Judikatūras krājums

TIESAS SPRIEDUMS (virspalāta)

2020. gada 6. oktobrī*

[Teksts labots ar 2020. gada 16. novembra rīkojumu]

Satura rādītājs

* Tiesvedības valoda: franču.

Lūgums sniegt prejudiciālu nolēmumu – Personas datu apstrāde elektronisko komunikāciju nozarē – Elektronisko komunikāciju pakalpojumu sniedzēji – Mitināšanas pakalpojumu sniedzēji un interneta piekļuves pakalpojuma sniedzēji – Informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta saglabāšana – Datu automatizēta analīze – Piekļuve datiem reāllaikā – Valsts drošības aizsardzība un terorisma apkarošana – Noziedzības apkarošana – Direktīva 2002/58/EK – Piemērošanas joma – 1. panta 3. punkts un 3. pants – Elektronisko komunikāciju konfidencialitāte – Aizsardzība – 5. pants un 15. panta 1. punkts – Direktīva 2000/31/EK – Piemērošanas joma – Eiropas Savienības Pamattiesību harta – 4., 6.–8. un 11. pants un 52. panta 1. punkts – LES 4. panta 2. punkts

Apvienotajās lietās C-511/18, C-512/18 un C-520/18

par lūgumiem sniegt prejudiciālu nolēmumu atbilstoši LESD 267. pantam, ko *Conseil d'État* (Valsts padome, Francija) iesniedza ar 2018. gada 26. jūlija lēmumiem, kas Tiesā reģistrēti 2018. gada 3. augustā (C-511/18 un C-512/18), un ko *Cour constitutionnelle* (Konstitucionālā tiesa, Beļģija) iesniedza ar 2018. gada 19. jūlija lēmumu, kas Tiesā reģistrēts 2018. gada 2. augustā (C-520/18), tiesvedībās

La Quadrature du Net (C-511/18 un C-512/18),

French Data Network (C-511/18 un C-512/18),

Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 un C-512/18),

Igwan.net (C-511/18)

pret

Premier ministre (C-511/18 un C-512/18),

Garde des Sceaux, ministre de la Justice (C-511/18 un C-512/18),

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18), piedaloties –

Privacy International (C-512/18),

Center for Democracy and Technology (C-512/18),

un

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

pret

Conseil des ministres,

piedaloties

Child Focus (C-520/18),

TIESA (virspalāta)

šādā sastāvā: priekšsēdētājs K. Lēnartss [*K. Lenaerts*], priekšsēdētāja vietniece R. Silva de Lapuerta [*R. Silva de Lapuerta*], palātu priekšsēdētāji Ž. K. Bonišo [*J.-C. Bonichot*], A. Arabadžijevs [*A. Arabadjiev*], A. Prehala [*A. Prechal*], M. Safjans [*M. Safjan*], P. Dž. Švīrebs [*P. G. Xuereb*] un L. S. Rosi [*L. S. Rossi*], tiesneši J. Malenovskis [*J. Malenovský*], L. Bejs Larsens [*L. Bay Larsen*], T. fon Danvics [*T. von Danwitz*] (referents), K. Toadere [*C. Toader*], K. Jirimēe [*K. Jürimäe*], K. Likurgs [*C. Lycourgos*] un N. Pisarra [*N. Piçarra*],

ģenerāladvokāts: M. Kamposs Sančess-Bordona [*M. Campos Sánchez-Bordona*],

sekretāre: S. Stremholma [*C. Strömholm*], administratore,

ņemot vērā rakstveida procesu un 2019. gada 9. un 10. septembra tiesas sēdi,

ņemot vērā apsvērumus, ko sniedza:

– *Quadrature du Net*, *Fédération des fournisseurs d'accès à Internet associatifs*, *Igwan.net* un *Center for Democracy and Technology* vārdā – *A. Fitzjean Ò Cobhthaigh*, advokāts,

– *French Data Network* vārdā – *Y. Padova*, advokāts,

– *Privacy International* vārdā – *H. Roy*, advokāts,

– *Ordre des barreaux francophones un germanophone* vārdā – *E. Kiehl*, *P. Limbrée*, *E. Lemmens*, *A. Cassart* un *J.-F. Henrotte*, advokāti,

– *Académie Fiscale ASBL* un UA vārdā – *J.-P. Riquet*,

– *Liga voor Mensenrechten ASBL* vārdā – *J. Vander Velpen*, advokāts,

– *Ligue des Droits de l'Homme ASBL* vārdā – *R. Jespers* un *J. Fermon*, advokāti,

– VZ, WY un XX vārdā – *D. Pattyn*, advokāts,

– *Child Focus* vārdā – *N. Buisseret*, *K. De Meester* un *J. Van Cauter*, advokāti,

– Francijas valdības vārdā – sākotnēji *D. Dubois*, *F. Alabrune* un *D. Colas*, kā arī *E. de Moustier* un *A.-L. Desjonquères*, vēlāk – *D. Dubois* un *F. Alabrune*, kā arī *E. de Moustier* un *A.-L. Desjonquères*, pārstāvji,

– Beļģijas valdības vārdā – *J.-C. Halleux* un *P. Cottin*, kā arī *C. Pochet*, pārstāvji, kuriem palīdz *J. Vanpraet*, *Y. Peeters*, *S. Depré* un *E. de Lophem*, advokāti,

– Čehijas valdības vārdā – *M. Smolek*, *J. Vláčil* un *O. Serdula*, pārstāvji,

– Dānijas valdības vārdā – sākotnēji *J. Nymann-Lindegren*, kā arī *M. Wolff* un *P. Ngo*, vēlāk – *J. Nymann-Lindegren* un *M. Wolff*, pārstāvji,

– Vācijas valdības vārdā – sākotnēji *J. Möller*, *M. Hellmann*, *E. Lankenau*, *R. Kanitz* un *T. Henze*, vēlāk – *J. Möller*, *M. Hellmann*, *E. Lankenau* un *R. Kanitz*, pārstāvji,

– Igaunijas valdības vārdā – *N. Grünberg* un *A. Kalbus*, pārstāves,

– Īrijas valdības vārdā – *A. Joyce*, kā arī *M. Browne* un *G. Hodge*, pārstāvji, kuriem palīdz *D. Fennelly*, *BL*,

– Spānijas valdības vārdā – sākotnēji *L. Aguilera Ruiz* un *A. Rubio González*, vēlāk – *L. Aguilera Ruiz*, pārstāvis,

– Kipras valdības vārdā – *E. Neofytou*, pārstāve,

– Latvijas valdības vārdā – V. Soņeca, pārstāve,

– Ungārijas valdības vārdā – sākotnēji *M. Z. Fehér* un *Z. Wagner*, vēlāk – *M. Z. Fehér*, pārstāvis,

– Nīderlandes valdības vārdā – *M. K. Bulterman* un *A. M. de Ree*, pārstāvji,

– Polijas valdības vārdā – *B. Majczyna*, kā arī *J. Sawicka* un *M. Pawlicka*, pārstāvji,

– Zviedrijas valdības vārdā – sākotnēji *H. Shev*, *H. Eklinder*, *C. Meyer-Seitz* un *A. Falk*, vēlāk – *H. Shev*, *H. Eklinder*, *C. Meyer-Seitz* un *J. Lundberg*, pārstāves,

– Apvienotās Karalistes valdības vārdā – *S. Brandon*, pārstāvis, kam palīdz *G. Facenna*, *QC*, un *C. Knight*, *barrister*,

– [Ievilkums dzēsts ar 2020. gada 16. novembra rīkojumu],

– Eiropas Komisijas vārdā – sākotnēji *H. Kranenborg* un *M. Wasmeier*, kā arī *P. Costa de Oliveira*, vēlāk – *H. Kranenborg* un *M. Wasmeier*, pārstāvji,

– Eiropas Datu aizsardzības uzraudzītāja vārdā – *T. Zerdick* un *A. Buchta*, pārstāvji,

noklausījusies ģenerāladvokāta secinājumus 2020. gada 15. janvāra tiesas sēdē,

pasludina šo spriedumu.

Spriedums

1 Lūgumi sniegt prejudiciālu nolēmumu ir par to, kā interpretēt, pirmkārt, Eiropas Parlamenta un Padomes Direktīvas 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV 2002, L 201, 37. lpp.), kurā grozījumi ir izdarīti ar Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 2009/136/EK (OV 2009, L 337, 11. lpp.) (turpmāk tekstā – "Direktīva 2002/58"), 15. panta 1. punktu, un, otrkārt, Eiropas Parlamenta un Padomes Direktīvas 2000/31/EK (2000. gada 8. jūnijs) par dažiem informācijas sabiedrības pakalpojumu tiesiskiem aspektiem, jo īpaši elektronisko tirdzniecību, iekšējā tirgū (Direktīva par elektronisko tirdzniecību) (OV 2000, L 178, 1. lpp.) 12.–15. pantu, tos skatot kopā ar Eiropas Savienības Pamattiesību hartas (turpmāk tekstā – "Harta") 4., 6.–8. un 11. pantu, kā arī 52. panta 1. punktu un LES 4. panta 2. punktu.

2 Lūgums lietā C-511/18 tika iesniegts strīdos starp *Quadrature du Net*, *French Data Network*, *Fédération des fournisseurs d'accès à Internet associatifs* (Asociēto interneta piekļuves pakalpojuma sniedzēju federācija) un *Igwan.net* un *Premier ministre* (premjerministrs, Francija), *Garde des Sceaux, ministre de la Justice* (tieslietu ministrs, Francija), *ministre de l'Intérieur* (iekšlietu ministrs, Francija) un *ministre des Armées* (bruņoto spēku ministrs, Francija) par *décret n.º 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement* (2015. gada

28. septembra Dekrēta Nr. 2015-1185 par specializēto izlūkdienestu noteikšanu) (2015. gada 29. septembra *JORF*, 1. dokuments no 97; turpmāk tekstā – "Dekrēts Nr. 2015-1185"), *décret n° 2015-1211, du 1er octobre 2015, relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État* (2015. gada 1. oktobra Dekrēta Nr. 2015-1211 par prāvām saistībā ar tādu izlūkdatu vākšanas metožu izmantošanu, kurām ir nepieciešama atļauja, un ar valsts drošības jautājumiem saistītajām datnēm) (2015. gada 2. oktobra *JORF*, 7. dokuments no 108; turpmāk tekstā – "Dekrēts Nr. 2015-1211"), *décret n° 2015-1639, du 11 décembre 2015, relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure* (2015. gada 11. decembra Dekrēta Nr. 2015-1639 par tādu dienestu noteikšanu, kuri nav specializētie izlūkdienesti, bet kuriem ir tiesības izmantot Iekšējās drošības kodeksa VIII daļas V sadaļā minētās metodes, kas pieņemtas, piemērojot Iekšējās drošības kodeksa L. 811.-4. pantu) (2015. gada 12. decembra *JORF*, 28. dokuments no 127; turpmāk tekstā – "Dekrēts Nr. 2015-1639"), kā arī *décret n° 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement* (2016. gada 29. janvāra Dekrēta Nr. 2016-67 par izlūkdatu vākšanas metodēm) (2016. gada 31. janvāra *JORF*, 2. dokuments no 113; turpmāk tekstā – "Dekrēts Nr. 2016-67") likumību.

3 Lūgums lietā C-512/18 ir iesniegts strīdos starp *French Data Network*, *Quadrature du Net* un *Fédération des fournisseurs d'accès à Internet associatifs* un premjerministru (Francija) un *Garde des Sceaux*, tieslietu ministru (Francija) par *code des postes et des communications électroniques* (Pasta un elektronisko komunikāciju kodekss; turpmāk tekstā – "*CPCE*") R. 10-13. panta un *décret n.° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne* (2011. gada 25. februāra Dekrēta Nr. 2011-219 par to datu saglabāšanu un paziņošanu, ar kuriem iespējams identificēt personas, kas ir piedalījušās tiešsaistes satura veidošanā) (2011. gada 1. marta *JORF*, 32. teksts no 170; turpmāk tekstā – "Dekrēts Nr. 2011-219"), likumību.

