantot ārpakalpojumus uzraudzības darbībām, apejot valsts tiesību aktos paredzētos noteikumus;

ii) absolūts aizliegums izlūkošanas iestādei, kas saņēmusi datus no ārvalstu izlūkdienesta, koplietot tos ar trešo personu bez tās nosūtītāja piekrišanas, ar šo noteikumu neierobežojot saņēmējas valsts tiesneša piekļuvi pārsūtītajiem datiem;

iii) absolūts aizliegums apmainīties ar datiem ar ārvalstu izlūkdienestiem, kas nenodrošina aizsardzības līmeni, kurš būtībā ir līdzvērtīgs Konvencijā garantētajam aizsardzības līmenim;

iv) absolūtu aizliegumu veikt datu masveida pārsūtīšanu uz ārvalstu izlūkdienestu vai tos saņemt no šī dienesta nepārtrauktā procesā tikai vienā konkrētā nolūkā;

v) tiesas atļauja pirms katras datu pārsūtīšanas/saņemšanas saskaņā ar tieši tiem pašiem principiem un noteikumiem par iekšzemes masveida pārtveršanu, tostarp, citu starpā, nepieciešamības un proporcionalitātes principu;

vi) šos noteikumus piemēro, neizšķirot pieprasītos un nepieprasītos datus, “jēldatus” (neizvērtētos) un izvērtētos datus;

k) pienākumu paziņot pārtveršanas subjektam, kad pārtveršana ir beigusies, izņemot tad, kad šāda izpaušana apdraudētu valsts drošības intereses, un tādā gadījumā kompetentajam tiesnesim jābūt pilnvarotam pārskatīt pēc savas iniciatīvas (*ex proprio motu*) vai pēc trešās personas iniciatīvas (piemēram, prokurora) visu pārtveršanas procesu, lai noteiktu, vai dati iegūti likumīgi un vai tie ir jāsaglabā vai jāiznīcina, un pārtveršanas subjektu tad aizstāv advokāts, kurš specializējies privātās dzīves neaizskaramības jomā;

l) īpašas garantijas attiecībā uz priviliģētu personu, piemēram, parlamenta deputātu, ārstu, juristu, žurnālistu un mācītāju, profesionālo saziņas aktu satura noslēpumu;

m) garantiju, ka notiesājoša sprieduma pamatā nevar būt vienīgi vai izšķirošā mērā pierādījumi, kas iegūti masveida pārtveršanas veidā;

n) šie principi attiecas uz uzraudzību, kas tiek veikta pašas Līgumslēdzējas puses teritorijā, kā arī uz tās uzraudzību, kas tiek veikta ārpus tās teritorijas, neatkarīgi no uzraudzības nolūka, datu stāvokļa (uzglabāti vai kustībā) vai datu valdījuma (pārtveršanas subjekta vai pakalpojuma sniedzēja valdījumā);

o) valsts pienākumu ievērot un īstenot indivīdu tiesības papildina pienākums aizsargāt personu tiesības no ārpus publiskā sektora esošo dalībnieku, tostarp, korporatīvo struktūru, ļaunprātīgas rīcības.

IV. APSTRĪDĒTĀ APVIENOTĀS KARALISTES PĀRTVERŠANAS REŽĪMA KRITIKA

A. Sakaru masveida pārtveršana saskaņā ar 2000. gada *RIPA*

35. Ņemot vērā iepriekš minēto, man ir principiāls iebildums, kas ir daudz plašāks par Lielās palātas niecīgo problēmu, proti, pret Apvienotās Karalistes masveida pārtveršanas režīmu, kāds tas bija 2017. gada 7. novembrī, proti, pirms 2016. gada Izmeklēšanas pilnvaru likuma (*IPA*) pilnīgas stāšanās spēkā.[[117]](#footnote-117)

36. Masveida pārtveršanas nolūks smagu noziegumu atklāšanā un izmeklēšanā, kā noteikts *RIPA* 81. panta 2. punkta b) apakšpunktā, pavisam noteikti nav savienojams ar starptautiskajās tiesībās dominējošo smaga nozieguma jēdzienu, ciktāl valsts tiesību aktos noteiktais jēdziens ietver nodarījumus, par kuriem paredzēts sods ar brīvības atņemšanu uz laiku, kas nepārsniedz četrus gadus. Turklāt nolūks aizsargāt Apvienotās Karalistes ekonomisko labklājību, ciktāl šīs intereses sasaucas ar valsts drošības interesēm, nav pietiekami precīzs, pieļaujot, ka masveida pārtveršanu veic, piemēram, ekonomiskai un rūpnieciskai spiegošanai un “tirdzniecības kara” nolūkā.[[118]](#footnote-118)

37. Parlamenta Izlūkošanas un drošības komiteja (*ISC*) arī nosodīja 8. panta 4. punktā noteikto valsts sekretāra apliecinājumu plašo formulējumu, un jānorāda, ka šis nosodījums bija pamatots.[[119]](#footnote-119)

38. Iekšējo un ārējo sakaru nodalīšana, kā norādīts *RIPA* 20. pantā, ir ļoti nepilnīga un nepietiekami ierobežo to personu kategorijas, kuru sakari var tikt pārtverti. Kā secinājusi *ISC*, šāda nodalīšana bija mulsinoša un nebija pārskatāma.[[120]](#footnote-120)

39. Valdība pamatoja šo nošķiršanu ar argumentu, ka, “iegūstot izlūkdatus par darbībām ārvalstīs, izlūkdienestiem nav tādas pašas iespējas identificēt mērķus vai draudus, kādas tiem ir Apvienotajā Karalistē”.[[121]](#footnote-121) *IPT* atkārtoti uzsvēra argumentu, norādot, ka “ir grūtāk izmeklēt terorisma un noziedzīgus draudus no ārvalstīm”.[[122]](#footnote-122) Šis pamatojums ir jāinterpretē, ņemot vērā Valdības 2014. gada paziņojumus, kuros atzīts, ka masveida materiāla pieprasījumi ārvalstu izlūkdienestam bija iesniegti “citādi, nevis saskaņā ar kādu starptautisku savstarpējās tiesiskās palīdzības līgumu”.[[123]](#footnote-123) Tādējādi apstrīdēto masveida pārtveršanas sistēmu izveidoja, lai izvairītos no laikietilpīgām un resursu ietilpīgām procedūrām un “stingrākām” saistībām, kas izriet no esošā starptautiskā tiesiskā regulējuma par savstarpēju tiesisko palīdzību, citiem vārdiem, lai apietu drošības pasākumus saskaņā ar esošo starptautisko savstarpējās palīdzības līgumu sistēmu un izmantotu situāciju, kad trūkst regulējuma par jaunajām starptautiskajām uzraudzības tehnoloģijām.

40. Turklāt, palielinoties to sakaru apjomam, ko uzskata par ārējiem,[[124]](#footnote-124) un eksponenciāli palielinoties Britu salās esošo personu arvien pieaugošā sakaru apjoma masveida pārtveršanai,[[125]](#footnote-125) ārējo/iekšējo sakaru nošķiršana tehniskā ziņā vienkārši vairs nav iespējama, līdz ar to tā ir bezjēdzīga. Teritoriālajā jurisdikcijā balstītā iekšējo un ārējo sakaru nošķiršana pēc būtības ir pretrunā ar mūsdienu sakaru plūsmu internetā, kur “Facebook” ziņojums, ar kuru dalījusies kāda draugu grupa Londonā, tiek maršrutēts caur Kaliforniju un līdz ar to attiecībā uz Apvienoto Karalisti ir ārējs.[[126]](#footnote-126) Kā Tiesai atgādināja Juridiskā biedrība, konfidenciāli sakari starp advokātiem un klientiem, pat ja abi atradušies Apvienotajā Karalistē, var būt pārtverti saskaņā ar 8. panta 4. punktā noteikto režīmu.[[127]](#footnote-127) Praksē Valdības norādītais plašais ārējo sakaru jēdziens ietver arī mākoņkrātuvi, informācijas meklēšanu “Google”, pārlūkošanu un darbības sociālajos tīklos.[[128]](#footnote-128) Attiecībā uz daudziem sakaru veidiem var pat nebūt iespējams atšķirt ārējos un iekšējos sakarus, jo saistītie sakaru dati ne vienmēr liecinās par paredzētā saņēmēja atrašanās vietu. Faktu izvērtējumu par to, vai konkrētie sakari ir ārēji vai iekšēji, atsevišķos gadījumos var veikt, vienīgi balstoties uz gūto pieredzi.[[129]](#footnote-129) Mūsdienu dzīves un saziņas apstākļu ciešāka saikne, kas sniedzas pāri valstu robežām, pavisam noteikti nav pamats tam, lai apstrādātu ārējos un iekšējos sakarus atšķirīgi, drīzāk gluži pretēji. Tas, protams, nav jāuztver kā aicinājums pazemināt iekšējo sakaru aizsardzības līmeni, bet gan paaugstināt ārējo sakaru aizsardzības līmeni.

41. Šajā ziņā nav acīmredzami, ka attiecībā uz saziņu starp personu Strasbūrā un personu Londonā saskaņā ar Konvenciju jāparedz ierobežotāka aizsardzība nekā attiecībā uz saziņu starp divām personām Londonā. Tāpēc šķiet, ka nav nekāda objektīva attaisnojuma atšķirīgai attieksmei pret šādām personām, izņemot pieņēmumu, ka draudi biežāk nāk no ārvalstīm un ka ārvalstnieki nav pelnījuši tik daudz uzticības kā pilsoņi, jo viņi rada nopietnāku risku valsts un sabiedrības drošībai nekā pilsoņi, tādējādi attaisnojot nepieciešamību uzraudzīt ārpus Britu salām nosūtītos vai saņemtossakarus.[[130]](#footnote-130) Tas izpaužas arī tajā, kā pret ārvalstniekiem izturas tiesā, kad viņi vēlas īstenot savas tiesības uz privātās dzīves neaizskaramību. *IPT* neizskata sūdzības no pieteikuma iesniedzējiem ārpus valsts teritorijas[[131]](#footnote-131). Šī pret ārvalstniekiem naidīgā “Weltanschauung” jeb nostāja nevar būt vēl neatbilstošāka Konvencijas būtībai.[[132]](#footnote-132) Konvencijas centrā ir indivīds, nevis valsts pilsonis, kas nozīmē to, ka Konvencijā noteiktajām tiesībām kā indivīda tiesībām ir jānodrošina aizsardzība ikreiz, kad kāda Līgumslēdzēja puse rīkojas un tādējādi potenciāli rada nepieciešamību pēc aizsardzības neatkarīgi no tā, kur, pret ko un kādā veidā tā rīkojas. Turklāt Konvencijā noteiktajām tiesībām jāattiecas uz visām Eiropas Padomes dalībvalstīm starptautiskajā sabiedrībā, ciktāl “Eiropas Padomes tiesisko kārtību vairs nevar sajaukt ar tradicionālo starptautisko savstarpējo egoismu. Suverenitāte vairs nav absolūta, kā tas bija Vestfālenes miera laikos, bet gan uz cilvēktiesību ievērošanu vērstas sabiedrības neatņemama daļa.”[[133]](#footnote-133)