4 Lūgums lietā C-520/18 tika iesniegts strīdā starp *Ordre des barreaux francophones et germanophone* (Franču valodas un vācu valodas advokātu kolēģijas), *Académie Fiscale ASBL*, UA, *Liga voor Mensenrechten ASBL*, *Ligue des Droits de l'Homme ASBL*, VZ, WY un XX un *Conseil des ministres* (Ministru padome, Beļģija) par *loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques* (2016. gada 29. maija Likuma par datu vākšanu un saglabāšanu elektronisko komunikāciju nozarē) (2016. gada 18. jūlija *Moniteur belge*, 44717. lpp.; turpmāk tekstā – "2016. gada 29. maija likums") likumību.

Atbilstošās tiesību normas

Savienības tiesības

Direktīva 95/46

5 Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV 1995, L 281, 31. lpp.) kopš 2018. gada 25. maija ir atcelta ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46 (OV 2016, L 119, 1. lpp.). Direktīvas 95/46 3. panta 2. punktā bija noteikts:

"Šī direktīva neattiecas uz personas datu apstrādi:

– tādu pasākumu gaitā, uz kuru neattiecas Kopienas tiesību akti, kā Līguma par Eiropas Savienību V un VI sadaļā paredzētie pasākumi un, jebkurā gadījumā, uz apstrādes operācijām attiecībā uz sabiedrisko drošību, aizsardzību, valsts drošību (ieskaitot valsts ekonomisko labklājību, ja apstrādes operācija attiecas uz valsts drošības jautājumiem) un uz valsts pasākumiem krimināltiesību jomā;

– ko veic fiziska persona tikai un vienīgi personiska vai mājsaimnieciska pasākuma gaitā."

6 Direktīvas 95/46 22. pants, kurš iekļauts tās III nodaļā "Tiesiskās aizsardzības līdzekļi, atbildība un sankcijas", bija formulēts šādi:

"Neierobežojot nevienu administratīva rakstura līdzekli, kuru var paredzēt, *inter alia*, 28. pantā minētajai uzraudzības iestādei pirms vēršanās tiesas iestādē, dalībvalstis nodrošina katras personas tiesības uz tiesiskas aizsardzības līdzekli par jebkuru tiesību, ko šai personai garantē minētajai datu apstrādei piemērojamais attiecīgās valsts likums, pārkāpumu."

Direktīva 97/66

7 Atbilstoši Eiropas Parlamenta un Padomes Direktīvas 97/66/EK (1997. gada 15. decembris) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (OV 1997, L 24, 1. lpp.) 5. pantam "Komunikāciju konfidencialitāte":

"1. Dalībvalstis ar valsts tiesisko regulējumu nodrošina komunikāciju, kas veiktas, izmantojot publisko komunikāciju tīklu vai publiski pieejamus komunikāciju pakalpojumus, konfidencialitāti. Īpaši tās aizliedz komunikāciju noklausīšanos, uztveršanu un uzglabāšanu vai tās cita veida pārtveršanu vai pārraudzību personām, kas nav lietotāji, bez attiecīgo lietotāju piekrišanas, izņemot gadījumus, kad šo darbību veikšana ir atļauta ar likumu atbilstoši 14. panta 1. punktam.

2. 1. punkts neietekmē ar likumu atļautu komunikāciju reģistrēšanu, ja to veic likumīgas uzņēmējdarbības prakses ietvaros, lai sniegtu pierādījumu par komerciālu darījumu vai par jebkuru citu uzņēmējdarbības komunikāciju." [Neoficiāls tulkojums]

Direktīva 2000/31

8 Direktīvas 2000/31 14. un 15. apsvērumā ir paredzēts:

"(14) Personu aizsardzību attiecībā uz personīgo datu apstrādi reglamentē tikai Direktīva [95/46] un Direktīva [97/66], kas pilnībā attiecas uz informācijas sabiedrības pakalpojumiem; šīs direktīvas jau izveido Kopienas juridisko struktūru personīgo datu jomā un tāpēc nav vajadzības ietvert šo jautājumu šajā direktīvā, lai nodrošinātu vienmērīgu iekšējā tirgus darbību, jo īpaši personīgo datu brīvu apriti starp dalībvalstīm; šīs direktīvas ieviešana un piemērošana būtu jāveic pilnīgi atbilstīgi principiem, kas saistīti ar personīgo datu aizsardzību, jo īpaši attiecībā uz nelūgtiem komercpaziņojumiem un starpnieku atbildību; šī direktīva nevar novērst anonīmu atklāto tīklu izmantošanu, tādu kā internets.

(15) Paziņojumu konfidencialitāti garantē Direktīvas [97/66] 5. pants; saskaņā ar Direktīvu 97/66/EK dalībvalstīm jāaizliedz jebkāda šādu paziņojumu aizturēšana un uzraudzība personām, kas nav sūtītāji vai saņēmēji, izņemot gadījumus, kad tās ir tiesiski pilnvarotas."

9 Direktīvas 2000/31 1. pants ir izteikts šādi:

"1. Šī direktīva cenšas veicināt pienācīgu iekšējā tirgus darbību, nodrošinot brīvu informācijas sabiedrības pakalpojumu apriti starp dalībvalstīm.

2. Šī direktīva līdz līmenim, kas nepieciešams, lai sasniegtu 1. punktā minēto mērķi, saskaņo konkrētus valsts noteikumus par informācijas sabiedrības pakalpojumiem attiecībā uz iekšējo tirgu, pakalpojumu sniedzēju reģistrācijas vietu, komerciņojumiem, elektroniskajiem kontraktiem, starpnieku saistībām, rīcības kodeksiem, strīdu noregulējumu bez tiesas, sūdzību ierosināšanu tiesā un sadarbību starp dalībvalstīm.

3. Šī direktīva papildina Kopienas tiesības, kas piemērojamas informācijas sabiedrības pakalpojumiem, neierobežojot aizsardzības līmeni, jo īpaši sabiedrības veselībai un patērētāju interesēm, kā noteikts Kopienas aktos un valsts tiesību aktos, kas tos ievieš, ciktāl tas neierobežo brīvību sniegt informācijas sabiedrības pakalpojumus.

[..]

5. Šī direktīva neattiecas uz:

[..]

b) jautājumiem, kuri attiecas uz informācijas sabiedrības pakalpojumiem un kuri ietverti Direktīvā [95/46] un [97/66];

[..]."

10 Direktīvas 2000/31 2. pants ir formulēts šādi:

"Šajā direktīvā terminiem ir šādas nozīmes:

a) "informācijas sabiedrības pakalpojumi": pakalpojumi tādā nozīmē, kā noteikts 1. panta 2. punktā [Eiropas Parlamenta un Padomes] Direktīvā 98/34/EK [(1998. gada 22. jūnijs), ar ko nosaka informācijas sniegšanas kārtību tehnisko standartu un noteikumu jomā (OV 1998, L 204, 37. lpp.)], kura grozīta ar [Eiropas Parlamenta un Padomes] Direktīvu 98/48/EK [(1998. gada 20. jūlijs) (OV 1998, L 217, 18. lpp.)];

[..].”

11 Direktīvas 2000/31 15. pantā ir paredzēts:

“1. Dalībvalstis neuzliek vispārējas saistības pakalpojuma sniedzējiem, piedāvājot 12., 13. un 14. pantā minētos pakalpojumus, pārraudzīt informāciju, ko tie pārraida vai uzglabā, kā arī neuzliek pienākumu aktīvi meklēt faktus un apstākļus, kas norāda uz nelegālu darbību.

2. Dalībvalstis var paredzēt pienākumu informācijas sabiedrības pakalpojumu sniedzējiem nekavējoties informēt kompetentās valsts iestādes par iespējamām veiktajām nelegālajām darbībām vai informāciju, ko sniedz pakalpojumu sniedzēju pakalpojumu saņēmēji, vai pienākumu kompetentajām iestādēm pēc to pieprasījuma darīt zināmu informāciju, kas ļauj identificēt tos pakalpojumu saņēmējus, ar kuriem pakalpojumu sniedzējiem ir glabāšanas līgumi.”

Direktīva 2002/21

12 Saskaņā ar Eiropas Parlamenta un Padomes Direktīvas 2002/21/EK (2002. gada 7. marts) par kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem (pamatdirektīva) (OV 2002, L 108, 33. lpp.) 10. apsvērumu:

““Informācijas sabiedrības pakalpojuma” definīcija 1. pantā [Direktīvā 98/34, kas grozīta ar Direktīvu 98/48], iekļauj plašu to ekonomisko darbību spektru, kas notiek tiešsaistē. Lielākā daļa minēto darbību nav iekļautas šīs direktīvas darbības jomā, jo tās neietilpst pilnīgi vai lielākoties signālu pārraides elektronisko komunikāciju tīklos. Balss telefona un elektroniskā pasta pārraides pakalpojumi ir iekļauti šajā direktīvā. Viens un tas pats uzņēmums, piemēram, interneta pakalpojumu nodrošinātājs, var piedāvāt gan elektronisko komunikāciju pakalpojumu, tādu kā piekļuvi internetam, gan pakalpojumus, kas nav iekļauti šajā direktīvā, tādus kā tīmekļa satura nodrošināšana.”

13 Direktīvas 2002/21 2. pantā ir paredzēts:

“Šajā direktīvā:

[..]

c) “elektronisko komunikāciju pakalpojums” nozīmē pakalpojumu, ko parasti nodrošina par atlīdzību, un kas pilnīgi vai galvenokārt sastāv no signālu pārraidīšanas elektronisko komunikāciju tīklos, ietverot telekomunikāciju pakalpojumus un pārraidīšanas pakalpojumus tīklos, ko izmanto apraidei, neiekļaujot pakalpojumus, kas saistīti ar redaktorisku atbildību par vai kas nodrošina saturu, kas pārraidīts, izmantojot elektronisko komunikāciju tīklus un pakalpojumus; tas neiekļauj informācijas sabiedrības pakalpojumus, kā noteikts Direktīvas [98/34] 1. pantā, kas nesastāv pilnībā vai galvenokārt no signālu pārraidīšanas elektronisko komunikāciju tīklos;

[..].”

Direktīva 2002/58

14 Direktīvas 2002/58 2., 6., 7., 11., 22., 26. un 30. apsvērumā ir noteikts:

“(2) Šī direktīva respektē pamattiesības un ievēro principus, kas jo īpaši ir atzīti [Hartā]. Šī direktīva jo īpaši nodrošina pilnībā tiesības, kas izklāstītas minētās hartas 7. un 8. pantā.

[..]

(6) Internets maina tradicionālās tirgus struktūras, nodrošinot kopēju, globālu infrastruktūru plaša elektronisko komunikāciju pakalpojumu klāsta piedāvājumam. Publiski pieejami elektronisko telekomunikāciju pakalpojumi internetā atklāj jaunas iespējas lietotājiem, taču rada jaunu risku to personas datiem un privātajai dzīvei.

(7) Attiecībā uz publisko komunikāciju tīklu jāizstrādā īpaši normatīvi un tehniskie noteikumi, lai aizsargātu fizisku personu pamattiesības un pamatbrīvības, kā arī juridisku personu likumīgās intereses, jo īpaši ņemot vērā arvien lielāku jaudu abonentu un lietotāju datu automatizētai glabāšanai un apstrādei.

[..]

(11) Tāpat kā Direktīva [95/46], arī šī direktīva neattiecas uz pamattiesību un pamatbrīvību aizsardzības jautājumiem, kas saistīti ar darbībām, kuras neregulē [Savienības] 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, 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 [parakstīta 1950. gada 4. novembrī Romā], 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.

[..]

(22) Aizliegums personām, kas nav lietotāji, vai bez to piekrišanas glabāt informāciju par komunikācijām un ar tām saistītu informāciju par datu plūsmu, nav paredzēts, lai aizliegtu jebkādu automātisku, pagaidu vai īslaicīgu šīs informācijas uzglabāšanu, ja to dara tikai tādēļ, lai veiktu pārraidīšanu elektronisko komunikāciju tīklā, un ar noteikumu, ka informāciju neuzglabā ilgāk, kā nepieciešams, lai veiktu pārraidīšanu un datu plūsmas pārvaldi, un ka uzglabāšanas laikā ir garantēta konfidencialitāte. [..]