42. Galu galā, *RIPA* noteiktā satura nošķiršana jaunā interneta laikmeta kontekstā bija neatbilstoša un palīdzēja vienīgi politiskajam mērķim, proti, leģitimizēt sistēmu Lielbritānijas sabiedrības acīs ar ilūziju, ka Apvienotās Karalistes teritoriālajā jurisdikcijā esošās personas tiks saudzētas no valdības īstenotās kontroles (“Big Brother”). Patiesībā tā tas nebija. Valsts sekretārs, ja viņš vai viņa to uzskatīja par nepieciešamu, varēja noteikt tāda materiāla pārbaudi, kas atlasīts, pamatojoties uz faktoriem, kas attiecas uz personu, kura atradās Britu salās,[[134]](#footnote-134) un izdarīt grozījumus apliecinājumā, lai atļautu atlasīt šīs personas sakarus[[135]](#footnote-135). Turklāt valsts sekretāra orderī nenorādītā iekšējo sakaru piezveja bija atļauta ikreiz, kad tas bija nepieciešams, lai iegūtu ārējos sakarus, uz ko attiecas orderis[[136]](#footnote-136), un, pēc pašas Valdības domām, tas “praksē ir neizbēgami”[[137]](#footnote-137). Ņemot vērā iepriekš minēto, jāatzīmē, ka attiecībā uz saistīto sakaru datu masveida pārtveršanu nebija noteikti pat ārējo sakaru ierobežojumi.

43. Pat ja masveida pārtveršana bija vērsta uz ārvalstu izlūkdatu vākšanu[[138]](#footnote-138), nevis noziegumu novēršanu, atklāšanu un izmeklēšanu[[139]](#footnote-139), tas neattaisnoja regulējuma trūkumu vai pārtverošo iestāžu pilnvaru plašumu. Jebkurā gadījumā digitālo sakaru attīstības rezultātā ārējo sakaru drošības pasākums vairs nefunkcionē kā jēgpilns ierobežojums,[[140]](#footnote-140) ja tas kādreiz tāds ir bijis. Manuprāt, tas nekad tāds nav bijis turpmāk minēto iemeslu dēļ.

44. Valsts sekretārs nesniedza atsevišķu atļauju 8. panta 4. punktā noteiktā ordera izpildei,[[141]](#footnote-141) jo ​​viņa pārtveršanas orderis paredzēja neierobežotu rīcības brīvību, turklāt tajā nebija minēts vai raksturots pārtveršanas subjekts, nebija paredzēts nepārprotams ierobežojums pārtveramo sakaru apmēram un nebija norādīti konkrēti nesēji vai selektori. Neviens īpašs noteikums nereglamentēja gadījumu, kad tika pieprasīti žurnālista, ārsta vai mācītāja sakari vai kad šāda netieša iejaukšanās bija iespējama, izņemot *IC* kodeksa nekaitīgo 4.28.–4.31. punktu.[[142]](#footnote-142) Nesēju izvēle un selektoru, tostarp spēcīgu selektoru, izmantošana ārējiem sakariem bija atkarīga no pārtverošās iestādes galīgā lēmuma.[[143]](#footnote-143) Vienkāršāk sakot, izlūkdienestu kopiena pilnībā kontrolēja atļauju piešķiršanas procedūru, neizpaužot valsts sekretāram svarīgu informāciju, kā rezultātā viņš nevarēja pienācīgi izvērtēt samērīgumu un nepieciešamību, bet tikai politiski piesedza sistēmas darbību.[[144]](#footnote-144)

45. Turklāt valsts sekretāra izdotais prakses kodekss nebija saistošs, ļaujot atkāpties no tajā minētajiem noteikumiem pamatota iemesla dēļ. Situāciju vēl jo vairāk pasliktināja tas, ka analītiķu ikdienas darbu reglamentēja iekšēji regulētie noteikumi, kas nebija pieejami sabiedrībai, pat ne virspusēji vai rediģētā veidā.[[145]](#footnote-145) Šāda pārtverošās iestādes administratīvā rīcības brīvība ir pretrunā ar likumības principa mērķi, saskaņā ar kuru masveida pārtveršanu reglamentējošajiem noteikumiem ir jābūt noteiktiem valsts tiesību aktos, turklāt šim likumam ir jābūt pieejamam un paredzamam attiecībā uz tā sekām.

46. Sistēmas regulējuma nepilnības vēl jo vairāk pasliktināja komisāra sakaru pārtveršanas jautājumos (*IC* komisārs) statuss, kas nebija neatkarīga iestāde un nenodrošināja efektīvu pārtveršanas ordera izpildes pārraudzību.[[146]](#footnote-146) Kā norādīts 2015. gada *ISC* ziņojumā, “lai gan abi komisāri ir bijušie tiesneši, viņi kā komisāri darbojas ārpus oficiālās tiesu sistēmas”, tādēļ secinot, ka “vairāki no šiem pienākumiem pašlaik tiek pildīti bez juridiskām pilnvarām. Tas ir neapmierinoši un nepieņemami.”[[147]](#footnote-147) Un tas attiecībā uz *IC* komisāra statusu vēl nav tas ļaunākais. Saskaņā ar likumu Ministru prezidents iecēla *IC* komisāru, kurš darbojās viņa vai viņas pakļautībā un bija atkarīgs no valsts sekretāra ieceltā personāla.[[148]](#footnote-148) Turklāt tas bija nepilnas slodzes darbs un Ministru prezidents varēja atbrīvot *IC* komisāru no amata jebkurā brīdī.[[149]](#footnote-149) Šis statuss acīmredzami nebija savienojams ar neatkarību, kas nepieciešama, lai efektīvi pārraudzītu 8. panta 4. punktā noteikto režīmu. Īsāk sakot, komisāri nebija “institucionāli, funkcionāli un finansiāli neatkarīgi no iestādēm, kuras viņi [bija] pilnvaroti pārraudzīt”, kā to paredz Tšvānes principi.[[150]](#footnote-150)

47. Pat ja argumentācijas apspriešanas nolūkā varētu pieņemt, ka komisāra īstenotā uzraudzība Apvienotajā Karalistē bija neatkarīga, tā nebija efektīva tā vienkāršā iemesla dēļ, ka, saskaroties ar nopietnu pārkāpumu, komisārs varētu vienīgi par to ziņot Ministru prezidentam, vēršot viņa vai viņas uzmanību uz šo pārkāpumu, un, ja tā, izlemt, cik lielā mērā šo pārkāpumu bija iespējams publiskot.[[151]](#footnote-151) Piemēram, viņš nevarēja ne nodot lietu izskatīšanai *IPT*, ne informēt cietušo par pārmērīgu pārtveršanu. Patiesībā komisārs pat nespēja konstatēt, ka pieteikuma iesniedzēji “Amnesty International” un Dienvidāfrikas Juridisko resursu centrs bija saskārušies ar pretlikumīgu uzraudzību!

48. Pārtveršanas un saglabāšanas periodu ilgumam likumā nebija noteikts maksimālais termiņš, un praksē šis trūkums netika novērsts.[[152]](#footnote-152) 8. panta 4. punktā noteiktos orderus varēja atjaunot *ad aeternum*.[[153]](#footnote-153) Turklāt saglabāšanas periodi dažādām pārtverošajām iestādēm[[154]](#footnote-154) atšķīrās un no “ierastā” maksimālā saglabāšanas termiņa (t. i., divi gadi) saskaņā ar *IC* kodeksa 7.9. punktu varēja atteikties pati pārtverošās iestādes vadošā amatpersona. Šis ir spilgts pierādījums tam, kuram Lielbritānijas masveida pārtveršanas sistēmā bija vadošā loma.[[155]](#footnote-155)

49. Pārtveršanas procesa beigās nebija jāizpilda pienākums par subjekta informēšanu.[[156]](#footnote-156) Ja šāda informēšana netika veikta, tiesības vērsties tiesā lielākoties bija veltīgas. Tā tas bija Apvienotajā Karalistē.[[157]](#footnote-157) *IPT* rīkojās tikai pēc tam, kad bija saņēmusi sūdzību no personas, kura uzskatīja, ka attiecībā uz to veikta slepena uzraudzība, kas nozīmēja, ka *IPT* bija tikai teorētiska garantija visiem tiem pārtveršanas subjektiem, kuriem nebija ne jausmas, ka viņu sakari ir pārtverti.[[158]](#footnote-158) *IPT* nepietiekamo pārraudzību vēl jo vairāk pasliktināja tas, ka tai nebija tiesību vērsties ECT, lai paziņotu par primāro tiesību neatbilstību, jo tā Konvencijas 4. panta izpratnē nebija “tiesa”, turklāt tās nolēmumi nebija pārsūdzami, un dīvainā kārtā valsts sekretāram bija tiesības pieņemt *IPT* procesuālos noteikumus, kas praksē nozīmēja to, ka uzraudzītajai iestādei bija tiesības noteikt noteikumus, kas reglamentē uzraudzības struktūru.[[159]](#footnote-159)

B. Pārtverto datu apmaiņa ar ārvalstu izlūkdienestiem

50. Nav skaidra tiesiskā regulējuma, kas būtu analogs *RIPA* un regulētu pilnvaras, kuras Lielbritānijas valdība var izmantot, lai pārtvertu datus no ārvalstīm. Tikai 2016. gada janvārī *IC* kodeksa 12. nodaļa noteica pamatu šādai apmaiņai.[[160]](#footnote-160) Saskaņā ar *IC* kodeksa 12.5. punktu un tā zemsvītras piezīmi ārvalstu izlūkdienestu pieprasījumus par pārtvertiem sakariem un saistītajiem sakaru datiem var iesniegt attiecībā uz “materiālu uz konkrētiem selektoriem, no tiem un par tiem”.[[161]](#footnote-161) *NSA* atteicās no “par” materiāla apkopošanas 2017. gada aprīlī, jo šādu rīcību tās pārmērīgā apmēra dēļ nevarēja veikt likumīgi.[[162]](#footnote-162) Tomēr Tiesas pārsteidzošā vēlme pieņemt atbildētājas Valdības “apkopojiet visu” politiku[[163]](#footnote-163) pārsniedz pat *NSA* pilnvaras, pieļaujot ne tikai “par” apkopošanas pieprasījumus, bet pat pieprasījumus par tādu materiālu, kas nav saistīts ar konkrētiem selektoriem.[[164]](#footnote-164)

51. Tiesa uzskata, ka attiecībā uz masveida materiāla pārsūtīšanu ārvalstu izlūkošanas partneriem ir jāveic “neatkarīga kontrole,[[165]](#footnote-165), bet ne attiecībā uz ārvalstu izlūkošanas iestāžu apkopoto materiālu[[166]](#footnote-166). Ja drošības pasākumi saistībā ar Apvienotās Karalistes pārtverošo iestāžu veikto tiešo uzraudzību ir neatbilstoši, tie būtu jāuzskata par neatbilstošiem arī to veiktajai netiešajai uzraudzībai, kas izriet no trešo personu pārtvertā materiāla izlūkdatu apmaiņas, vēl jo vairāk, ja šādu materiālu apkopo trešā persona, kurai Konvencija nav saistoša. Ja pastāv lielāks risks, ka materiāls tiks apkopots un uzglabāts pretēji Konvencijā noteiktajam, un tāpēc ir visvairāk nepieciešama neatkarīga pārraudzība, Tiesa ir atteikusies no šī drošības pasākuma bez jebkāda pienācīga pamatojuma.[[167]](#footnote-167) Šajā ziņā *IC* komisāra un *IPT* īstenotā pārraudzība, uz kuru atsaucās Valdība un Lielās palātas vairākums, bija praktiski neefektīva, ko varēja novērot, gan kontrolējot trešās personas pārtvertā materiāla izlūkdatu apmaiņu, gan pārraugot valsts līmeņa uzraudzību, jo *IPT* iejaucās vienīgi tad, ja bija iesniegta sūdzība, savukārt *IC* komisāram nebija citu pilnvaru, kā vien iesniegt ziņojumu Ministru prezidentam, lai vērstu viņa vai viņas uzmanību uz kādu nopietnu pārkāpumu.