[..]

(26) Tādi dati, kas attiecas uz abonentiem un ir apstrādāti elektronisko komunikāciju tīklos, lai izveidotu savienojumu un pārraidītu informāciju, iekļauj informāciju par fizisku personu privāto dzīvi un attiecas uz tiesībām ievērot juridisku personu likumīgās intereses. Šādus datus drīkst uzglabāt tikai tādā apmērā, cik vajadzīgs, lai sniegtu pakalpojumu ar nolūku sagatavot rēķinus un veikt norēķinus par starpsavienojumiem, un tos glabā ierobežotu laiku. Jebkuru tālāku šādu datu apstrādi [..] var atļaut tikai tad, ja abonents ir tam piekritis, pamatojoties uz publiski pieejamu komunikāciju pakalpojumu sniedzēja dotu precīzu un pilnīgu informāciju par tādas tālākas apstrādes veidiem, ko tas nodomājis veikt, un par abonenta tiesībām nesniegt vai atsaukt savu piekrišanu šādai apstrādei. Informācija par datu plūsmu, ko izmanto komunikāciju pakalpojumu tirdzniecībā [..] arī būtu jādzēš vai jāpadara anonīma [..].

[..]

(30) Sistēmas elektronisko komunikāciju tīklu nodrošināšanai un pakalpojumu sniegšanai jāveido tā, lai ierobežotu nepieciešamo personas datu apjomu līdz stingri noteiktam minimumam. [..]”

15 Direktīvas 2002/58 1. pantā "Darbības joma un mērķis" ir noteikts:

"1. Šajā direktīvā paredzēta dalībvalstu to noteikumu saskaņošana, ar kuriem jānodrošina pamattiesību un pamatbrīvību līdzvērtīgs aizsardzības līmenis, un jo īpaši tiesības uz privāto dzīvi un konfidencialitāti saistībā ar personas datu apstrādi elektronisko komunikāciju nozarē, kā arī jānodrošina šo datu un elektronisko komunikāciju iekārtu un pakalpojumu brīva aprite [Eiropas Savienībā].

2. Šīs direktīvas noteikumi precizē un papildina Direktīv[u] [95/46] 1. punktā minētaj[ā] nolūk[ā]. 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."

16 Saskaņā ar Direktīvas 2002/58 2. pantu "Definīcijas":

"Izņemot gadījumus, kad noteikts citādi, piemēro definīcijas, kas minētas Direktīvā [95/46] un Direktīvā [2002/21].

Piemēro arī šādas definīcijas:

a) "lietotājs" ir jebkura fiziska persona, kas izmanto publiski pieejamu elektronisko komunikāciju pakalpojumu personīgiem vai uzņēmējdarbības mērķiem, ne vienmēr būdama šā pakalpojuma abonents;

b) "informācija par datu plūsmu" ir jebkuri dati, kas apstrādāti ar nolūku pārsūtīt komunikāciju elektronisko komunikāciju tīklā vai ar nolūku sagatavot rēķinu;

c) "atrašanās vietas dati" ir jebkuri dati, kuri apstrādāti elektronisko komunikāciju tīklā vai kurus apstrādā elektronisko komunikāciju pakalpojuma sniedzējs, norādot publiski pieejamu elektronisko komunikāciju pakalpojuma lietotāja galaiekārtas ģeogrāfisko atrašanās vietu;

d) "komunikācija" ir jebkāda informācija, ar kuru apmainās vai kuru pārsūta starp noteiktu skaitu personu, izmantojot publiski pieejamu elektronisko komunikāciju pakalpojumu. Tajā neiekļauj informāciju, kas, izmantojot elektronisko komunikāciju tīklu, pārsūtīta sabiedrībai kā apraides pakalpojuma daļa, izņemot līdz līmenim, kad informāciju var attiecināt uz identificējamu abonentu vai lietotāju, kas saņem šo informāciju;

[..]."

17 Direktīvas 2002/58 3. pantā "Attiecīgie pakalpojumi" ir paredzēts:

"Šī direktīva attiecas uz personas datu apstrādi saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiskos komunikāciju tīklos Kopienā, tostarp publiskos komunikāciju tīklos, kuros var izmantot datu vākšanas un identifikācijas ierīces."

18 Saskaņā ar Direktīvas 2002/58 5. pantu "Komunikāciju konfidencialitāte":

"1. Dalībvalstis nodrošina komunikāciju un saistītās informācijas par datu plūsmu konfidencialitāti ar publisko komunikāciju tīkla un publiski pieejamu elektronisko komunikāciju pakalpojumiem, ievērojot valsts tiesību aktus. Īpaši tās aizliedz komunikāciju un saistītās informācijas par datu plūsmu noklausīšanos, ierakstīšanu, uzglabāšanu vai cita veida aizturēšanu vai pārraudzību personām, kas nav

lietotāji, bez attiecīgo lietotāju piekrišanas, izņemot gadījumus, kad to darīt ir ar likumu atļauts saskaņā ar 15. panta 1. punktu. Šis punkts neliedz tehnisko uzglabāšanu, kas nepieciešama komunikāciju pārsūtīšanai, neierobežojot konfidencialitātes principu.

[..]

3. Dalībvalstis nodrošina, ka informācijas uzglabāšana abonenta vai lietotāja galaiekārtā vai piekļuves iegūšana šādā iekārtā jau uzglabātai informācijai ir atļauta tikai ar nosacījumu, ka attiecīgais abonents vai lietotājs ir devis savu piekrišanu un saskaņā ar Direktīvu [95/46] nodrošināts ar skaidru un visaptverošu informāciju, tostarp par apstrādes nolūku. Tas neliedz jebkādu tehnisku uzglabāšanu vai piekļuvi, kas paredzēta vienīgi, lai veiktu saziņas pārraidīšanu elektronisko sakaru tīklā, vai kas noteikti nepieciešama tā informācijas sabiedrības pakalpojuma sniedzējam, kuru skaidri pieprasījis abonents vai lietotājs."

19 Direktīvas 2002/58 6. pantā "Informācija par datu plūsmu" ir noteikts:

"1. Informācija par datu plūsmu, kas attiecas uz abonentiem un lietotājiem un ko publisko komunikāciju tīkla pakalpojumu sniedzējs vai publiski pieejamu elektronisko komunikāciju pakalpojuma sniedzējs apstrādā vai uzglabā, ir jādzēš vai jāpadara anonīma, kad tā vairs nav nepieciešama komunikāciju pārraidīšanai, neierobežojot šā panta 2., 3. un 5. pantu un 15. panta 1. punktu.

2. Var apstrādāt informāciju par datu plūsmu, kas nepieciešama, lai abonentam sagatavotu rēķinu un veiktu norēķinus par starpsavienojumiem. Šāda apstrāde ir pieļaujama tikai tik ilgi, kamēr nav beidzies termiņš, kura laikā var likumīgi apstrīdēt rēķinu vai saņemt maksājumu.

3. Elektronisko komunikāciju pakalpojumu tirdzniecības nolūkā vai pievienotās vērtības pakalpojumu sniegšanas nolūkā publiski pieejamu elektronisko komunikāciju pakalpojuma sniedzējs var apstrādāt 1. punktā minēto informāciju līdz līmenim un tik ilgi, cik nepieciešams šādiem pakalpojumiem vai tirdzniecībai, ja abonents vai lietotājs, uz kuru šī informācija attiecas, pirms tam ir devis savu piekrišanu. Lietotājiem vai abonentiem dod iespēju jebkurā laikā atsaukt savu piekrišanu informācijas par datu plūsmu apstrādei.

[..]

5. Informācijas par datu plūsmu apstrāde saskaņā ar 1., 2., 3. un 4. punktu ir jāierobežo līdz personām, kas darbojas ar pilnvaru no publisko komunikāciju tīklu pakalpojumu sniedzējiem un tādu publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzējiem, kas apstrādā rēķinu sagatavošanas vai datu plūsmas pārvaldi, klientu pieprasījumus, pārkāpumu noteikšanu, elektronisko komunikāciju pakalpojumu tirdzniecību vai pievienotās vērtības pakalpojumu sniegšanu, un tā jāierobežo līdz līmenim, kas nepieciešams šādu darbību veikšanai."

20 Šīs direktīvas 9. panta "Atrašanās vietas dati, kas nav informācija par datu plūsmu" 1. punktā ir paredzēts:

"Ja var apstrādāt atrašanās vietas datus, kas nav informācija par datu plūsmu, attiecībā uz publisko komunikāciju tīklu vai publiski pieejamu elektronisko komunikāciju pakalpojumu lietotājiem vai abonentiem, šādus datus var apstrādāt tikai tad, kad tie ir padarīti anonīmi, vai ar lietotāju vai abonentu piekrišanu, līdz tādam līmenim un tik ilgi, cik nepieciešams, lai sniegtu pievienotās vērtības pakalpojumus. Pakalpojuma sniedzējam ir jāinformē lietotāji vai abonenti pirms to piekrišanas saņemšanas par apstrādājamajiem atrašanās vietas datu veidiem, ja dati nav informācija par datu plūsmu, par apstrādes nolūku un ilgumu un par to, vai šos datus pārsūtīs trešajai personai ar nolūku sniegt pievienotās vērtības pakalpojumu. [..]"

21 Minētās direktīvas 15. pantā "Direktīvas [95/46] dažu noteikumu piemērošana" ir noteikts:

"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 krimināl pārkāpumu vai elektroniskās komunikāciju sistēmas nevēlamas izmantošanas novēršanu, izmeklēšanu, noteikšanu un krimināl vajāšanu, kā noteikts Direktīvas [95/46] 13. panta 1. punktā. Tālab dalībvalstis, cita starpā, var pieņemt tiesību aktus, paredzot datu saglabāšanu ierobežotā laikposmā, kas pamatots ar šajā punktā noteiktajiem iemesliem. Visi šajā punktā minētie pasākumi ir saskaņā ar [Savienības] tiesību aktu vispārējiem principiem, tostarp tie[m], kas minēti Eiropas Savienības dibināšanas līguma 6. panta 1. un 2. punktā.

[..]

2. Direktīvas [95/46] III nodaļas noteikumus par tiesiskās aizsardzības līdzekļiem, atbildību un sankcijām piemēro, ņemot vērā valsts noteikumus, kas pieņemti saskaņā ar šo direktīvu, un ņemot vērā individuālās tiesības, kuras izriet no šīs direktīvas.

[..]"

Regula 2016/679

22 Regulas 2016/679 10. apsvērumā ir noteikts:

"Lai nodrošinātu konsekventu un augsta līmeņa aizsardzību fiziskām personām un novērstu šķēršļus personu datu apritei Savienībā, fiziskas personas tiesību un brīvību aizsardzības līmenim attiecībā uz šādu datu apstrādi visās dalībvalstīs vajadzētu būt vienādam. Visā Savienībā būtu jānodrošina noteikumu par fiziskas personas pamattiesību un brīvību aizsardzību attiecībā uz personas datu apstrādi vienveidīga piemērošana. [..]"

23 Šīs regulas 2. pantā ir noteikts:

"1. Šo regulu piemēro personas datu apstrādei, kas pilnībā vai daļēji veikta ar automatizētiem līdzekļiem, un tādu personas datu apstrādei, kuri veido daļu no kartotēkas vai ir paredzēti, lai veidotu daļu no kartotēkas, ja apstrādi neveic ar automatizētiem līdzekļiem.

2. Šo regulu nepiemēro personas datu apstrādei:

a) tādas darbības gaitā, kas neietilpst Savienības tiesību aktu darbības jomā;

b) ko īsteno dalībvalstis, veicot darbības, kas ir LES V sadaļas 2. nodaļas darbības jomā;

[..]

d) ko veic kompetentas iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināl sodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu.

[..]

4. Šī regula neskar Direktīvas [2000/31] piemērošanu, jo īpaši attiecībā uz minētās direktīvas 12.–15. panta noteikumiem par starpnieku pakalpojumu sniedzēju saistībām."

24 Minētās regulas 4. pantā ir paredzēts:

"Šajā regulā:

1) "personas dati" ir jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu ("datu subjekts"); identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem;

2) "apstrāde" ir jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana;

[..]."

25 Regulas 2016/679 5. pantā ir noteikts:

"1. Personas dati:

a) tiek apstrādāti likumīgi, godprātīgi un datu subjektam pārredzamā veidā ("likumīgums, godprātība un pārredzamība");

b) tiek vākti konkrētos, skaidros un leģitīmos nolūkos, un to turpmāku apstrādi neveic ar minētajiem nolūkiem nesavietojamā veidā; turpmāka apstrāde arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos saskaņā ar 89. panta 1. punktu nav uzskatāma par nesavietojamu ar sākotnējiem nolūkiem ("nolūka ierobežojumi");

c) ir adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams to apstrādes nolūkos ("datu minimizēšana");

d) ir precīzi un, ja vajadzīgs, atjaunināti; ir jāveic visi saprātīgi pasākumi, lai nodrošinātu, ka neprecīzi personas dati, ņemot vērā nolūkus, kādos tie tiek apstrādāti, bez kavēšanās tiktu dzēsti vai laboti ("precizitāte");

e) tiek glabāti veidā, kas pieļauj datu subjektu identifikāciju, ne ilgāk kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā; personas datus var glabāt ilgāk, ciktāl personas datus apstrādās tikai arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos saskaņā ar 89. panta 1. punktu, ar noteikumu, ka tiek īstenoti atbilstoši tehniski un organizatoriski pasākumi, kas šajā regulā paredzēti, lai aizsargātu datu subjekta tiesības un brīvības ("glabāšanas ierobežojums");

f) tiek apstrādāti tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus ("integritāte un konfidencialitāte").

[..]"

26 Šīs regulas 6. pants ir formulēts šādi:

"1. Apstrāde ir likumīga tikai tādā apmērā un tikai tad, ja ir piemērojams vismaz viens no turpmāk minētajiem pamatojumiem:

[..]

c) apstrāde ir vajadzīga, lai izpildītu uz pārzini attiecināmu juridisku pienākumu;

[..]

3. Šā panta 1. punkta c) un e) apakšpunktā minēto apstrādes pamatu nosaka ar:

a) Savienības tiesību aktiem; vai

b) dalībvalsts tiesību aktiem, kas piemērojami pārzinim.

Apstrādes nolūku nosaka minētajā juridiskajā pamatā [..] Minētajā juridiskajā pamatā var būt ietverti konkrēti noteikumi, lai pielāgotu šīs regulas noteikumu piemērošanu, cita starpā vispārēji nosacījumi, kas reglamentē pārziņa īstenotu apstrādes likumību; apstrādājamo datu veidi; attiecīgie datu subjekti; vienības, kurām personas dati var tikt izpausti, un mērķi, kādiem tie var tikt izpausti; apstrādes nolūka ierobežojumi; glabāšanas termiņi; un apstrādes darbības un apstrādes procedūras, tostarp pasākumi, lai nodrošinātu likumīgu un godprātīgu apstrādi, piemēram, citās konkrētās datu apstrādes situācijās, kas paredzētas IX nodaļā. Savienības vai dalībvalsts tiesību akti atbilst sabiedrības interešu mērķim un ir samērīgi ar izvirzīto leģitīmo mērķi.

[..]"

27 Minētās regulas 23. pantā ir paredzēts:

"1. Saskaņā ar Savienības vai dalībvalsts tiesību aktiem, kas piemērojami datu pārzinim vai apstrādātājam, ar leģislatīvu pasākumu var ierobežot to pienākumu un tiesību darbības jomu, kas paredzēti 12.-22. pantā un 34. pantā, kā arī 5. pantā, ciktāl tā noteikumi atbilst 12.-22. pantā paredzētajām tiesībām un pienākumiem, – ja ar šādu ierobežojumu tiek ievērota pamattiesību un pamatbrīvību būtība un tas demokrātiskā sabiedrībā ir nepieciešams un samērīgs, lai garantētu:

a) valsts drošību;

b) aizsardzību;

c) sabiedrisko drošību;

d) noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu vai saukšanu pie atbildības par tiem vai kriminālsodu izpildi, tostarp aizsardzību pret sabiedriskās drošības apdraudējumiem un to novēršanu;

e) citus svarīgus Savienības vai dalībvalsts vispārējo sabiedrības interešu mērķus, jo īpaši Savienībai vai dalībvalstij svarīgas ekonomiskās vai finanšu intereses, tostarp monetāros, budžeta un nodokļu jautājumus, sabiedrības veselību un sociālo nodrošinājumu;

f) tiesu neatkarības un tiesvedības aizsardzību;

g) reglamentētu profesiju ētikas kodeksu pārkāpumu novēršanu, izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem;

h) uzraudzības, pārbaudes vai regulatīvo funkciju, kas – pat, ja tikai epizodiski – ir saistīta ar oficiālu pilnvaru īstenošanu a) līdz e) un g) apakšpunktā minētajos gadījumos;

i) datu subjekta aizsardzību vai citu personu tiesību un brīvību aizsardzību;

j) civilprasību izpildi.

2. Jo īpaši – jebkurā leģislatīvā pasākumā, kas minēts 1. punktā, ietver konkrētus noteikumus attiecīgā gadījumā vismaz par:

a) nolūkiem, kādos veic apstrādi, vai apstrādes kategorijām;

b) personas datu kategorijām;

c) ieviesto ierobežojumu darbības jomu;

d) garantijām, lai novērstu ļaunprātīgu izmantošanu vai nelikumīgu piekļuvi vai nosūtīšanu;

e) pārziņa vai pārziņu kategoriju noteikšanu;

f) glabāšanas laikposmiem un piemērojamām garantijām, ņemot vērā apstrādes vai apstrādes kategoriju raksturu, darbības jomu un nolūkus;

g) riskiem attiecībā uz datu subjektu tiesībām un brīvībām; un

h) datu subjektu tiesībām saņemt informāciju par ierobežojumu, izņemot tad, ja tas var kaitēt ierobežojuma mērķim."

28 Saskaņā ar minētās regulas 79. panta 1. punktu:

"Neskarot pieejamos administratīvos vai ārpustiesas tiesību aizsardzības līdzekļus, tai skaitā tiesības iesniegt sūdzību uzraudzības iestādē, ievērojot 77. pantu, ikvienam datu subjektam ir tiesības uz efektīvu tiesību aizsardzību tiesā, ja viņš uzskata, ka viņa tiesības saskaņā ar šo regulu ir pārkāptas, tādas viņa personas datu apstrādes rezultātā, kura neatbilst šai regulai."

29 Saskaņā ar Regulas 2016/679 94. pantu:

"1. Direktīvu [95/46] atceļ no 2018. gada 25. maija.

2. Atsauces uz atcelto direktīvu uzskata par atsaucēm uz šo regulu. Atsauces uz Darba grupu personu aizsardzībai attiecībā uz personas datu apstrādi, kas izveidota ar Direktīvas [95/46] 29. pantu, uzskata par atsaucēm uz Eiropas Datu aizsardzības kolēģiju, kas izveidota ar šo regulu."

30 Šīs regulas 95. pantā ir noteikts:

"Šī regula neuzliek papildu pienākumus fiziskām vai juridiskām personām attiecībā uz apstrādi saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiskos komunikāciju tīklos Savienībā jautājumos, saistībā ar kuriem tām ir piemērojami Direktīvas [2002/58] īpašie noteikumi ar to pašu mērķi."

Francijas tiesības

Iekšējās drošības kodekss

31 Iekšējā drošības kodeksa (turpmāk tekstā – "IDK") likumdošanas daļas VIII daļas L. 801-1. līdz L. 898-1. pantā ir paredzēti noteikumi par izlūkdatu ievākšanu.

32 IDK L. 811.-3. pantā ir noteikts:

"Lai veiktu attiecīgos uzdevumus, specializētie izlūkdienesti var izmantot šīs daļas V sadaļā minētās metodes izlūkdatu iegūšanai, kas attiecas uz šādu nācijas pamatinterešu aizsardzību un veicināšanu:

1° Valsts neatkarība, teritorijas integritāte un valsts aizsardzība;

2° Svarīgākās ārpolitikas intereses, Francijas Eiropas un starptautisko saistību izpilde un jebkāda veida ārvalstu iejaukšanās novēršana;

3° Francijas svarīgākās ekonomiskās, rūpnieciskās un zinātniskās intereses;

4° Terorisma novēršana;

5° Preventīva rīcība attiecībā uz:
   a) kaitējumu iestāžu republikāniskajai formai;
   b) darbībām likvidēto grupu, piemērojot L. 212-1. pantu, uzturēšanai vai atjaunošanai;
   c) pūļa vardarbību, kas var nopietni apdraudēt sabiedrisko mieru;

6° Organizētas noziedzības un pārkāpumu novēršanu;

7° Masu iznīcināšanas ieroču izplatīšanas novēršanu."

33 IDK L. 811-4. pantā ir noteikts:

"*Conseil d'État* [Valsts padome] dekrētā, kas ir pieņemts pēc *Commission nationale de contrôle des techniques de renseignement* [Nacionālā izlūkdatu vākšanas metožu kontroles komisija] atzinuma, ir noteikti dienesti, kas nav speciālie izlūkdienesti un kas atrodas aizsardzības ministra, iekšlietu ministra un tieslietu ministra, kā arī par ekonomiku, budžetu vai muitu atbildīgo ministru pakļautībā, kuriem var tikt atļauts izmantot šīs daļas V sadaļā minētās metodes saskaņā ar šajā pašā daļā paredzētajiem nosacījumiem. Tajā attiecībā uz katru dienestu ir precizēti L. 811-3. pantā minētie mērķi un metodes, kas var būt pamats atļaujas saņemšanai."

34 IDK L. 821-1. panta pirmajā daļā ir precizēts:

"Šīs daļas V sadaļas I līdz IV nodaļā minēto izlūkdatu vākšanas metožu izmantošanai valsts teritorijā ir nepieciešama premjerministra iepriekšēja atļauja, kas tiek izsniegta pēc Nacionālās izlūkdatu vākšanas metožu kontroles komisijas atzinuma."

35 IDK L. 821-2. pantā ir paredzēts:

"L. 821-1. pantā minēto atļauju izsniedz, pamatojoties uz rakstisku un pamatotu aizsardzības ministra, iekšlietu ministra, tieslietu ministra vai par ekonomiku, budžetu vai muitu atbildīgo ministru pieteikumu. Katrs ministrs var deleģēt šo piešķiršanu individuāli vienīgi tiem tiešajiem līdzstrādniekiem, kuriem ir piešķirta valsts aizsardzības noslēpuma atļauja.

Pieteikumā precizē:

1° Īstenojamo metodi vai metodes;

2° Dienestu, attiecībā uz kuru tas ir iesniegts;

3° Vēlamo mērķi vai mērķus;

4° Pasākuma pamatojumu;

5° Atļaujas derīguma termiņu;

6° Attiecīgo personu vai personas, vietu vai vietas vai transportlīdzekli.

Piemērojot 6. punktu, personas, kuru identitāte nav zināma, var noteikt pēc to identifikatora vai pazīmēm, un vietas vai transportlīdzekļus var noteikt saistībā ar pieteikumā norādītajām personām.

[..]"

36 Saskaņā ar IDK L. 821-3. panta pirmo daļu:

"Pieteikumu nosūta priekšsēdētājam vai, ja tas nav iespējams, kādam no L. 831-1. panta 2. un 3. punktā minētajiem Nacionālās izlūkdatu vākšanas metožu kontroles komisijas locekļiem, kurš sniedz atzinumu premjerministram divdesmit četru stundu laikā. Ja pieteikumu izskata slēgtā sastāvā vai komisijas plēnumā, par to nekavējoties informē premjerministru, un atzinums tiek sniegts septiņdesmit divu stundu laikā."

37 IDK L. 821-4. pantā ir noteikts:

"Atļauju šīs daļas V sadaļas I līdz IV nodaļā minēto metožu izmantošanai izsniedz premjerministrs uz laiku, kas nepārsniedz četrus mēnešus. [..] Atļaujā ietver L. 821-2. panta 1.–6. punktā paredzēto pamatojumu un norādes. Ikvienu atļauju var pagarināt saskaņā ar tiem pašiem nosacījumiem, kas paredzēti šajā nodaļā.