52. Vairākuma argumentācijas absurdās sekas ir vēl acīmredzamākas šādā piemērā, proti, ja viens londonietis vietnē “Twitter” nosūta ziņu kādam citam londonietim un šī ziņa tiek pārraidīta, izmantojot serveri ASV, Tiesa atzīst, ka, Valdības komunikāciju galvenajai pārvaldei (*GCHQ*) pārtverot šo ziņu un saistītos sakaru datus, kad tā atstāj Apvienoto Karalisti pa kabeli, kas ved uz Amerikas Savienotajām Valstīm, ir jāgarantē atsevišķa atļauja. Taču, ja *NSA* pārtver to pašu ziņu tā paša kabeļa otrā galā un pēc tam nodod kopiju *GCHQ* vai ar to saistītos sakaru datus, garantija par atsevišķu atļauju nav piemērojama. Šāda rīcība ir pilnībā patvaļīga, ja tiem pašiem datiem tiek noteikta atšķirīga tiesiskā aizsardzība, pamatojoties vienīgi uz tās iestādes nejaušo atrašanās vietu, kura ir veikusi sākotnējo pārtveršanu. Tas, ka nav drošības pasākumu sistēmas no ārvalstīm pārtvertu datu izmantošanai, kas paredz tādus pašus aizsardzības mehānismus kā tā, ko piemēro mītnes valstī savākto datu pārtveršanai, nozīmē, ka Apvienotās Karalistes tiesību akti nav atbilstoši tam, lai nodrošinātu aizsardzību pret patvaļu un ļaunprātību.[[168]](#footnote-168)

53. Turklāt saskaņā ar *IC* kodeksa 12.6. punktu *RIPA* 15. un 16. pants neattiecās uz visiem materiāliem, kas saņemti no ārvalstu izlūkdienestiem un kas varētu būt iegūti masveida pārtveršanas veidā, bet gan vienīgi uz pieprasīto pārtveršanas materiālu vai “ja tas pats par sevi liecinājis par pārtveršanu”, kas saņēmējas valsts (Apvienotās Karalistes) iekšējo garantiju sistēmu padarīja atkarīgu no ārvalstu izlūkdienestu lēmuma.

54. Ar citām pusēm veiktās masveida materiāla apmaiņas izvērtējums būtu nepilnīgs, ja netiktu minēta vēl viena būtiska iezīme. Jāpiebilst, ka *IC* kodeksa 7.3. punkts ļāva pārtverto materiālu izpaust citām pusēm tikai tādēļ vien, ka tas bija ērti, kas ir pārsteidzoši vienkāršots kritērijs. “Nepieciešamības zināt princips”[[169]](#footnote-169) ir loģisks pretstats nepieciešamības un proporcionalitātes izvērtējumam, proti, princips, kas paredz, ka var atklāt tikai tik daudz pārtveramā materiāla, cik nepieciešams saņēmējam, ir pretstatā šādam izvērtējumam. Šādu izpaušanas pilnvaru īstenošanu nereglamentē konkrēta likumā noteikta prasība, bet gan nosaka, iespējams, maldīgi, vienīgi izvirzītais nolūks. Tādējādi papildu iejaukšanās personas tiesībās, kam par pamatu bija pārtvertā materiāla izpaušana citām pusēm, attiecībā uz tās nepieciešamību un samērīgumu vērtēta savtīgos nolūkos. Vienkāršāk sakot, indivīda sakari tiek uztverti kā valsts īpašums, prece, ar ko valsts pēc saviem ieskatiem var dalīties ar citām pusēm, lai “noskaidrotu, vai siena kaudzē atrodama adata”.[[170]](#footnote-170)

C. Saistīto sakaru datu masveida pārtveršana

55. Visbeidzot, *RIPA* 16. panta 2. punkts neattiecās uz saistīto sakaru datu masveida pārtveršanu, kas nozīmēja to, ka jebkurš analītiķis varēja izmantot spēcīgu selektoru, kas attiecas uz personu, par kuru zināms, ka tā atrodas Britu salās, bez nepieciešamības saņemt attiecīgo valsts sekretāra izdoto apliecinājumu, un, kas ir vēl ļaunāk, pārtvertos datus var saglabāt “vairākus mēnešus”, ja nepieciešams, un tik ilgi, cik nepieciešams, lai atklātu “vēl nezināmo”.[[171]](#footnote-171) Praktiskā ziņā saistīto sakaru datu pārtveršanu un apstrādi ierobežoja vienīgi pārtveršanas pakalpojumu ietilpība. Patiesībā *RIPA* īsti neregulē ārvalstu izlūkdatu vākšanas varu, jo tehnoloģiju attīstības rezultātā tā ir pārtapusi par valsts līmeņa uzraudzības varu, tāpēc Valdība tagad uzskata, ka Britu salu drošības pasākumi, kas paredzēti *RIPA* 16. pantā, nav “nepieciešami”, lai nodrošinātu atbilstību Konvencijai.[[172]](#footnote-172)

56. Arī mani Valdības arguments[[173]](#footnote-173) par šādu iespējamību nepārliecina. Tiesnesis netraucēti noteiktajā kārtībā var izvērtēt, cik lielā mērā pieprasījums atļaujas piešķiršanai ir nepieciešams un samērīgs, lai katrā atsevišķā gadījumā iegūtu ar kādu personu saistītus sakaru datus, neradot nopietnu risku to izmantošanai.[[174]](#footnote-174) Ja šo atļaujas piešķiršanas procesu iespējams vērst uz žurnālistiem un citiem speciālistiem, kuru saistītie sakaru dati ir juridiski aizsargāti, kā to atzinusi Tiesa,[[175]](#footnote-175) kāpēc to nevarētu vērst uz “parasto mirstīgo” sakaru datiem? Šādas plaša mēroga apstiprināšanas sistēmas ir pilnīgi iespējamas. Galvenā ideja ir tāda, ka attiecībā uz plaša mēroga iejaukšanos tiesībās uz privātās dzīves neaizskaramību ir jānodrošina plaša mēroga drošības pasākumu sistēma.

57. Neskatoties uz tās ierobežojošo ietekmi gan Britu salās, gan ārpus tām, Tiesas iecietība pret šādu praksi nav saprotama, ņemot vērā, ka pati Tiesa uzskata 16. panta 2. punktu par “galveno likumā noteikto drošības pasākumu, kas ierobežo kārtību, kādā pārtverto materiālu atlasa pārbaudei”.[[176]](#footnote-176)

D. Sākotnējais secinājums

58. Kopumā faktam, ka spriedumos lietās “Vēbere un Sarāvija” (2006) un ““Liberty” un citi” (2008) izvērtētās uzraudzības darbības joma bija daudz šaurāka nekā pašlaik, nav jābūt par pamatu tam, lai Tiesa ieņemtu mazāk stingru nostāju attiecībā uz nepieciešamo aizsardzības līmeni, kas pašlaik jānodrošina tiesībām uz privātās dzīves neaizskaramību. Ņemot vērā uzraudzības darbību eksponenciālo pieaugumu pēdējo desmit gadu laikā un sabiedrības sašutumu, ko tas izraisījis, ir nepieciešama stingrāka izlūkdienestu darbības pārraudzība, lai saglabātu demokrātiju un aizstāvētu tiesiskumu. Nevis otrādi. Palielinoties valsts pilnvaru ļaunprātīgas izmantošanas riskam, ir jāpalielina, nevis jāsamazina Konvencijā paredzētie drošības pasākumi un atbilstošās valsts tiesību aktos noteiktās garantijas.[[177]](#footnote-177) Citiem vārdiem, Tiesas standartiem pašlaik jābūt stingrākiem nekā 2006. vai 2008. gadā. Tas ir tieši pretēji tam, kas noteikts ar šo spriedumu. Šajā spriedumā Tiesa ir piekāpusies vispārējas masveida pārtveršanas *fait accompli*, bīstami pieņemot, ka, ja tas ir lietderīgi, tas ir pieļaujami. Demokrātiskā sabiedrībā lietderība nav tas pats, kas nepieciešamība un samērīgums. Kā tiesnesis Brendeizs [*Brandeis*] norādījis spriedumā lietā “Olmsteds [*Olmstead*] pret Amerikas Savienotajām Valstīm”,[[178]](#footnote-178) “tāpat nav nozīmes tam, ka [telefona noklausīšanās] iejaukšanās notikusi tiesībaizsardzības nolūkā. Pieredzei mums jāiemāca būt visnotaļ piesardzīgiem, lai aizsargātu brīvību, ja valdības mērķi ir labvēlīgi.”

V. SECINĀJUMI

59. Šis spriedums būtiski maina Eiropā pastāvošo līdzsvaru starp tiesībām uz privātās dzīves neaizskaramību un sabiedrības drošības interesēm, jo tas pieļauj nemērķētu elektronisko sakaru un saistīto sakaru datu uzraudzību un, vēl ļaunāk, datu apmaiņu ar trešām valstīm, kurās nav līdzvērtīgu aizsardzības mehānismu tiem, kādi ir Eiropas Padomes valstīs. Šāds secinājums ir vēl jo vairāk pamatots, ņemot vērā EST kategorisko iebildumu par vispārinātu piekļuvi elektroniskajiem sakariem,[[179]](#footnote-179) tās acīmredzamo nevēlēšanos pieļaut vispārēju un neselektīvu datplūsmas datu un atrašanās vietas datu saglabāšanu[[180]](#footnote-180) un datu apmaiņas ierobežošanu ar ārvalstu izlūkdienestiem, kas nenodrošina aizsardzības līmeni, kāds būtībā ir līdzvērtīgs tam, ko garantē Pamattiesību harta[[181]](#footnote-181). Visos šajos trīs aspektos Strasbūras tiesa atpaliek no Luksemburgas tiesas, kurai ir vadošā loma, aizsargājot tiesības uz privātās dzīves neaizskaramību Eiropā.