Ja atļauja tiek izsniegta pēc Nacionālās izlūkdatu vākšanas metožu kontroles komisijas noraidoša atzinuma, tajā norāda iemeslus, kuru dēļ šis atzinums nav ticis ievērots.

[..]"

38 IDK L. 833-4. pantā, kas ir ietverts šīs sadaļas III nodaļā, ir noteikts:

"Pēc savas ierosmes vai, saņemot sūdzību no jebkuras personas, kura vēlas pārbaudīt, vai attiecībā uz viņu nav nelikumīgi izmantota kāda izlūkdatu ievākšanas metode, komisija pārbauda minēto metodi vai metodes, lai pārliecinātos, ka tās tika vai tiek izmantotas atbilstoši šai daļai. Tā paziņo sūdzības iesniedzējam, ka tā ir veikusi vajadzīgās pārbaudes, neapstiprinot un neatceļot to izmantošanu."

39 IDK L. 841-1. panta pirmās un otrās daļas redakcija ir šāda:

"Ievērojot šā kodeksa L. 854-9. pantā paredzētos īpašos noteikumus, *Conseil d'État* kompetencē ir izskatīt prasības pieteikumus par šīs daļas V sadaļā minēto izlūkdatu ievākšanas metožu izmantošanu atbilstoši Administratīvā procesa kodeksa VII daļas VII sadaļas III *bis* nodaļā paredzētajiem nosacījumiem.

Tajā var vērsties:

1° Jebkura persona, kas vēlas pārliecināties, ka attiecībā uz viņu nav nelikumīgi izmantota neviena izlūkdatu ievākšanas metode, un kura pamato L. 833-4. pantā paredzētās procedūras iepriekšēju izmantošanu;

2° Nacionālā izlūkdatu vākšanas metožu kontroles komisija saskaņā ar L. 833-8. pantā paredzētajiem nosacījumiem."

40 IDK likumdošanas daļas VIII daļas V sadaļā, kas attiecas uz "izlūkdatu ievākšanas metodēm, kurām vajadzīga atļauja", tostarp ir ietverta I nodaļa "Administratīvā piekļuve pieslēguma datiem", kurā ir IDK L. 851-1. līdz L. 851-7. pants.

41 IDK L. 851-1. pantā ir noteikts:

"Šīs daļas II sadaļas I nodaļā paredzētajos apstākļos no elektronisko komunikāciju operatoriem un no personām, kas ir minētas [*CPCE*] L. 34-1. pantā, kā arī personām, kas ir minētas *loi n.º 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* [(2004. gada 21. jūnija Likuma Nr. 2004-575 par uzticēšanās veicināšanu digitālajā ekonomikā)] [(2004. gada 22. jūnija *JORF*, 11168. lpp.)] 6. panta I punkta 1. un 2. apakšpunktā, var vākt informāciju vai dokumentus, kas tiek apstrādāti vai saglabāti to tīklos vai elektronisko komunikāciju pakalpojumos, tai skaitā tehniskus datus saistībā ar abonenta vai pieslēguma elektronisko komunikāciju pakalpojumiem numuru noteikšanu, konkrētas personas visu abonenta vai pieslēguma numuru uzskaiti, izmantoto galaiekārtu atrašanās vietas datus, kā arī informāciju par abonenta komunikāciju, kas ietver izejošo un ienākošo zvanu numurus, komunikāciju ilgumu un datumu.

Atkāpjoties no L. 821-2. panta, rakstiskus un pamatotus lūgumus par tehniskajiem datiem saistībā ar abonenta numuru vai pieslēguma elektronisko komunikāciju pakalpojumiem identifikāciju vai visu sarakstā iekļautās personas abonenta vai pieslēguma numuru identificēšanu individuāli norīkoti un pilnvaroti L. 811.-2. un L. 811.-4. pantā minēto izlūkdienestu darbinieki tieši iesniedz Nacionālajai izlūkdatu vākšanas metožu kontroles komisijai. Komisija sniedz atzinumu atbilstoši L. 821-3. pantā paredzētajiem nosacījumiem.

Premjerministra dienesta pienākums ir iegūt informāciju vai dokumentus no šā panta pirmajā daļā minētajiem operatoriem un personām. Nacionālajai izlūkdatu vākšanas metožu kontroles komisijai ir pastāvīga, pilnīga, tieša un tūlītēja piekļuve savāktajai informācijai vai dokumentiem.

Šī panta īstenošanas noteikumi tiek noteikti ar *Conseil d'État* dekrētu, kas pieņemts pēc Nacionālās informātikas un brīvību komisijas un Nacionālās izlūkdatu vākšanas metožu kontroles komisijas atzinuma."

42 IDK L. 851-2. pantā ir noteikts:

"I – Saskaņā ar šīs daļas II sadaļas I nodaļā paredzētajiem nosacījumiem un vienīgi terorisma novēršanas nolūkā L. 851-1. pantā minēto operatoru un personu tīklos var tikt individuāli atļauta šajā pašā L. 851-1. pantā minētās informācijas vai dokumentu ievākšana par iepriekš identificētu personu, kas var būt saistīta ar draudiem. Ja ir nopietni iemesli uzskatīt, ka viena vai vairākas personas, kas ietilpst attiecīgās personas, uz kuru attiecas atļauja, lokā, var sniegt informāciju atbilstoši atļaujas mērķim, to var piešķirt arī par katru no šīm personām individuāli.

I *bis* Maksimālo atļauju skaitu, kas izsniegtas vienlaicīgi, piemērojot šo spēkā esošo pantu, nosaka premjerministrs, pamatojoties uz Nacionālās izlūkdatu vākšanas metožu kontroles komisijas atzinumu. Lēmumu, ar kuru nosaka šo kvotu, un tās sadalījumu starp L. 821-2. panta pirmajā daļā minētajiem ministriem, kā arī izsniegto aizturēšanas atļauju skaitu dara zināmu komisijai.

[..]"

43 IDK L. 851-3. pantā ir paredzēts:

"I – Saskaņā ar šīs daļas II sadaļas I nodaļā paredzētajiem nosacījumiem un tikai un vienīgi terorisma novēršanas vajadzībām L. 851-1. pantā minētajiem operatoriem un personām var tikt noteikts pienākums to tīklos veikt automatizētu apstrādi, kas, atkarībā no atļaujā precizētajiem parametriem, ir paredzēta, lai noteiktu pieslēgumus, kuri var atklāt terorisma draudus.

Šajā automatizētajā apstrādē izmanto vienīgi L. 851-1. pantā minēto informāciju vai dokumentus, neievācot citus datus kā tikai tos, kas atbilst automātiskās apstrādes izveides parametriem, un neļaujot identificēt personas, uz kurām šī informācija vai dokumenti attiecas.

Ievērojot samērīguma principu, premjerministra atļaujā ir precizēts šīs apstrādes veikšanas tehniskais apjoms.

II. – Nacionālā izlūkdatu vākšanas metožu kontroles komisija sniedz atzinumu par atļaujas pieteikumu attiecībā uz automatizētu apstrādi un izmantotajiem atklāšanas rādītājiem. Tai ir pastāvīga, pilnīga un tieša piekļuve šādai apstrādei, kā arī savāktajai informācijai un datiem. Tā ir informēta par jebkādām izmaiņām apstrādē un rādītājos, un tā var sniegt ieteikumus.

Pirmā atļauja veikt automatizēto apstrādi, kas paredzēta šā panta I daļā, tiek izsniegta uz diviem mēnešiem. Atļauju var pagarināt saskaņā ar nosacījumiem, kas paredzēti šīs daļas II sadaļas I nodaļā. Pagarināšanas pieteikumā ir iekļauts to identifikatoru saraksts, par kuriem tiek ziņots ar automatizēto apstrādi, un šo brīdinājumu atbilstības analīze.

III. – L. 871-6. pantā paredzētie nosacījumi ir piemērojami materiālām darbībām, ko šai īstenošanai veic L. 851-1. pantā minētie operatori un personas.

IV. – Ja šā panta I daļā minētā apstrāde atklāj datus, kas var liecināt par terorisma draudu esamību, premjerministrs vai kāda no tā pilnvarotajām personām, pamatojoties uz Nacionālās izlūkdatu vākšanas metožu kontroles komisijas atzinumu, kas sniegts saskaņā ar šīs daļas II sadaļas I nodaļā paredzētajiem nosacījumiem, var atļaut attiecīgās personas vai personu identifikāciju un ar to saistīto datu ievākšanu. Šie dati tiek izmantoti sešdesmit dienu laikā pēc šīs ievākšanas veikšanas un pēc šī termiņa beigām tiek iznīcināti, izņemot gadījumus, kad ir nopietni pierādījumi, kas apstiprina, ka pastāv ar vienu vai vairākām no attiecīgajām personām saistīti terorisma draudi.

[..]"

44 IDK L. 851-4. pants ir izteikts šādā redakcijā:

"Ievērojot šīs daļas II sadaļas I nodaļā paredzētos nosacījumus, L. 851-1. pantā minēto izmantoto galaiekārtu atrašanās vietas tehniskos datus var ievākt pēc tīkla pieprasījuma, un operatori tos var reāllaikā nodot premjerministra dienestam."

45 IDK R. 851-5. pantā, kas ir ietverts šī kodeksa normatīvajā daļā, ir paredzēts:

"I. – Informācija vai dokumenti, kas minēti L. 851-1. pantā, izņemot saziņas saturu vai izmantoto informāciju, ir:

1° Uzskaitīta [*CPCE*] R. 10-13. un R. 10-14. pantā un Dekrēta [Nr. 2011-219] 1. pantā.

2° Tehniskie dati, izņemot tos, kas minēti 1. punktā, kuri:

a) ļauj noteikt galaiekārtu atrašanās vietu;

b) ir saistīti ar piekļuvi tīkla galaiekārtām vai komunikāciju pakalpojumiem sabiedrībai tiešsaistē;

c) ir saistīti ar elektronisko komunikāciju pārraidīšanu tīklos;

d) ir saistīti ar lietotāja identifikāciju un autentifikāciju, savienošanu, tīklu vai komunikāciju pakalpojumu sabiedrībai tiešsaistē;

e) ir saistīti ar galaiekārtu īpašībām un to programmatūras konfigurācijas datiem.

II. – Piemērojot L. 851-1. pantu, var ievākt vienīgi I punkta 1. apakšpunktā minēto informāciju un dokumentus. Šī ievākšana notiek vēlāk.

I punkta 2. apakšpunktā uzskaitīto informāciju var ievākt, vienīgi piemērojot L. 851-2. un L. 851-3. pantu, ievērojot šajos pantos paredzētos nosacījumus un ierobežojumus un piemērojot R. 851-9. pantu."

CPCE

46 *CPCE* L. 34-1. pantā ir noteikts:

"I. – Šo pantu piemēro personas datu apstrādei, sniedzot sabiedrībai elektroniskās komunikācijas pakalpojumus; konkrēti – to piemēro tīkliem, kuros ir datu vākšanas un identifikācijas iekārtas.

II. – Elektronisko komunikāciju operatori un it īpaši personas, kas piedāvā sabiedrībai piekļuvi komunikāciju pakalpojumiem tiešsaistē, dzēš vai anonimizē visu informāciju par datu plūsmu, ja vien III, IV, V un VI punktā nav noteikts citādi.

Personas, kas sniedz elektronisko komunikāciju pakalpojumus sabiedrībai, saskaņā ar iepriekšējā rindkopā noteikto paredz iekšējās procedūras, lai izpildītu kompetento iestāžu pieprasījumus.

Personām, kuras, veicot savu galveno vai papildu uzņēmējdarbību, piedāvā sabiedrībai pieslēgumu, kas ar piekļuvi tīklam nodrošina komunikāciju tiešsaistē, pat bez maksas, ir pienākums ievērot tiesību normas, kuras saskaņā ar šo punktu piemērojamas elektronisko komunikāciju pakalpojumu sniedzējiem.

III. – Lai veiktu noziedzīgu nodarījumu vai *code de la propriété intellectuelle* [Intelektuālā īpašuma kodekss] L. 336-3. pantā noteiktā pienākuma neizpildes gadījumu izmeklēšanu, atklāšanu un kriminālvajāšanu par tiem vai lai novērstu Kriminālkodeksa 323-1. līdz 323-3-1. pantā minētos sodāmos uzbrukumus datu automātiskās apstrādes sistēmām, konkrētu datu kategoriju dzēšanas vai anonimizēšanas operācijas var atlikt uz laiku, kas nepārsniedz vienu gadu, ar vienīgo mērķi vajadzības gadījumā nodrošināt tos tiesu iestādei vai augstajai iestādei, kas minēta Intelektuālā īpašuma kodeksa L. 331-12. pantā, vai nacionālajai informācijas sistēmu drošības iestādei, kas minēta *code de la défense* [Aizsardzības kodekss] L. 2321-1. pantā. *Conseil d'État* dekrētā, kas ir pieņemts pēc Nacionālās informātikas un brīvību komisijas atzinuma, VI [nodaļā] paredzētajās robežās tiek noteiktas šīs datu kategorijas un to saglabāšanas ilgums atkarībā no operatoru darbības un komunikāciju rakstura, kā arī vajadzības gadījumā kārtība, kādā ir kompensējamas identificējamās un konkrētās papildizmaksas, kas rodas saistībā ar pakalpojumiem, kurus operatori tālab sniedz pēc valsts pieprasījuma.

[..]

VI. – Saskaņā ar III, IV un V punktā paredzētajiem nosacījumiem saglabāti un apstrādāti tiek tikai tie dati, kas attiecas uz operatoru sniegto pakalpojumu lietotāju identificēšanu, šo operatoru nodrošināto komunikāciju tehniskajiem parametriem un galaiekārtu atrašanās vietu.

Tie nekādā gadījumā un nekādā veidā neattiecas uz komunikāciju saturu vai šo komunikāciju laikā izmantoto informāciju.

Šo datu saglabāšanu un apstrādi veic saskaņā ar noteikumiem, kas paredzēti 1978. gada 6. janvāra Likumā Nr. 78-17 par informātiku, datnēm un brīvībām.

Operatori veic visus vajadzīgos pasākumus, lai novērstu šo datu izmantošanu šajā pantā neparedzētiem mērķiem."

47 *CPCE* R. 10-13. pants ir izteikts šādā redakcijā:

"I. – Piemērojot L. 34-1. panta III punktu, elektronisko komunikāciju operatori, lai izmeklētu, atklātu un veiktu kriminālvajāšanu par noziedzīgiem nodarījumiem, saglabā:

a) informāciju, kas ļauj identificēt lietotāju;

b) informāciju par izmantotajām komunikāciju galaiekārtām;

c) tehniskos parametrus, kā arī katras komunikācijas datumu, laiku un ilgumu;

d) datus par pieprasītajiem vai izmantotajiem papildu pakalpojumiem un šo pakalpojumu sniedzējiem;

e) datus, kas ļauj identificēt komunikācijas adresātu vai adresātus.

II. – Saistībā ar telefonijas darbībām operatoram ir jāsaglabā dati, kas ir norādīti II punktā un kas turklāt palīdz noteikt komunikācijas izcelsmi un atrašanās vietu.

III. – Šajā pantā minēto datu glabāšanas termiņš ir viens gads no reģistrācijas dienas.

IV. – Identificējamās un konkrētās papildizmaksas, kas rodas operatoriem, kuriem tiesu iestādes ir nosūtījušas pieprasījumu sniegt datus par šajā pantā minētajām kategorijām, tiek kompensētas atbilstoši Kriminālprocesa kodeksa R. 213-1. pantā paredzētajai kārtībai."

48 *CPCE* R. 10-14. pantā ir paredzēts:

"I. – Piemērojot L. 34-1. panta IV punktu, elektronisko komunikāciju operatoriem ir atļauts saglabāt norēķinu un samaksas darbību vajadzībām tehniska rakstura datus, kas ļauj identificēt lietotāju, kā arī R. 10-13. panta I punkta b), c) un d) apakšpunktā minētos datus.

II. – Telefonijas darbībām operatori papildus I punktā minētajiem datiem var saglabāt tehniska rakstura datus par komunikācijas atrašanās vietu, komunikācijas saņēmēja vai saņēmēju identifikāciju un datus, kas ļauj sagatavot rēķinu.

III. – Šī panta I un II punktā minētos datus drīkst saglabāt vienīgi tad, ja tie ir nepieciešami rēķinu sagatavošanai un samaksai par sniegtajiem pakalpojumiem. To glabāšana ir jāierobežo līdz šim mērķim absolūti nepieciešamajam laikam, nepārsniedzot vienu gadu.

IV. – Tīklu un iekārtu drošībai operatori var saglabāt ne ilgāk kā trīs mēnešus:

a) datus, kas ļauj identificēt komunikācijas avotu;

b) tehniskos parametrus, kā arī katras komunikācijas datumu, laiku un ilgumu;

c) tehniskus datus, kas ļauj identificēt komunikācijas adresātu vai adresātus;

d) datus par pieprasītajiem vai izmantotajiem papildu pakalpojumiem un šo pakalpojumu sniedzējiem."

Loi n.º 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (2004. gada 21. jūnija Likums Nr. 2004-575 par uzticēšanās veicināšanu digitālajā ekonomikā)

49 2004. gada 21. jūnija Likuma Nr. 2004-575 par uzticēšanās veicināšanu digitālajā ekonomikā (2004. gada 22. jūnija *JORF*, 11168. lpp.; turpmāk tekstā – "*LCEN*") 6. pantā ir paredzēts:

"I. – 1. Personas, kuru darbība ir piekļuves nodrošināšana komunikāciju pakalpojumiem tiešsaistē, informē savus abonentus par tehniskiem līdzekļiem, kas ļauj ierobežot piekļuvi noteiktiem pakalpojumiem vai tos atlasīt, un piedāvā tiem vismaz vienu no šiem līdzekļiem.

[..]

2. Fiziskām un juridiskām personām, kuras – pat bez maksas –, izmantojot publiskos komunikāciju pakalpojumus, nodrošina jebkāda veida signālu, teksta, attēlu, skaņu un ziņojumu, ko ir snieguši šo pakalpojumu adresāti, glabāšanu, lai darītu tos pieejamus sabiedrībai, nevar tikt sauktas pie civiltiesiskās atbildības par darbībām vai informāciju, kas uzglabāta pēc šo pakalpojumu saņēmēja pieprasījuma, ja tās faktiski nav zinājušas par to prettiesiskumu vai par faktiem un apstākļiem, kuri šķiet prettiesiski, vai arī, ja kopš brīža, kad tās par to ir uzzinājušas, tās ir veikušas atbilstošas darbības, lai šos datus izņemtu vai liegtu tiem pieeju.

[..]

II. – I punkta 1. un 2. apakšpunktā minētās personas tur un saglabā datus, kas ļauj identificēt jebkuru personu, kura ir piedalījusies to sniegto pakalpojumu satura vai tā daļas radīšanā.

Tās personām, kuras sniedz komunikācijas pakalpojumus sabiedrībai tiešsaistē, nodrošina tehniskos līdzekļus, kas ļauj tām izpildīt III daļā paredzētos identifikācijas nosacījumus.

Tiesu iestāde var pieprasīt I punkta 1. un 2. apakšpunktā minētajiem pakalpojumu sniedzējiem paziņot pirmajā daļā minētos datus.

Krimināl kodeksa 226-17., 226.-21. un 226.-22. panta noteikumi ir piemērojami šo datu apstrādei.

Conseil d'État dekrētā, kas pieņemts pēc Nacionālās informātikas un brīvību komisijas atzinuma, ir definēti pirmajā daļā minētie dati un noteikts to saglabāšanas ilgums un noteikumi.

[..]"

Dekrēts Nr. 2011-219

50 Dekrēta Nr. 2011-219 I nodaļā, kas pieņemta, pamatojoties uz *LCEN* 6. panta II punkta pēdējo daļu, ir ietverts šī dekrēta 1.–4. pants.

51 Dekrēta Nr. 2011-219 1. pantā ir noteikts:

"[*LCEN*] 6. panta II daļā minētie dati, kas personām ir jāsaglabā saskaņā ar šo pantu, ir šādi:

1° Attiecībā uz šī paša panta I daļas 1. punktā minētajām personām un attiecībā uz katru viņu abonentu pieslēgumu:

a) pieslēguma identifikators;

b) identifikators, kuru šīs personas piešķīrušas abonentam;

c) pieslēgumam izmantotā termināla identifikators, ja tām ir piekļuve tam;

d) pieslēguma sākuma un beigu datums un laiks;

e) abonenta līnijas parametri;

2° Personām, kas minētas I panta 2. punktā, un attiecībā uz katru izveidošanas darbību:

a) pieslēguma identifikators komunikācijas avotā;

b) darbības saturam piešķirtais identifikators, kas ir darbības priekšmets;

c) protokolu veidi, kas izmantoti, lai pieslēgtos pakalpojumam un pārsūtītu saturu;

d) darbības veids;

e) darbības datums un laiks;

f) darbības veicēja izmantotais identifikators, ja tas to ir sniedzis;

3° Attiecībā uz šī paša panta I daļas 1. un 2. punktā minētajām personām – informācija, ko sniedz lietotājs, noslēdzot līgumu vai izveidojot kontu:

a) pieslēguma identifikators, izveidojot kontu;

b) vārds, uzvārds vai uzņēmuma nosaukums;

c) piesaistītās pasta adreses;

d) izmantotie pseidonīmi;

e) elektroniskā pasta vai piesaistīto kontu adreses;

f) tālruņa numuri;

g) parole, kā arī atjaunotie dati, kas ļauj to pārbaudīt vai mainīt;

4° Personām, kas minētas šī paša panta I daļas 1. un 2. punktā, ja līguma noslēgšana vai konta atvēršana ir maksas, šāda informācija par katru maksājuma darījumu:

a) maksāšanas veids;

b) darījuma references numurs;

c) summa;

d) darījuma datums un laiks.

3.° un 4.° punktā minētie dati ir jāsaglabā tikai, ciktāl personas tos parasti vāc."

52 Šī dekrēta 2. pants ir formulēts šādi:

"Ieguldījums satura radīšanai ietver darbības, kas attiecas uz:

a) sākotnējo satura radīšanu;

b) satura un ar saturu saistīto datu izmaiņas;

c) satura liegšanu."

53 Minētā dekrēta 3. pantā ir paredzēts:

"1. pantā norādīto datu glabāšanas laiks ir viens gads:

a) Attiecībā uz 1.° un 2.° punktā minētajiem datiem, sākot no satura izveidošanas dienas, par katru darbību, kas veicina 2. pantā definētā satura izveidošanu;

b) Attiecībā uz 3.° punktā minētajiem datiem – no līguma izbeigšanas vai konta slēgšanas dienas;

c) Attiecībā uz 4.° punktā minētajiem datiem – par katru rēķinu vai maksājuma darījumu, sākot no rēķina izsniegšanas vai maksājuma darījuma datuma."

Beļģijas tiesības

54 Ar 2016. gada 29. maija likumu tostarp tika grozīts *loi du 13 juin 2005 relative aux communications électroniques* (2005. gada 13. jūnija likums par elektroniskajām komunikācijām) (*Moniteur belge*, 2005. gada 20. jūnijs, 28070. lpp.; turpmāk tekstā – "2005. gada 13. jūnija likums"), *code d'instruction criminelle* (Krimināllizmeklēšanas kodekss) un *loi du 30 novembre 1998 organique des services de renseignement et de sécurité* (1998. gada 30. novembra konstitutīvais likums par izlūkdienestiem un drošības dienestiem) (*Moniteur belge*, 1998. gada 18. decembris, 40312. lpp.; turpmāk tekstā – " 1998. gada 30. novembra likums").