60. Izšķiroties starp šā sprieduma pozitīvo un negatīvo ietekmi, un es vairāk nosliecos uz negatīvu ietekmi, ar šo spriedumu Strasbūras tiesa ir pavērusi iespēju elektroniskai valsts īstenotai kontrolei Eiropā. Ja šī ir jaunā norma, ko manu izglītoto kolēģu vairākums vēlas panākt Eiropā, es viņiem nevaru pievienoties, un man ar smagu sirdi un Gregorio Allegri vārdiem jāatzīst: *Miserere mei, Deus* jeb “Dievs, apžēlojies!”

TIESNEŠU LEMENSA, VEHABOVIČA, RANCONI UN BOŠŅAKA KOPĪGAIS DAĻĒJI NEPIEKRĪTOŠAIS VIEDOKLIS

1. Mēs piekrītam šim spriedumam, izņemot saskaņā ar Konvencijas 8. un 10. pantu iesniegtās sūdzības izvērtējumu par to, ka atbildētājas valsts iestādes ir saņēmušas pieprasīto pārtverto materiālu no ārvalstu izlūkdienestiem (skat. šā sprieduma rezolutīvās daļas 3. un 5. punktu).

2. Šajā spriedumā tāpat kā šodien pasludinātajā spriedumā lietā ““Centrum för rättvisa” pret Zviedriju” (pieteikums Nr. 35252/08) masveida pārtveršanas režīmiem Lielā palāta ir noteikusi efektīvu “no gala līdz galam” drošības pasākumu sistēmu, kurā ir trīs galvenie pīlāri jeb stūrakmeņi, lai samazinātu šādu pilnvaru ļaunprātīgas izmantošanas risku. Šie galvenie pīlāri ir šādi: 1) masveida pārtveršanas atļaujas sniegšana jau pašā sākumā, kad no izpildvaras neatkarīga struktūra precizē operācijas mērķi un apmēru; 2) iepriekšēja iekšēja atļauja tad, kad tiek izmantoti spēcīgie selektori, kas saistīti ar identificējamām personām, un 3) neatkarīgas iestādes veikta operācijas pārraudzība līdzās *post facto* pārskatīšanai, ko veic no izpildvaras neatkarīga struktūra (skat. sprieduma 350.–359. punktu).

3. Tie paši “no gala līdz galam” drošības pasākumi, kas noteikti masveida pārtveršanas režīmam, jāpiemēro arī režīmam, kurā iestādes pašas nepārtver pārrobežu sakarus un saistītos sakaru datus, bet gan lūdz ārvalstu izlūkdienestus pārtvert šādus datus vai pārraidīt jau pārtvertos datus. Tomēr, lai gan, saņemot pārtverto materiālu, drošības pasākumi tā pārbaudei, izmantošanai un uzglabāšanai, tālākai pārraidei, kā arī dzēšanai un iznīcināšanai ir piemērojami vienādi (skat. sprieduma 498. punktu), pirmais pīlārs, proti, iepriekšēja neatkarīga atļauja, pēc vairākuma domām, pilnībā izzūd. Vairākuma argumentācija šajā ziņā mūs nepārliecina. Kāpēc jānošķir veids, kādā dati nonākuši iestāžu rīcībā, un tas, vai tās datus ir pārtvērušas pašas vai arī to uzdevušas veikt kādai ārvalstu iestādei? Līdz ar to, mūsu ieskatā, arī attiecībā uz pirmo pīlāru jāpiemēro tie paši drošības pasākumi, kas noteikti attiecībā uz masveida pārtveršanu.

4. Mēs varam pilnībā pievienoties Tiesas sprieduma 496. un 497. punktā sniegtajam izvērtējumam, jo īpaši tam, ka iejaukšanās 8. pantā noteiktajās tiesībās jau ir paredzēta sākotnējā pieprasījumā ārvalstu iestādēm un ka Konvencijā paredzētie aizsardzības mehānismi būtu neefektīvi, ja valstis varētu apiet savus Konvencijā noteiktos pienākumus, pieprasot datus no valstīm, kuras nav līgumslēdzējas valstis. Tāpēc dalībvalstīs ir jābūt ieviestiem skaidriem un detalizētiem noteikumiem, kas paredz efektīvu aizsardzību pret to pilnvaru ļaunprātīgu izmantošanu, lai apietu attiecīgās valsts tiesību aktus un/vai tās pienākumus, kas noteikti Konvencijā.

5. Vienīgais, par ko mēs, vienlaicīgi cienot kolēģu nostāju, nepiekrītam vairākumam, ir jautājums par to, ko uzskata par “efektīvām garantijām”.

6. Vairākums vispirms atsaucies uz faktu, ka pieprasījumi bija vai nu balstīti uz valsts sekretāra jau atļautiem, vai arī konkrēti apstiprinātiem orderiem (skat. sprieduma 505. punktu). Tomēr mēs iebilstam, ka valsts sekretārs nav neatkarīgs no izpildvaras un ka šajā ziņā režīmam, kas regulē izlūkdatu saņemšanu no ārvalstu izlūkdienestiem, ir raksturīgs tāds pats trūkums kā masveida pārtveršanas režīmam (skat. sprieduma 377. punktu).

7. Otrkārt, vairākums, šķiet, ir pieņēmis, ka valsts tiesību akti, kas aizliedz jebkādu noteikumu apiešanu, ir efektīvs drošības pasākums (skat. sprieduma 506. punktu). Visu cieņu, taču mēs tam nepiekrītam. Kā norādīts iepriekš, piemēram, tiesneša Ranconi atsevišķajā viedoklī spriedumā lietā “Breiers [*Breyer*] pret Vāciju ” (pieteikums Nr. 50001/12, 2020. gada 30. janvāris), valsts tiesību aktos ir noteikts vienīgi juridiskais pamats, kas paredz iejaukšanās likumību; tas papildus un pats par sevi nav efektīvs drošības pasākums, lai aizsargātu personu pret valsts tiesību aktu patvaļīgu piemērošanu, ko veic valsts iestādes, un no pilnvaru ļaunprātīgas izmantošanas. Šādai aizsardzībai ir jābūt plašākai par tiesību normām, jo īpaši tad, kad šīs normas un juridiskās pilnvaras ir formulētas plaši.

8. Citiem vārdiem, tiesību normu, kas aizliedz apiešanu vai pilnvaru cita veida ļaunprātīgu izmantošanu, vienlaicīgi nevar uzskatīt par drošības pasākumu aizsardzībai pret šādu rīcību. Efektīvs drošības pasākums paredz tāda mehānisma pieejamību, kas spēj nodrošināt šīs normas pareizu piemērošanu. Tomēr šāda veida drošības pasākumu trūkst attiecībā uz pieprasījumiem, ar kuriem ārvalstu izlūkdienestiem ir prasīts pārtvert un pārsūtīt datus. Mūsuprāt, tāpat kā masveida pārtveršanas režīmā, pirmais pīlārs līdzīgi jāpiemēro “no gala līdz galam” drošības pasākumiem. Līdz ar to jebkuram šādam pieprasījumam ir nepieciešama iepriekšēja atļauja no kādas neatkarīgas struktūras, kas spēj novērtēt, vai šāda rīcība ir nepieciešama un samērīga ar izvirzīto mērķi (skat. sprieduma 350. un 351. punktu), un nodrošināt, ka šīs pilnvaras netiek izmantotas, lai apietu valsts tiesību aktus un/vai pienākumus, kas noteikti Konvencijā.

9. Šo iemeslu dēļ mēs esam balsojuši pret atzinumu, ka nav pārkāpts Konvencijas 8. pants attiecībā uz izlūkdatu saņemšanu no ārvalstu izlūkdienestiem.

10. Tā kā vairākums ir secinājis, ka ar izlūkdatu apmaiņas režīmu nav pārkāpts Konvencijas 10. pants, pamatojoties uz tiem pašiem iemesliem, kas viņiem ļāva secināt, ka nav pārkāpts Konvencijas 8. pants (skat. sprieduma 516. punktu), mēs nepiekrītam tā secinājumiem saskaņā ar 10. pantu.

PAPILDINĀJUMS

**Lietas dalībnieku saraksts**

|  |  |
| --- | --- |
| Pieteikuma Nr.  | Lietas dalībnieki |
| 58170/13 | “Big Brother Watch” |
| 58170/13 | “English PEN” |
| 58170/13 | “Open Rights Group” |
| 58170/13 | Dr. Konstance Kurca [*Constanze Kurz*] |
| 62322/14 | Pētnieciskās žurnālistikas birojs |
| 62322/14 | Alise Rosa [*Alice Ross*] |
| 24960/15 | “Amnesty International Limited” |
| 24960/15 | “Bytes For All” |
| 24960/15 | Nacionālā Pilsoņu brīvību padome (“Liberty”) |
| 24960/15 | “Privacy International” |
| 24960/15 | Amerikas Pilsoņu brīvību savienība |
| 24960/15 | Kanādas Pilsoņu brīvību asociācija |
| 24960/15 | Ēģiptes Personas tiesību iniciatīva |
| 24960/15 | Ungārijas Pilsoņu brīvību savienība |
| 24960/15 | “The Irish Council For Civil Liberties Limited” |
| 24960/15 | Juridisko resursu centrs |