55 2005. gada 13. jūnija likuma 126. pantā, redakcijā, kas izriet no 2016. gada 29. maija likuma, ir noteikts:

"1. § Ja vien 1992. gada 8. decembra likumā par privātās dzīves aizsardzību saistībā ar personas datu apstrādi nav noteikts citādi, subjekti, kas sabiedrībai sniedz telefonijas (tostarp ar interneta palīdzību), interneta piekļuves, elektroniskā pasta (izmantojot internetu) pakalpojumus, kā arī operatori, kas nodrošina publiskus elektronisko komunikāciju tīklus, un operatori, kas sniedz kādu no iepriekš minētajiem pakalpojumiem, saglabā 3. punktā minētos datus, kurus tie rada vai apstrādā saistībā ar attiecīgo komunikāciju pakalpojumu sniegšanu.

Šis pants neattiecas uz komunikācijas saturu.

Pienākums saglabāt 3. punktā minētos datus attiecas arī uz neveiksmīgiem zvaniem, ja šie dati saistībā ar attiecīgo komunikāciju pakalpojumu sniegšanu:

1° attiecas uz telefonijas datiem, ko iegūst vai apstrādā publiski pieejamu elektronisko komunikāciju pakalpojumu operatori vai publiski pieejamu elektronisko komunikāciju tīklu operatori, vai

2° attiecas uz interneta datiem, kurus ir iegrāmatojuši šie pakalpojumu sniedzēji.

2. § Tikai šādas iestādes, iesniedzot pieprasījumu, var iegūt no 1. punkta pirmajā daļā paredzētajiem pakalpojumu sniedzējiem un operatoriem datus, kas saglabāti saskaņā ar šo pantu, turpmāk norādītajiem mērķiem un saskaņā ar turpmāk izklāstītajiem nosacījumiem:

1° tiesu iestādes – lai veiktu izmeklēšanu, pierādījumu savākšanu un kriminālvajāšanu par noziedzīgiem nodarījumiem, īstenojot Kriminālizmeklēšanas kodeksa 46.a un 88.a pantā paredzētos pasākumus, ievērojot šajos pantos izklāstītos nosacījumus;

2° izlūkdienesti un drošības dienesti – lai pildītu izlūkošanas uzdevumus, izmantojot datu vākšanas metodes, kas paredzētas 1998. gada 30. novembra konstitutīvā likuma par izlūkdienestiem un drošības dienestiem 16/2., 18/7. un 18/8. pantā, ievērojot šajā likumā izklāstītos nosacījumus;

3° jebkurš [*Institut belge des services postaux et des telecomunications* (Beļģijas pasta un telekomunikāciju pakalpojumu institūts)] kriminālpolicijas darbinieks – lai atklātu un izmeklētu šī panta 114. un 124. pantā minētos pārkāpumus, kā arī veiktu kriminālvajāšanu par tiem;

4° neatliekamās palīdzības dienesti, kas sniedz palīdzību uz vietas, ja saistībā ar neatliekamās palīdzības zvanu tie neiegūst no attiecīgā pakalpojumu sniedzēja vai operatora zvanītāja identifikācijas datus, kas paredzēti 107. panta 2. punkta trešajā daļā, vai saņem nepilnīgus vai nepareizus datus. Var pieprasīt vienīgi zvanītāja identifikācijas datus, un tam jānotiek ne vēlāk kā 24 stundu laikā pēc izsaukuma;

5° kriminālpolicijas darbinieks Federālās policijas Bezvēsts pazudušo personu grupā – saistībā ar viņa pienākumu sniegt palīdzību briesmās esošai personai, meklēt cilvēkus, kuru pazušana ir satraucoša, un tad, ja ir pamatoti pieņēmumi vai nopietnas pazīmes, ka pastāv tieši draudi pazudušās personas fiziskajai drošībai. No attiecīgā operatora vai pakalpojumu sniedzēja – ar Karaļa izraudzītā policijas dienesta starpniecību – var pieprasīt vienīgi tos 3. punkta pirmajā un otrajā daļā minētos datus par pazudušu personu, kas saglabāti 48 stundu laikā pirms datu saņemšanas pieteikuma iesniegšanas;

6° telekomunikāciju ombuda dienests, lai identificētu personu, kura ir ļaunprātīgi izmantojusi elektronisko komunikāciju tīklu vai pakalpojumu, atbilstoši 1991. gada 21. marta Likuma par dažu valsts tautsaimniecības uzņēmumu reformu 43.*bis* panta 3. punkta 7.° apakšpunktā paredzētajiem nosacījumiem. Var pieprasīt vienīgi identifikācijas datus.

Šī panta 1. punkta pirmajā daļā minētie pakalpojumu sniedzēji un operatori nodrošina, ka šā panta 3. punktā minētā informācija ir neierobežoti pieejama no Beļģijas un ka šos datus un jebkādu citu nepieciešamo informāciju, kas saistīta ar šiem datiem, var nosūtīt nekavējoties un tikai šajā punktā paredzētajām iestādēm.

Ja vien citās tiesību normās nav noteikts citādi, 1. punkta pirmajā daļā minētie pakalpojumu sniedzēji un operatori nedrīkst izmantot saskaņā ar 3. punktu saglabātos datus kādiem citiem mērķiem.

3. § Datus, kas ļauj identificēt lietotāju vai abonentu un saziņas līdzekļus, izņemot datus, kas konkrēti paredzēti otrajā un trešajā daļā, saglabā divpadsmit mēnešus no dienas, kad komunikācija ar izmantotā pakalpojuma palīdzību bija iespējama pēdējo reizi.

Datus, kas attiecas uz galaiekārtas piekļuvi un savienojumu ar tīklu un pakalpojumu un uz šīs iekārtas atrašanās vietu, tostarp tīkla pieslēgumpunktu, saglabā divpadsmit mēnešus, skaitot no komunikācijas datuma.

Komunikācijas datus, kas neietver saturu, tostarp to izcelsmi un galamērķi, saglabā divpadsmit mēnešus, skaitot no komunikācijas datuma.

Karalis ar lēmumu, kas tiek pieņemts Ministru Padomē, pēc tieslietu ministra un [par elektronisko komunikāciju jautājumiem atbildīgā] ministra priekšlikuma, saņēmis Privātās dzīves aizsardzības komisijas un Institūta atzinumus, nosaka, kuri dati ir saglabājami atbilstoši pirmajā līdz trešajā daļā paredzētajām kategorijām, kā arī prasības, kādām šiem datiem ir jāatbilst.

[..]"

Pamatlietas un prejudiciālie jautājumi

Lieta C-511/18

56 Ar prasības pieteikumiem, kas iesniegti 2015. gada 30. novembrī un 2016. gada 16. martā un kas apvienoti pamattiesvedībā, *Quadrature du Net*, *French Data Network* un *Fédération des fournisseurs d'accès à Internet associatifs*, kā arī *Igwan.net* vērsās *Conseil d'État* (Valsts padome, Francija) ar prasību atcelt Dekrētus Nr. 2015-1185, Nr. 2015-1211, Nr. 2015-1639 un Nr. 2016-67, pamatojoties tostarp uz to, ka tajos neesot ievērota Francijas Konstitūcija, Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija (turpmāk tekstā – "ECPAK"), kā arī Direktīvas 2000/31 un 2002/58, tās lasot kopā ar Hartas 7., 8. un 47. pantu.

57 Konkrētāk, attiecībā uz pamatiem par Direktīvas 2000/31 neievērošanu iesniedzējtiesa norāda, ka IDK L. 851-3. pantā elektronisko komunikāciju operatoriem un tehnisko pakalpojumu sniedzējiem ir noteikts pienākums "savos tīklos veikt automatizētu apstrādi, kas atkarībā no atļaujā precizētajiem parametriem ir paredzēta, lai noteiktu pieslēgumus, kuri var atklāt terorisma draudus". Ar šo metodi vienīgi esot paredzēts ierobežotu laiku no visiem šo operatoru un šo pakalpojumu sniedzēju apstrādātajiem pieslēguma datiem vākt tos datus, kuriem varētu būt saikne ar šādu smagu pārkāpumu. Šādos apstākļos ar minētajām tiesību normām, kurās neesot noteikts vispārējs aktīvās uzraudzības pienākums, neesot pārkāpts Direktīvas 2000/31 15. pants.

58 Attiecībā uz pamatiem par Direktīvas 2002/58 neievērošanu iesniedzējtiesa uzskata, ka it īpaši no šīs direktīvas tiesību normām, kā arī no 2016. gada 21. decembra sprieduma *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, turpmāk tekstā – "spriedums *Tele2*", EU:C:2016:970) izriet, ka valsts tiesību normas, kurās elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikti pienākumi, piemēram, informācijas par datu plūsmu un to lietotāju un abonentu atrašanās vietas datu visaptveroša un nediferencēta saglabāšana minētās direktīvas 15. panta 1. punktā minētajiem mērķiem, kuru skaitā ir valsts drošības, aizsardzības un sabiedrības drošības aizsardzība, ietilpst šīs pašas direktīvas piemērošanas jomā, ciktāl šis tiesiskais regulējums reglamentē minēto pakalpojumu sniedzēju darbību. Tas pats attiecoties uz tiesisko regulējumu, kas regulē valsts iestāžu piekļuvi datiem, kā arī to izmantošanu.

59 Iesniedzējtiesa no tā secina, ka Direktīvas 2002/58 piemērošanas jomā ietilpst gan no IDK L. 851-1. panta izrietošais saglabāšanas pienākums, gan minētā kodeksa L. 851-1., L. 851-2. un L. 851-4. pantā paredzētā administratīvā piekļuve šiem datiem, tostarp reāllaikā. Kā uzskata šī tiesa, tas pats attiecas uz šī kodeksa L. 851-3. panta normām, kas – lai gan tajās attiecīgajiem operatoriem nav uzlikts vispārējs saglabāšanas pienākums – tiem tomēr liek savos tīklos īstenot automatizētu apstrādi, kuras mērķis ir atklāt pieslēgumus, kuri var būt saistīti ar terorisma draudiem.

60 Savukārt šī tiesa uzskata, ka Direktīvas 2002/58 piemērošanas jomā neietilpst prasībās atcelt tiesību aktus norādītie IDK noteikumi, kuri attiecas uz tādām izlūkdatu iegūšanas metodēm, ko valsts veic tieši, nevis reglamentējot elektronisko komunikāciju pakalpojumu sniedzēju darbību, viņiem uzliekot

īpašus pienākumus. Līdz ar to nevar tikt uzskatīts, ka ar šīm normām tiek īstenotas Savienības tiesības, un tādējādi nevarot lietderīgi izvirzīt pamatus, ar kuriem tiek apgalvots, ka nav ievērota Direktīva 2002/58.

61 Līdz ar to, lai atrisinātu strīdus par Dekrētu Nr. 2015-1185, Nr. 2015-1211, Nr. 2015-1639 un Nr. 2016-67 tiesiskumu, ņemot vērā Direktīvu 2002/58, ciktāl tie pieņemti IDK L. 851-1. līdz L. 851-4. panta īstenošanai, rodoties trīs Savienības tiesību interpretācijas jautājumi.

62 Attiecībā uz Direktīvas 2002/58 15. panta 1. punkta interpretāciju iesniedzējtiesa vēlas noskaidrot, pirmkārt, vai visaptverošas un nediferencētas saglabāšanas pienākums, kas elektronisko komunikāciju pakalpojumu sniedzējiem ir uzlikts, pamatojoties uz IDK L. 851-1. un R. 851-5. pantu, it īpaši, ņemot vērā garantijas un kontroles, kam ir pakārtota administratīvā piekļuve pieslēguma datiem un to izmantošana, nav uzskatāms par iejaukšanos, ko attaisno Hartas 6. pantā garantētās tiesības uz drošību un valsts drošības prasības, par kurām atbilstoši LES 4. pantam ir atbildīgas vienīgi dalībvalstis.