1. Visi pārējie 12.2. punktā minētie pieprasījumi (ar attiecīgo *RIPA* noteikto pārtveršanas orderi vai bez tā) tiks iesniegti saistībā ar materiālu, kas paredzēts konkrētiem selektoriem, no tiem izriet vai tos raksturo (līdz ar to attiecas uz konkrētu personu vai personām). Šādos apstākļos valsts sekretārs jau būs apstiprinājis pieprasījumu par konkrēto(-ām) personu(-ām), kā noteikts (sic) punktos. 12.2. [↑](#footnote-ref-1)
2. Pirms Apvienotā Karaliste izstājās no Eiropas Savienības, tā 2018. gada 23. maijā sniedza karalisko piekrišanu 2018. gada Datu aizsardzības likumam [*Data Protection Act 2018*], kas paredz tādus pašus noteikumus un aizsardzības pasākumus. [↑](#footnote-ref-2)
3. Ruth Gavison (1980), “Privacy and the Limits of Law”, *Yale Law Journal* 89, p. 347. [↑](#footnote-ref-3)
4. Jeffrey Reiman (1995), “Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Technology of the Future”, *Santa Clara High Technology Law Journal* 11:1, p. 42. [↑](#footnote-ref-4)
5. George Orwell (2008), *Nineteen Eighty-Four* (London: Penguin), pp. 4–5. [↑](#footnote-ref-5)
6. Daniel Solove (2008), *Understanding Privacy* (Cambridge, MA: Harvard University Press), p. 98. [↑](#footnote-ref-6)
7. Spriedums lietā “Osborns [*Osborn*] pret Amerikas Savienotajām Valstīm” 385 U.S. 323 (1966). [↑](#footnote-ref-7)
8. Skat., piemēram, Eiropas Padomes Parlamentārās asamblejas rekomendāciju Nr. 1402(1999) par iekšējās drošības dienestu kontroli Eiropas Padomes dalībvalstīs [*Recommendation 1402 (1999) of the Parliamentary Assembly of the Council of Europe on the control of internal security services in Council of Europe member states*], jo īpaši A pamatnostādnes ii) punktu. Šī rekomendācija attiecas uz iekšējās drošības dienestu darbību, taču tā, mūsuprāt, ideāli attiecināma arī uz ārvalstu izlūkdienestiem. [↑](#footnote-ref-8)
9. Šī ir otrā reize, kad es paužu atsevišķu viedokli par masveida pārtveršanu. 2016. gada 12. janvāra sprieduma lietā Nr. 37138/14 “Zabo un Visija pret Ungāriju” man bija iespēja paust savus uzskatus par Ungārijas masveida pārtveršanas režīma bīstamo ceļu un nevēlamajām sekām šī ceļa galā. Ņemot vērā Lielajā palātā notikušo apspriedi un rūpīgi izvērtējot visus pretrunīgos argumentus, es varu apstiprināt, ka mana nostāja šajā jautājumā nav mainījusies. Patiesībā es pašlaik esmu guvis vēl lielāku pārliecību, ka mani 2016. gadā izklāstītie secinājumi diemžēl ir aktuāli līdz pat šim brīdim. Tādēļ šis viedoklis ir jāizvērtē, to lasot kopā ar secinājumiem, kurus es izklāstīju pirms pieciem gadiem. [↑](#footnote-ref-9)
10. Šī paraugprakse ir izklāstīta, piemēram, 2015. gada 27. janvāra spriedumā lietā Nr. 59552/08 “Rohlens [*Rohlena*] pret Čehijas Republiku” [*GC*]. [↑](#footnote-ref-10)
11. Valsts tiesību aktos definētais jēdziens ir līdzīgs. Skat. *RIPA* 20. pantu. [↑](#footnote-ref-11)
12. Valsts tiesību aktos definētais jēdziens ir atšķirīgs. Skat. *RIPA* 20. pantu. [↑](#footnote-ref-12)
13. Valsts tiesību aktos definētais jēdziens ir ierobežotāks. Skat. *RIPA* 20. pantu. 21. panta 4., 6. un 7. punktā ir definēts jēdziens “sakaru dati”. [↑](#footnote-ref-13)
14. Šis jēdziens ir līdzīgs *RIPA* 20. pantā definētajam jēdzienam. [↑](#footnote-ref-14)
15. Šis jēdziens ir ietverts *RIPA* 81. pantā, ko var izmantot arī Tiesa. [↑](#footnote-ref-15)
16. Šā sprieduma 323. punkts. [↑](#footnote-ref-16)
17. Šā sprieduma 33. un 50. punkts. [↑](#footnote-ref-17)
18. Šā sprieduma 136. punkts. [↑](#footnote-ref-18)
19. Šā sprieduma 424. punkts. [↑](#footnote-ref-19)
20. Šā sprieduma 353. punkts. [↑](#footnote-ref-20)
21. Šā sprieduma 354. punkts. [↑](#footnote-ref-21)
22. “Liberty and Security in a Changing World”, Report and Recommendations of the President’s Review Group on Intelligence and Communications Technologies, 12 December 2013, p. 114. [↑](#footnote-ref-22)
23. Spriedums lietā ““Centrum för rättvisa” pret Zviedriju” (Nr. 35252/08), pasludināts tajā pašā dienā, kad tika pasludināts šis spriedums. Ir noprotams, ka Francijas, Nīderlandes un Norvēģijas valdības balstījušās tieši uz šo aspektu; tās norādīja, ka nebija pamata attiecībā uz masveida pārtveršanu papildus paredzēt prasību par pamatotām aizdomām (šā sprieduma 301., 305. un 309. punkts). [↑](#footnote-ref-23)
24. Skat. atbildētājas Valdības mutvārdu argumentus Lielās palātas 2019. gada 10. jūlija sēdē: “Tās [prasības par pamatotām aizdomām un turpmāku informēšanu] būtībā neatbilst režīma darbībai, kas nav atkarīga no skaidri definētu uzraudzības mērķu esības. 8. panta 4. punktā noteiktais režīms pēc būtības ir nemērķēts režīms. Tas ir ieviests, lai atklātu vēl nezināmus valsts drošības un smagu noziegumu draudus. Līdz ar to tas vienkārši nav sasaistāms ar pamatotām aizdomām. Šāda prasība izkropļotu tā lietderību (..).” Galu galā, argumenta pamatā ir uz aizdomām nebalstītas masveida pārtveršanas “lietderība”. [↑](#footnote-ref-24)
25. Šā sprieduma 348. punkts. [↑](#footnote-ref-25)
26. ““Liberty” un citi pret Apvienoto Karalisti”, Nr. 58243/00, 63. punkts, 2008. gada 1. jūlijs. [↑](#footnote-ref-26)
27. “Vēbere un Sarāvija pret Vāciju” (lēmums), Nr. 54934/00, 95. un 114. punkts, ECT 2006-XI. [↑](#footnote-ref-27)
28. ““Liberty” un citi”, minēts iepriekš, 63.–65. punkts. [↑](#footnote-ref-28)
29. “Kenedijs pret Apvienoto Karalisti”, Nr. 26839/05, 158.–160. punkts, 2010. gada 18. maijs. [↑](#footnote-ref-29)
30. “Romāns Zaharovs pret Krieviju” [*GC*], Nr. 47143/06, 231. un 264. punkts, ECT 2015. [↑](#footnote-ref-30)
31. “Zabo un Visija pret Ungāriju”, minēts iepriekš. [↑](#footnote-ref-31)
32. “Mustafa Sezgins Tanrikulu pret Turciju”, Nr. 27473/06, 2017. gada 18. jūlijs. [↑](#footnote-ref-32)
33. “Romāns Zaharovs”, minēts iepriekš, 231. un 264. punkts. [↑](#footnote-ref-33)
34. Turpat, 175.–178. punkts. [↑](#footnote-ref-34)
35. Turpat, 31. punkts un 246.–248. punkts. [↑](#footnote-ref-35)
36. Turpat, 265. punkts. Lietas attiecībā uz “teritorijas uzraudzības” atļauju pavisam noteikti bija saistītas ar iespējamu masveida uzraudzību. [↑](#footnote-ref-36)
37. “Zabo un Visija pret Ungāriju”, minēts iepriekš. [↑](#footnote-ref-37)
38. Turpat, 67. punkts. [↑](#footnote-ref-38)
39. Turpat, 63. punkts. [↑](#footnote-ref-39)
40. Turpat, 71. punkts. [↑](#footnote-ref-40)
41. Turpat, 56. punkts. [↑](#footnote-ref-41)
42. “Mustafa Sezgins Tanrikulu pret Turciju”, minēts iepriekš, 56. un 57. punkts. [↑](#footnote-ref-42)
43. Šā sprieduma 341. punkts. Šajā prasībā nav ņemti vērā spriedumi lietās “Romāns Zaharovs” un “Zabo un Visija”, kā norādīts iepriekš. [↑](#footnote-ref-43)
44. Šā sprieduma 344.–346. punkts. [↑](#footnote-ref-44)
45. Šā sprieduma 344. punkts. [↑](#footnote-ref-45)
46. Šo dokumentu detalizēts izvērtējums sniegts manos secinājumos spriedumā iepriekš minētajā lietā “Zabo un Visija”. [↑](#footnote-ref-46)
47. UN doc. CCPR/C/GBR/CO/7. [↑](#footnote-ref-47)
48. CommDH (2016)20. [↑](#footnote-ref-48)
49. “Zabo un Visija”, minēts iepriekš, 66. punkts: “Praktiski iespējams, ka Ungārijā slepeni tiek uzraudzīta ikviena persona.” [↑](#footnote-ref-49)
50. “Mustafa Sezgins Tanrikulu”, minēts iepriekš, 7. punkts. [↑](#footnote-ref-50)
51. Šā sprieduma 209.–241. punkts. Es šeit atsaucos uz spriedumiem lietās “Digital Rights Ireland Ltd” (par Datu saglabāšanas direktīvu 2006/24/EK, ar ko “rada iejaukšanos gandrīz visu Eiropas iedzīvotāju pamattiesībās”), “Maksimillians Šrēmss” (kritizēts tiesiskais regulējums, saskaņā ar kuru valsts iestādēm “vispārīgi tiek ļauts piekļūt elektroniskiem sakariem”), “Privacy International” (par valsts tiesisko regulējumu, kas uzliek elektronisko sakaru pakalpojumu sniedzējiem par pienākumu izpaust datplūsmas datus un atrašanās vietas datus izlūkošanas aģentūrām, veicot visaptverošu un neselektīvu pārsūtīšanu, kas ietekmē “visas personas, kuras izmanto elektronisko sakaru pakalpojumus”) un ““La Quadrature du Net” un citi” (nopelti tiesību akti, kas prasa pakalpojumu sniedzējiem “visaptveroši un neselektīvi” saglabāt datplūsmas datus un atrašanās vietas datus). Pirmās divas lietas attiecās uz personas datu apstrādi tiesībaizsardzības nolūkos, savukārt pēdējās divas – uz izlūkdienestu veiktās slepenās uzraudzības izvērtējumu. [↑](#footnote-ref-51)
52. Skat. turpmāk pilnu izvērtējumu par teritoriālās jurisdikcijas nespēju atšķirt iekšējos un ārējos sakarus, lai attaisnotu izlūkdienestu veikto masveida pārtveršanu. [↑](#footnote-ref-52)
53. Skat. atbildētājas Valdības 2019. gada 2. maija apsvērumus Lielajā palātā, 42. lpp. (“daudzi tūkstoši vienas nedēļas laikā attiecībā uz personām, par kurām bija zināms vai tika uzskatīts, ka tās atrodas Apvienotajā Karalistē”). [↑](#footnote-ref-53)
54. Šā sprieduma 345. punkts. [↑](#footnote-ref-54)
55. Turpat. [↑](#footnote-ref-55)
56. Jānorāda, ka Francijas un Nīderlandes valdība tāpat kā palāta uzstāja, ka nav pareizi pieņemt, ka masveida pārtveršana rada lielāku iejaukšanos personas tiesībās uz privātās dzīves neaizskaramību nekā mērķēta pārtveršana (šā sprieduma 300. un 306. punkts). [↑](#footnote-ref-56)
57. Kā secināts Tiesas pētījuma ziņojumā par Albāniju, Andoru, Austriju, Beļģiju, Bosniju un Hercegovinu, Horvātiju, Čehijas Republiku, Grieķiju, Īriju, Islandi, Itāliju, Lihtenšteinu, Moldovu, Monako, Melnkalni, Ziemeļmaķedoniju, Poliju, Portugāli, Rumāniju, Sanmarīno, Serbiju, Turciju un Ukrainu. Līdz ar to sprieduma 242.–246. punktā nav precīzi raksturota situācija Eiropā. [↑](#footnote-ref-57)
58. *PACE* rezolūcija 2031 (2015). [↑](#footnote-ref-58)
59. Council of Europe Human Rights Commissioner’s Memorandum on Surveillance and Oversight Mechanisms in the United Kingdom, CommDH (2016)20, May 2016, p. 10. [↑](#footnote-ref-59)
60. Šā sprieduma 242. punkts. [↑](#footnote-ref-60)
61. Šā sprieduma 345. punkts. Es šeit atsaucos uz kritiku, ko EST vērsusi pret jēdzienu “smags noziegums” (skat. šā sprieduma 212. punktu). [↑](#footnote-ref-61)
62. Skat. Venēcijas komisijas 2015. gada Ziņojumu par sakaru izlūkošanas aģentūru demokrātisku pārraudzību, 9., 25. un 26. lpp. (“jābūt konkrētiem faktiem, kas norāda uz noziedzīgu nodarījumu/drošību apdraudošu rīcību, un izmeklētājiem ir jābūt “iespējamam iemeslam”, “pamatotām aizdomām” vai līdzīgam uzskatam”) un iepriekš minēto Eiropas Padomes cilvēktiesību komisāra Memorandu, 6. lpp. [↑](#footnote-ref-62)
63. Šā sprieduma 346. punkts. [↑](#footnote-ref-63)
64. Kā EST norādījusi sava sprieduma iepriekš minētajā lietā “Digital Rights Ireland” 55. punktā, “nepieciešamība pēc .. drošības pasākumiem ir lielāka tad, ja .. tiek veikta personas datu automātiska apstrāde”. [↑](#footnote-ref-64)
65. Tiesas izvērtējuma c) apakšpunkta iii) iedaļa. [↑](#footnote-ref-65)
66. Šā sprieduma 348. punkts. [↑](#footnote-ref-66)
67. Turpat. [↑](#footnote-ref-67)
68. Piemērs izriet no EST judikatūras (skat. šā sprieduma 220. punktu). [↑](#footnote-ref-68)
69. Piemērs izriet no asās kritikas, kas Eiropas Parlamenta 2014. gada 12. marta rezolūcijā vērsta pret ASV *NSA* uzraudzības programmu, iepriekš minētā Venēcijas komisijas ziņojuma, 18. lpp., un iepriekš minētā Eiropas Padomes cilvēktiesību komisāra Memoranda, 8. lpp. [↑](#footnote-ref-69)
70. “Zabo un Visija”, minēts iepriekš, 71. punkts. [↑](#footnote-ref-70)
71. “Romāns Zaharovs”, minēts iepriekš, 260., 262. un 263. punkts. [↑](#footnote-ref-71)
72. Šā sprieduma 348. punkts. [↑](#footnote-ref-72)
73. Šā sprieduma 330. punkts. [↑](#footnote-ref-73)
74. Šā sprieduma 350. punkts. [↑](#footnote-ref-74)
75. Turpat. [↑](#footnote-ref-75)
76. Turpat. [↑](#footnote-ref-76)
77. Šā sprieduma 351. punkts. [↑](#footnote-ref-77)
78. Šā sprieduma 352. punkts. [↑](#footnote-ref-78)
79. Šā sprieduma 355. punkts. [↑](#footnote-ref-79)
80. Turpat. [↑](#footnote-ref-80)
81. Šā sprieduma 356. punkts. [↑](#footnote-ref-81)
82. Šā sprieduma 359. punkts [↑](#footnote-ref-82)
83. Šā sprieduma 350. punkts. [↑](#footnote-ref-83)
84. Šā sprieduma 348. punkts. [↑](#footnote-ref-84)
85. Šā sprieduma 360. punkts. [↑](#footnote-ref-85)
86. Skat., piemēram, šā sprieduma 370. punktu *in fine*. [↑](#footnote-ref-86)
87. Lai gan Tiesas valoda nav konsekventa, ņemot vērā, ka tā dažkārt atsaucas uz neatkarīgas iestādes jēdzienu, bet citreiz uz neatkarīgas struktūras jēdzienu, šķiet, ka starp šiem jēdzieniem nav būtiskas atšķirības. [↑](#footnote-ref-87)
88. Šā sprieduma 352. punkts. [↑](#footnote-ref-88)
89. Šā sprieduma 354. punkts. [↑](#footnote-ref-89)
90. Šā sprieduma 355. punkts. [↑](#footnote-ref-90)
91. Turpat. Kā norādīts iepriekš minētajā Venēcijas komisijas ziņojumā, 28. lpp., “iekšējie kontroles pasākumi nav pietiekami”. Līdz ar to sprieduma 199. punktā ir kļūdaini interpretēta Venēcijas komisijas nostāja. [↑](#footnote-ref-91)
92. Šā sprieduma 356. punkts. [↑](#footnote-ref-92)
93. Šā sprieduma 359. punkts. [↑](#footnote-ref-93)
94. Venēcijas komisijas ziņojums, minēts iepriekš, 32. lpp. (“Eiropas valstīs atsevišķos gadījumos ieteicams saņemt *ex ante* tiesas atļauju.”). Līdz ar to sprieduma 197. punktā ir sagrozīts Venēcijas komisijas vēstījums. Arī Eiropas Padomes cilvēktiesību komisārs ir ierosinājis paredzēt *ex ante* tiesas atļauju (Memorands, minēts iepriekš, 28. punkts). [↑](#footnote-ref-94)
95. Tas vien, ka tiesas atļauja pati par sevi varētu nenodrošināt pietiekamu aizsardzību pret pilnvaru ļaunprātīgu izmantošanu, nav iemesls secinājumam, ka šāda atļauja nav nepieciešama. Jāņem vērā, ka *ex ante* tiesas atļauja tika ieviesta ar *IPA*, taču šajā gadījumā netiek *ex professo* apspriests ar *IPA* ieviestais tiesas pārskatīšanas standarts, jo 2016. gada likumu Tiesa neizvērtē. [↑](#footnote-ref-95)
96. Skat. visas starptautiskās iestādes, ko esmu norādījis spriedumam iepriekš minētajā lietā “Zabo un Visija” pievienotajos secinājumos. [↑](#footnote-ref-96)
97. Tādēļ es uzskatu, ka nevainīgu personu datu masveida apkopošana, ko Tiesa atzinusi šajā spriedumā, neatbilst 2008. gada 4. decembra sprieduma lietās Nr. 30562/04 un Nr. 30566/04 “S. un Mārpers pret Apvienoto Karalisti” 135. punktā, 2011. gada 21. jūnija sprieduma lietā Nr. 30194/09 “Šimovoloss [*Shimovolos*] pret Krieviju” 68. un 69. punktā, 2013. gada 18. aprīļa sprieduma lietā Nr. 19522/09 “M. K. pret Franciju” 37. punktā un īpaši sprieduma iepriekš minētajā lietā “Mustafa Sezgins Tanrikulu pret Turciju” 57.–59. punktā noteiktajiem principiem. [↑](#footnote-ref-97)
98. Šis ir universāls standarts, kas ietverts Apvienoto Nāciju Organizācijas 2010. gada 17. maija Labās prakses apkopojumā par tiesisko un institucionālo sistēmu un pasākumiem, kas uzliek izlūkošanas aģentūrām par pienākumu ievērot cilvēktiesības, vienlaikus apkarojot terorismu, tostarp par to pārraudzību [*United Nations Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*] (A/HRC/14/46): “Prakse Nr. 21. Valsts tiesību aktos ir izklāstīti izlūkdienestiem pieejamie datu apkopošanas pasākumu veidi; pieļaujamie izlūkdatu apkopošanas mērķi; personu kategorijas un darbības, uz ko var attiekties izlūkdatu apkopošana; aizdomu slieksnis, kas nepieciešams, lai pamatotu datu apkopošanas pasākumu izmantošanu; ierobežojumi attiecībā uz atļauto datu apkopošanas pasākumu izmantošanas ilgumu, kā arī procedūras izlūkdatu apkopošanas pasākumu izmantošanas atļaušanai, pārraudzībai un pārskatīšanai.” [↑](#footnote-ref-98)
99. Tas nav 2010. gada 14. septembra sprieduma lietā Nr. 38224/03 ““Sanoma Uitgevers B.V.” pret Nīderlandi” [*GC*] 90.–92. punktā noteiktais režīms; skat. European Union Fundamental Rights Agency (FRA), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*, volume II: *Field perspectives and legal updates*, 2017, p. 12: “ES dalībvalstīm jāizveido īpašas juridiskas procedūras, lai aizsargātu tādu grupu kā parlamenta deputātu, tiesu iestāžu, juristu un plašsaziņas līdzekļu speciālistu profesionālās privilēģijas. Šo procedūru īstenošana jāpārrauga neatkarīgai iestādei.” [↑](#footnote-ref-99)
100. Venēcijas komisijas ziņojums, minēts iepriekš, 26. lpp. [↑](#footnote-ref-100)
101. Tas ir universāls un Eiropā noteikts standarts, kas attiecīgi ietverts iepriekš minētajā Apvienoto Nāciju Organizācijas apkopojumā (“Prakse Nr. 25. Ir izveidota neatkarīga institūcija, kas pārrauga kārtību, kādā izlūkdienesti izmanto personas datus. Šai iestādei ir piekļuve visām izlūkdienestu rīcībā esošajām datnēm, un tai ir tiesības dot rīkojumu izpaust informāciju attiecīgajām personām, kā arī iznīcināt datnes vai tajās esošo personisko informāciju.”) un iepriekš minētā *FRA* dokumenta “Surveillance by intelligence services” 11. lpp. (“Dalībvalstīm arī jāpiešķir pārraudzības struktūrām pilnvaras pašām uzsākt izmeklēšanu, kā arī pastāvīga, pilnīga un tieša piekļuve to pilnvaru izpildei nepieciešamajai informācijai un dokumentiem.”). [↑](#footnote-ref-101)
102. “Zabo un Visija”, minēts iepriekš, 86. punkts. Spriežot pēc loģikas spriedumā lietā “Zabo un Visija”, šī ir vēl viena minimālā prasībā papildus spriedumā lietā “Vēbere un Sarāvija” noteiktajiem kritērijiem. Saistībā ar informēšanas procesa priekšrocībām “pārmērīgas izmantošanas ierobežošanā” skat. iepriekš minētā Venēcijas komisijas ziņojuma 35. lpp., kā arī Eiropas Padomes cilvēktiesību komisāra 2015. gada ziņojuma par Vāciju 17. lpp. un 2016. gada ziņojuma par Apvienoto Karalisti 5. lpp. [↑](#footnote-ref-102)
103. Šā sprieduma 358. punkts. [↑](#footnote-ref-103)
104. Šā sprieduma 362. punkts. [↑](#footnote-ref-104)
105. Turpat. [↑](#footnote-ref-105)
106. Turpat. [↑](#footnote-ref-106)
107. Turpat. [↑](#footnote-ref-107)
108. Vairākums ir ignorējis faktu, ka Konvencijas par personu aizsardzību attiecībā uz personas datu automātisko apstrādi Papildprotokola 2. pantā par uzraudzības iestādēm un pārrobežu datu plūsmām (ETS Nr. 181) ir noteikts, ka pusēm ir jānodrošina atbilstošs aizsardzības līmenis personas datu pārsūtīšanai uz trešām valstīm un ka atkāpes ir pieļaujamas vienīgi tad, ja pastāv leģitīmas dominējošas intereses. Šīs konvencijas paskaidrojuma ziņojumā piebilsts, ka izņēmumi ir jāinterpretē šauri, “lai izņēmums nekļūtu par noteikumu” (31. punkts). Ir svarīgi atzīmēt, ka šo protokolu ir ratificējušas 44 valstis, tostarp 8 valstis, kas nav Eiropas Padomes dalībvalstis. Apvienotā Karaliste to nav ratificējusi. Līdzās šim Eiropas Padomes standartam Eiropas Savienība pieļauj vienīgi personas datu pārsūtīšanu uz trešo valsti, kas nodrošina aizsardzības līmeni, kas būtībā ir līdzvērtīgs Eiropas Savienībā garantētajam aizsardzības līmenim (šā sprieduma 234. punkts). [↑](#footnote-ref-108)
109. Venēcijas komisijas ziņojums, minēts iepriekš, 2015. gads, 34. lpp. (“Informācijas nosūtītāja jeb “trešās personas princips” nav jāpiemēro pārraudzības struktūrai.”), kā arī *FRA* dokuments “Surveillance by intelligence services”, minēts iepriekš, 2017. gads, 13. un 106. lpp. (“Neraugoties uz trešās personas principu, ES dalībvalstīm jāapsver iespēja piešķirt pārraudzības struktūrām pilnvērtīgu piekļuvi datiem, kas pārsūtīti starptautiskās sadarbības ietvaros. Tas paplašinātu pārraudzības pilnvaras attiecībā uz visiem datiem, kas pieejami izlūkdienestiem un kurus tie apstrādā.”). [↑](#footnote-ref-109)
110. Šā sprieduma 342. punkts. [↑](#footnote-ref-110)
111. Galu galā, Tiesa ņēma vērā Valdības draudus, ka tad, “ja dalībvalstīm, kuras izmanto masveida pārtveršanas režīmu, SSD [saistītajiem sakaru datiem] jāpiemēro tādi paši aizsardzības mehānismi kā saturam, tā rezultātā, visticamāk, tiks vājināta attiecībā uz saturu noteiktā aizsardzības mehānisma efektivitāte” (atbildētājas Valdības 2019. gada 2. maija apsvērumi Lielajā palātā, 42. lpp.). [↑](#footnote-ref-111)
112. Šā sprieduma 364. punkts, to aplūkojot kopā ar 361. punktu. [↑](#footnote-ref-112)
113. Šā sprieduma 347. punkts. [↑](#footnote-ref-113)
114. Spriedumā iepriekš minētajā lietā ““Liberty” un citi” visi prasītāji bija NVO, kuri apgalvoja, ka ir pārkāptas viņu tiesības uz korespondences neaizskaramību. Šīs tiesības ir aplūkotas arī šajā lietā. [↑](#footnote-ref-114)
115. Tādēļ, izņemot iepriekš 8. punktā minētās iestādes, es esmu ņēmis vērā arī iepriekš minēto Apvienoto Nāciju 2010. gada apkopojumu, iepriekš minēto Venēcijas komisijas 2015. gada ziņojumu, kā arī iepriekš minēto *FRA* 2017. gada ziņojumu. [↑](#footnote-ref-115)
116. Apvienoto Nāciju Organizācijas Konvencijas pret starptautisko organizēto noziedzību 2. panta b) punktā jēdziens “smags noziegums” definēts kā tāds noziedzīgs nodarījums, kas sodāms ar brīvības atņemšanu vismaz uz četriem gadiem vai arī ar smagāku sodu. Atsauce uz to minēta arī Ministru komitejas Ieteikuma Rec(2005)10 paskaidrojošajā ziņojumā. [↑](#footnote-ref-116)
117. Šā sprieduma 270. punkts. Tas nozīmē, ka, tāpat kā Lielā palāta, es neesmu ņēmis vērā izmaiņas, ko ieviesa ar *IPA* un jauno 2018. gada *IC* kodeksu. Tās šī Tiesa neizvērtēja. [↑](#footnote-ref-117)
118. Skat. interesanto diskusiju par šo jautājumu starp lietas dalībniekiem Lielās palātas 2019. gada 10. jūlija sēdē. Tiesa ir aizstāvējusi dažādus viedokļus par valsts drošības nolūka precizitāti (salīdzināt un pretstatīt ar 2009. gada 10. februāra sprieduma lietā Nr. 25198/02 “Jordači [*Iordachi*] un citi pret Moldovu” 46. punktu un iepriekš minētā sprieduma lietā “Kenedijs pret Apvienoto Karalisti” 159. punktu). [↑](#footnote-ref-118)
119. Šā sprieduma 146. punkts. [↑](#footnote-ref-119)
120. Šā sprieduma 145. punkts. [↑](#footnote-ref-120)
121. Skat. atbildētājas Valdības 2019. gada 2. maija apsvērumus Lielajā palātā, 9. lpp. [↑](#footnote-ref-121)
122. Šā sprieduma 51. punkts, ko Tiesa ir atkārtoti norādījusi 375. punktā. [↑](#footnote-ref-122)
123. Šā sprieduma 36. un 116. punkts, kurā minēta norāde uz *IC* kodeksa 12.2. punktu. [↑](#footnote-ref-123)
124. Šā sprieduma 47. punkts. [↑](#footnote-ref-124)
125. Kā norādījusi Valdība: “Tomēr fakts, ka elektroniskos sakarus var pārraidīt pa jebkādiem kanāliem, lai sasniegtu galamērķi, neizbēgami nozīmē to, ka daļu sakaru, kas plūst pa nesēju starp Apvienoto Karalisti un citu valsti, veidos “iekšējie sakari”, t. i., sakari starp personām, kas atrodas Britu salās.” (Skat. tās 2019. gada 2. maija apsvērumus Lielajā palātā, 20. lpp.) [↑](#footnote-ref-125)
126. Šā sprieduma 75. punkts. [↑](#footnote-ref-126)
127. Šā sprieduma 321. punkts. Skat. arī *IPT* spriedumu lietā “Belhažs un citi pret Drošības dienestu un citiem”, IPT/13/132-9/H. [↑](#footnote-ref-127)
128. Šā sprieduma 75. punkts. Šāda prakse, šķiet, ir pretrunā ar *IC* kodeksa 6.5. punktu. [↑](#footnote-ref-128)
129. Atbildētāja Valdība pati to atzina (skat. tās 2019. gada 2. maija apsvērumus Lielajā palātā, 37. lpp.). [↑](#footnote-ref-129)
130. Nepietiek vien ar apgalvojumu, ka, tā kā Lielbritānijas tiesību akti “neļauj pārtverto materiālu atlasīt pārbaudei pēc faktora, kas “attiecas uz personu, par kuru zināms, ka tā pašlaik atrodas Britu salās”, jebkāda no tā izrietoša atšķirīga attieksme nebūtu balstīta tieši uz pilsonību vai nacionālo piederību, bet drīzāk uz ģeogrāfisko atrašanās vietu”, kā tas tika atzīts palātas spriedumā (517. punkts), ņemot vērā acīmredzamo iemeslu, ka lielākā daļa cilvēku, par kuriem zināms, ka tie pašlaik atrodas Britu salās, ir Lielbritānijas pilsoņi, un otrādi – lielākā daļa ārpus Britu salām esoši cilvēku ir ārvalstnieki. Labvēlīgāku attieksmi pret pilsoņiem atzina arī *FRA* (dokuments “Surveillance by intelligence services”, minēts iepriekš, 45. lpp.: “Tad, kad izlūkdienesti veic uzraudzību valsts ietvaros, piemērojamie tiesiskie drošības pasākumi ir efektīvāki salīdzinājumā ar tiem, kas ieviesti attiecībā uz ārvalstu uzraudzību.”). [↑](#footnote-ref-130)
131. IPT, *Human Rights Watch & Ors v SoS for the Foreign & Commonwealth Office & Ors*, 16 May 2016: “Attiecībā uz jebkuru pamatoto uzskatu, ka jebkuru darbību, uz ko attiecas *RIPA* 68. panta 5. punkts, ir veicis kāds no izlūkošanas dienestiem vai tā veikta to vārdā, sūdzības iesniedzējam ir jāpierāda, ka šāds uzskats ir pamatots, lai viņš varētu pierādīt, ka viņš ir potenciāli pakļauts šādas rīcības riskam. Turklāt šim prasītājam attiecībā uz šādu sūdzību ir jāpierāda, ka viņš atrodas vai attiecīgajā brīdī atradās Apvienotajā Karalistē.” [↑](#footnote-ref-131)
132. Iepriekš minētā Venēcijas komisijas ziņojuma 17. lpp. ir pausta tāda pati “pamatota” kritika, kādu paudis ANO īpašais ziņotājs vārda brīvības jautājumos, atsaucoties uz *ICCPR* (skat. šā sprieduma 313. punktu). [↑](#footnote-ref-132)
133. Manu secinājumu 2016. gada 20. oktobra lietā Nr. 7334/13 “Muršičs [*Mursić*] pret Horvātiju” [*GC*] 22. punkts. [↑](#footnote-ref-133)
134. *RIPA* 16. panta 3. punkts. [↑](#footnote-ref-134)
135. *IC* kodeksa 6.2. punkts. [↑](#footnote-ref-135)
136. *RIPA* 5. panta 6. punkta a) apakšpunkts un *IC* kodeksa 6.6. punkts. [↑](#footnote-ref-136)
137. Atbildētājas Valdības 2019. gada 2. maija apsvērumi Lielajā palātā, 37. lpp. [↑](#footnote-ref-137)
138. Saskaņā ar *IC* kodeksa 6.2. punktu “8. panta 4. punktā paredzētā pārtveršana ir izlūkdatu iegūšanas veids”. [↑](#footnote-ref-138)
139. *RIPA* 81. pantā ir definēta nozieguma novēršana un atklāšana, bet ne izmeklēšana. [↑](#footnote-ref-139)
140. Iepriekš minētā Venēcijas komisijas ziņojuma 11. lpp. ir minēts tas pats. [↑](#footnote-ref-140)
141. Apvienotās Karalistes parlaments savā 2015. gada *ISC* ziņojumā atzina valsts sekretāra neatkarības trūkumu, līdz 2016. gadā tika mainīta *IPA* izveide. [↑](#footnote-ref-141)
142. Tiesību normas, kas attiecas uz 8. panta 4. punktā noteikto materiālu, ko atlasa pārbaudei un uzskata par konfidenciālu informāciju (*IC* kodeksa 4.32. punkts). Atbildētāja Valdība tagad atzīst, ka “sakaru datu pieprasījumi, kas paredzēti žurnālistikas avotu identificēšanai, ir jāapstiprina tiesai” (Apvienotās Karalistes atbilde Eiropas Padomes cilvēktiesību komisāram – Memorands par uzraudzības un pārraudzības mehānismiem Apvienotajā Karalistē, 24. lpp.). [↑](#footnote-ref-142)
143. Šā sprieduma 146.–147. punkts. [↑](#footnote-ref-143)
144. Tāds bija arī 2015. gada *ISC* ziņojumā sniegtais secinājums (skat. šā sprieduma 147. punktu). Nav pārsteigums, ka 2016. gadā tika izdoti 3007 pārtveršanas orderi un valsts sekretārs noraidīja tikai piecus pieprasījumus (šā sprieduma 170. punkts). Skaitļi runā paši par sevi, proti, valsts sekretārs piedalījās vienīgi pieprasījumu “apzīmogošanā”. [↑](#footnote-ref-144)
145. Šā sprieduma 33. punkts. [↑](#footnote-ref-145)
146. Skat. palātas sprieduma 347. punktu un tiesnešu Koskelo un Turkovičas kopīgā atsevišķā viedokļa 26. punktu, kurā norādīts, ka Apvienotās Karalistes sistēma patiesībā atpaliek no Vācijas drošības pasākumu sistēmas, kas bija spēkā brīdī, kad pasludināja spriedumu lietās “Klass un citi” un “Vēbere un Sarāvija”. [↑](#footnote-ref-146)
147. Diemžēl vairākums nebija ņēmis vērā šo 2015. gada *ISC* ziņojuma rindkopu, kas minēta sprieduma 142. punktā. [↑](#footnote-ref-147)
148. 2000. gada *RIPA* 57. pants. [↑](#footnote-ref-148)
149. Pieteikuma iesniedzēja kritika Lielās palātas 2019. gada 10. jūlija sēdē ir pamatota, proti, viens pensionēts tiesnesis, kas strādā nepilnu darba laiku un ar nelielu sekretariātu un veic pieticīgu izlases izvērtējumu, “nevar cerēt, ka viņš varēs nodrošināt jēgpilnu pārraudzību”. [↑](#footnote-ref-149)
150. Attiecībā uz šiem principiem un to lomu Eiropas Padomē skat. manu atsevišķo viedokli iepriekš minētajā lietā “Zabo un Visija”. [↑](#footnote-ref-150)
151. Kā atbildētāja Valdība atzinusi mutvārdu argumentos Lielās palātas 2019. gada 10. jūlija sēdē. [↑](#footnote-ref-151)
152. Kā norādījusi atbildētāja Valdība (šā sprieduma 403. punkts). Šķiet, ka nav nodrošināta atbilstība par starptautiskajiem rīcībpolitikas dokumentiem (šā sprieduma 59. punkts). [↑](#footnote-ref-152)
153. *IC* kodeksa 6.22.–6.24. punkts. [↑](#footnote-ref-153)
154. Sprieduma 176. punkts. [↑](#footnote-ref-154)
155. Diezgan pārsteidzoši, ka vairākums sprieduma 405. punktā uzskatījis atbildētājas Valdības Lielajā palātā raksturotās prakses nostiprināšanu tiesību aktos tikai par “vēlamu”. [↑](#footnote-ref-155)
156. Ar *IPA* komisāram tika uzlikts par pienākumu izvērtēt, vai ir noticis nopietns pārkāpums, un tas būtu sabiedrības interesēs par to informēt attiecīgo personu, taču šis noteikums šajā lietā Tiesā netiek izvērtēts. *IPA* politikas izvēle liecina par piekāpšanos tam, ka iepriekšējā sistēma bija neatbilstoša, un vēl ir jānogaida, lai redzētu, vai *IPA* paredzētais risinājums ir efektīvs. [↑](#footnote-ref-156)
157. To pasliktina Valdības t. s. “NCND” (“ne apstiprināšanas, ne noliegšanas”) nostāja, kā rezultātā “persona nevar zināt, vai attiecībā uz to ir veikta uzraudzība”, turklāt “ar uzraudzību saistītie lēmumi netiek efektīvi pārbaudīti”, kā secināja Eiropas Padomes cilvēktiesību komisārs (Memorands, minēts iepriekš). [↑](#footnote-ref-157)
158. Tādējādi vairākuma secinājums, ka *IPT* ir “nodrošinājusi stabilu tiesiskās aizsardzības līdzekli ikvienai personai, kurai radušās aizdomas, ka izlūkdienesti ir pārtvēruši tās sakarus” (415. punkts), neatklāj sistēmai raksturīgo trūkumu, proti, tās virtuālo būtību, tiem, kam nav iemesla aizdomām, ka attiecībā uz viņiem ir veikta slepena uzraudzība. [↑](#footnote-ref-158)
159. *RIPA* 69. panta 1. punkts. [↑](#footnote-ref-159)
160. Atbildētāja Valdība apgalvoja, ka “pat pirms kodeksa 12. nodaļas izdošanas tā bija “pieejama”, jo bija izpausta”, atsaucoties uz 2014. gada oktobra paziņojumu (skat. tās 2019. gada 2. maija apsvērumus Lielajā palātā, 49. lpp.). Tādējādi pat Valdība ir atzinusi, ka pirms tam šis likums nebija pieejams. [↑](#footnote-ref-160)
161. Šā sprieduma 116. punkts. [↑](#footnote-ref-161)
162. Šā sprieduma 263. punkts. [↑](#footnote-ref-162)
163. Kā atbildētāja Valdība norādījusi Lielās palātas 2019. gada 10. jūlija sēdē: “Tādējādi, ja jautājums ir par to, vai jūsu rīcībā ir liels daudzums datu pat pēc filtrēšanas procesa pabeigšanas, tad atbilde uz šo jautājumu ir “jā”, kas turklāt ir ļoti labi, mēs apstiprinām.” [↑](#footnote-ref-163)
164. Šā sprieduma 502. un 503. punkts. [↑](#footnote-ref-164)
165. Šā sprieduma 362. punkts. [↑](#footnote-ref-165)
166. Šā sprieduma 513. punkts. [↑](#footnote-ref-166)
167. Diemžēl Tiesa ir atstājusi bez ievērības Cilvēktiesību komitejas pausto nostāju tās 2015. gada noslēguma apsvērumos par Apvienoto Karalisti, UN Doc. CCPR/C/GBR/CO/7, 2015. gada 17. augusts, 24. punkts, kur tā bija paudusi bažas par “atbilstošu drošības pasākumu trūkumu saistībā ar privātu sakaru iegūšanu no ārvalstu drošības aģentūrām un personīgo sakaru datu koplietošanu ar šīm aģentūrām”. [↑](#footnote-ref-167)
168. Tieši uz to ir atsaukusies Venēcijas komisija (skat. šā sprieduma 201. punktu). [↑](#footnote-ref-168)
169. *IC* kodeksa 7.3. punkts (skat. šā sprieduma 96. un 390. punktu). [↑](#footnote-ref-169)
170. Atbildētājas Valdības mutvārdu argumenti Lielās palātas 2019. gada 10. jūlija sēdē. [↑](#footnote-ref-170)
171. Šā sprieduma 422.–423. punkts. [↑](#footnote-ref-171)
172. Skat. atbildētājas Valdības mutvārdu argumentus Lielās palātas 2019. gada 10. jūlija sēdē. Šādi pārtverošā iestāde varētu masveida pārtveršanas veidā iegūt saturu, ko tā būtu ieguvusi atbilstoši atsevišķam un mērķētam orderim, kas minēts 8. pantā, un līdz ar to apiet šīs Tiesas spriedumu iepriekš minētajā lietā “Kenedijs pret Apvienoto Karalisti”. [↑](#footnote-ref-172)
173. Šā sprieduma 420. punkts. [↑](#footnote-ref-173)
174. Mans spriedums ir balstīts uz manu kā krimināltiesību tiesneša pieredzi ļoti sarežģītās krimināllietās, kurās policija bieži pieprasīja pārtvert lielu daudzumu saistīto sakaru datu. [↑](#footnote-ref-174)
175. Šā sprieduma 450. punkts. [↑](#footnote-ref-175)
176. Salīdzināt un pretstatīt ar 420. un 421. punktu. Jāatzīmē, ka 420. punktā ir minēts “galvenais likumā noteiktais drošības pasākums”, taču 421. punktā tā nozīme šķietami ir mazinājusies, jo tas ir raksturots kā “svarīgs drošības pasākums”. Neprecīzas valodas lietojums 421. punktā ir mulsinošs, taču satura trūkums ir vēl satraucošāks. Tiesa apzināti manipulēja ar valodas līdzekļiem, lai saistīto sakaru datu masveida pārtveršanas kontekstā piešķirtu 381. un 382. punktā paustajām bažām atšķirīgu nozīmi. To visu acīmredzami papildina “visaptverošais izvērtējums”, kas ļauj Tiesai sasniegt jebkuru rezultātu (skat. šī “visaptverošā taisnīguma” kritērija izvērtējumu manos secinājumos, kas pievienoti 2020. gada 15. oktobra spriedumam lietā Nr. 80982/12 “Muhameds [*Muhammad*] un Muhameds pret Rumāniju” [*GC*] un 2018. gada 18. decembra spriedumam lietā Nr. 36658/05 “Murtazalijeva [*Murtazaliyeva*] pret Krieviju” [*GC*]). [↑](#footnote-ref-176)
177. “Zabo un Visija”, minēts iepriekš, 70. punkts: “Ir jāuzlabo garantijas, kas nepieciešamas atkarībā no apmēra, kādā tiek piemērota Konvencijas judikatūra par pārtveršanu, lai risinātu jautājumu par šādu uzraudzības praksi.” Līdzīgi *PACE* rezolūcijā 2045 (2015) ir uzsvērta nepieciešamība stiprināt masveida uzraudzības pārraudzību. [↑](#footnote-ref-177)
178. 277 US 438. [↑](#footnote-ref-178)
179. Šā sprieduma 226. punkts. [↑](#footnote-ref-179)
180. Šā sprieduma 211., 217. un 239-241. punkts. [↑](#footnote-ref-180)
181. Šā sprieduma 234. punkts. [↑](#footnote-ref-181)