63 Otrkārt, attiecībā uz citiem pienākumiem, kas var tikt noteikti elektronisko komunikāciju pakalpojumu sniedzējiem, iesniedzējtiesa norāda, ka IDK L. 851-2. panta noteikumi ļauj vākt šī kodeksa L. 851-1. pantā minēto informāciju vai dokumentus no šīm pašām personām tikai un vienīgi terorisma novēršanas vajadzībām. Šī vākšana, kas attiecoties vienīgi uz vienu vai vairākām personām, kas iepriekš identificētas kā personas, kuras tiek turētas aizdomās par saikni ar terorisma draudiem, tiekot veikta reāllaikā. Tas pats attiecoties uz minētā kodeksa L. 851-4. pantu, kurā operatoriem reāllaikā ir ļauts pārsūtīt vienīgi tehniskus datus par galaiekārtu atrašanās vietu. Šīs metodes dažādiem mērķiem un dažādā kārtībā reglamentējot administratīvo piekļuvi reāllaikā datiem, kas saglabāti atbilstoši *CPCE* un *LCEN*, tomēr nenosakot attiecīgajiem pakalpojumu sniedzējiem papildu saglabāšanas prasību salīdzinājumā ar to, kas esot nepieciešama rēķinu sagatavošanai un to pakalpojumu sniegšanai. Tāpat arī IDK L. 851-3. panta noteikumi, kuros pakalpojumu sniedzējiem ir paredzēts pienākums ieviest savos tīklos automatizētu savienojumu analīzi, neparedzot visaptverošu un nediferencētu saglabāšanu.

64 Pirmām kārtām, iesniedzējtiesa uzskata, ka gan visaptveroša un nediferencēta saglabāšana, gan piekļuve reāllaikā pieslēguma datiem kontekstā, kurā pastāv būtisks un pastāvīgs valsts drošības apdraudējums, kas ir it īpaši saistīts ar terorisma risku, nodrošina operacionālo lietderīgumu, kam nav ekvivalenta. Proti, visaptveroša un nediferencēta saglabāšana ļautu izlūkdienestiem piekļūt ar komunikācijām saistītajiem datiem, pirms tiek identificēti iemesli, kas ļauj uzskatīt, ka attiecīgā persona rada apdraudējumu sabiedriskajai drošībai, aizsardzībai vai valsts drošībai. Turklāt piekļuve pieslēgumu datiem reāllaikā ļaujot ar augstu reaģētspēju izsekot tādu personu rīcībai, kuras var radīt tiešus draudus sabiedriskajai kārtībai.

65 Otrām kārtām, IDK L. 851-3. pantā paredzētā metode, pamatojoties uz šajā nolūkā precīzi definētiem kritērijiem, ļaujot atklāt personas, kuru rīcība, ņemot vērā viņu komunikācijas veidus, var atklāt terorisma draudus.

66 Treškārt, attiecībā uz kompetento iestāžu piekļuvi saglabātajiem datiem iesniedzējtiesa vaicā, vai Direktīva 2002/58, to lasot Hartas kontekstā, ir jāinterpretē tādējādi, ka tajā visos gadījumos pieslēguma datu vākšanas likumība ir pakļauta prasībai par datu subjektu informēšanu, kad šāda informācija vairs nevar apdraudēt kompetento iestāžu veiktās izmeklēšanas vai arī šādas procedūras var tikt uzskatītas par likumīgām, ņemot vērā visas pārējās valsts tiesībās paredzētās procesuālās garantijas, ciktāl tās nodrošina tiesību uz tiesību aizsardzību efektivitāti.

67 Attiecībā uz šīm citām procesuālajām garantijām iesniedzējtiesa it īpaši precizē, ka jebkura persona, kura vēlas pārbaudīt, vai attiecībā uz viņu netiek nelikumīgi izmantota izlūkdatu ievākšanas metode, var vērsties *Conseil d'État* (Valsts padome) specializētajā sastāvā, kuram, ņemot vērā informāciju, kas tam ir paziņota ārpus sacīkstes procedūras, ir jāpārbauda, vai attiecībā uz pieteikuma iesniedzēju ir izmantota šāda metode un vai tā ir īstenota atbilstoši IDK VIII daļai. Pilnvaras, kuras šim sastāvam esot piešķirtas, lai izskatītu pieteikumus, nodrošinot tā veiktās pārbaudes tiesā efektivitāti. Tādējādi tam esot

pilnvaras izskatīt prasības, pēc savas ierosmes konstatēt visus pārkāpumus un likt valsts pārvaldei veikt visus vajadzīgos pasākumus, lai novērstu konstatētos pārkāpumus. Turklāt Nacionālajai izlūkdatu iegūšanas metožu kontroles komisijai esot jāpārbauda, vai izlūkdatu ievākšanas metodes valsts teritorijā tiek īstenotas saskaņā ar prasībām, kas izriet no IDK. Tādējādi apstāklis, ka pamatlietā apstrīdētajās tiesību normās nav paredzēta datu subjektu informēšana par tos skarošajiem uzraudzības pasākumiem, pats par sevi neesot uzskatāms par tiesību uz privātās dzīves neaizskaramību pārkāpumu.

68 Šādos apstākļos *Conseil d'État* nolēma apturēt tiesvedību un uzdot Tiesai šādus prejudiciālus jautājumus:

"1) Vai visaptverošas un nediferencētas saglabāšanas pienākums, kas pakalpojumu sniedzējiem ir uzlikts, pamatojoties uz Direktīvas [2002/58] 15. panta 1. punkta atļaujošajām normām, kontekstā, kurā pastāv būtiski un pastāvīgi valsts drošības apdraudējumi un it īpaši terorisma risks, ir uzskatāms par iejaukšanos, ko attaisno [Hartas] 6. pantā garantētās tiesības uz drošību un valsts drošības prasības, par kurām atbilstoši [LES] 4. pantam ir atbildīgas vienīgi dalībvalstis?

2) Vai Direktīva [2002/58], to lasot [Hartas] gaismā, ir jāinterpretē tādējādi, ka tajā ir atļauti tādi likumdošanas pasākumi kā informācijas par datu plūsmu un noteiktu personu atrašanās vietas datu vākšana reāllaikā, kuri, lai gan tie ietekmē elektronisko komunikāciju pakalpojumu sniedzēju tiesības un pienākumus, tiem tomēr neuzliek konkrētu pienākumu saglabāt viņu datus?

3) Vai Direktīva [2002/58], to lasot [Hartas] gaismā, ir jāinterpretē tādējādi, ka tajā visos gadījumos pieslēguma datu vākšanas procedūru likumība ir pakļauta prasībai par attiecīgo personu informēšanu, kad šāda informācija vairs nevar apdraudēt kompetento iestāžu veiktās izmeklēšanas, vai arī šādas procedūras var tikt uzskatītas par likumīgām, ņemot vērā visas pārējās pastāvošās procesuālās garantijas, ciktāl tās nodrošina, ka tiesības uz tiesību aizsardzību ir efektīvas?"

Lieta C-512/18

69 Ar prasības pieteikumu, kas iesniegts 2015. gada 1. septembrī, *French Data Network*, *Quadrature du Net* un *Fédération des fournisseurs d'accès à Internet associatifs* vērsās *Conseil d'État* (Valsts padome) ar prasību atcelt netiešo lēmumu, kurš izriet no tā, ka premjerministrs nav sniedzis atbildi uz viņu lūgumu atcelt *CPCE* R. 10-13. pantu, kā arī Dekrētu Nr. 2011-219, pamatojoties it īpaši uz to, ka ar šiem tiesību aktiem esot pārkāpts Direktīvas 2002/58 15. panta 1. punkts, to lasot Hartas 7., 8. un 11. panta kontekstā. *Privacy International*, kā arī *Center for Democracy and Technology* tika atļauts iestāties pamatlietā.

70 Attiecībā uz *CPCE* R. 10-13. pantu un tajā paredzēto pienākumu visaptveroši un nediferencēti saglabāt ar komunikācijām saistītos datus, iesniedzējtiesa, kura pauž lietā C-511/18 izteiktajiem apsvērumiem līdzīgus apsvērumus, norāda, ka šāda saglabāšana ļauj tiesu iestādei piekļūt ar datiem, kas saistīti ar komunikācijām, kuras persona veikusi, pirms tā tika turēta aizdomās par noziedzīga nodarījuma izdarīšanu, tādējādi šādai saglabāšanai ir lietderīgums, kam nav ekvivalenta, lai izmeklētu un atklātu noziedzīgus nodarījumus, kā arī veiktu kriminālvajāšanu par tiem.

71 Attiecībā uz Dekrētu Nr. 2011-219 iesniedzējtiesa uzskata, ka *LCEN* 6. panta II daļa, kurā ir noteikts pienākums turēt un saglabāt vienīgi tos datus, kas attiecas uz satura radīšanu, ietilpst nevis Direktīvas 2002/58 piemērošanas jomā, jo saskaņā ar tās 3. panta 1. punktu tā attiecas vienīgi uz publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiskos komunikāciju tīklos Savienībā, bet gan Direktīvas 2000/31 piemērošanas jomā.

72 Šī tiesa tomēr uzskata, ka no Direktīvas 2000/31 15. panta 1. un 2. punkta izriet, ka ar to netiek ieviests principiāls aizliegums saglabāt datus, kuri attiecas uz satura radīšanu, no kā varētu atkāpties tikai izņēmuma kārtā. Tādējādi rodoties jautājums, vai minētās direktīvas 12., 14. un 15. pants, tos lasot

Hartas 6., 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, ir jāinterpretē tādējādi, ka tajos dalībvalstij ir ļauts pieņemt valsts tiesisko regulējumu, kāda ir *LCEN* 6. panta II daļa, ar ko attiecīgajām personām ir likts saglabāt datus, kuri var ļaut identificēt jebkādu personu, kas ir piedalījusies tās sniegto pakalpojumu satura vai daļas no satura radīšanā, lai tiesu iestāde vajadzības gadījumā no tām varētu pieprasīt šos datus ar nolūku nodrošināt, ka tiek ievēroti noteikumi par civiltiesisko atbildību vai krimināltatbildību.

73 Šādos apstākļos *Conseil d'État* nolēma apturēt tiesvedību un uzdot Tiesai šādus prejudiciālus jautājumus:

"1) Vai visaptverošas un nediferencētas saglabāšanas pienākums, kas pakalpojumu sniedzējiem ir uzlikts, pamatojoties uz Direktīvas [2002/58] 15. panta 1. punkta atļaujošajām normām, it īpaši, ņemot vērā garantijas un kontroles, kam šo datu vākšana un izmantošana ir pēc tam pakārtotas, ir uzskatāms par iejaukšanos, ko attaisno [Hartas] 6. pantā garantētās tiesības uz drošību un valsts drošības prasības, par kurām atbilstoši [LES] 4. pantam ir atbildīgas vienīgi dalībvalstis?

2) Vai Direktīvas [2000/31] noteikumi, tos lasot [Hartas] 6., 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, ir jāinterpretē tādējādi, ka tajos valstij ir ļauts paredzēt valsts tiesisko regulējumu, ar ko personām, kuru darbība sastāv no komunikāciju pakalpojumu piedāvāšanas sabiedrībai tiešsaistē, un fiziskām vai juridiskām personām, kuras – pat bez maksas –, lai darītu tos pieejamus sabiedrībai, izmantojot publiskos komunikāciju pakalpojumus tiešsaistē, nodrošina jebkāda veida signālu, teksta, attēlu, skaņu vai ziņojumu, ko snieguši šo pakalpojumu adresāti, glabāšanu, ir likts saglabāt datus, kas var ļaut identificēt jebkādu personu, kura ir piedalījusies tās sniegto pakalpojumu satura vai tā daļas radīšanā, lai tiesu iestāde vajadzības gadījumā no tām varētu pieprasīt šo datu paziņošanu nolūkā nodrošināt, ka tiek ievēroti noteikumi par civiltiesisko atbildību vai krimināltatbildību?"

Lieta C-520/18

74 Ar prasības pieteikumiem, kas iesniegti 2017. gada 10. janvārī, 16. janvārī, 17. janvārī un 18. janvārī un kas apvienoti pamattiesvedībā, *Ordre des barreaux francophones et germanophone*, *Académie Fiscale ASBL* un UA, *Liga voor Mensenrechten ASBL* un *Ligue des Droits de l'Homme ASBL*, kā arī VZ, WY un XX cēla prasību *Cour constitutionnelle* (Konstitucionālā tiesa, Beļģija), lūdzot atcelt 2016. gada 29. maija likumu, pamatojoties uz to, ka ar to esot pārkāpts Beļģijas Konstitūcijas 10. un 11. pants, tos lasot saistībā ar ECPAK 5., 6.–11., 14., 15., 17. un 18. pantu, Hartas 7., 8., 11. un 47. pantu, kā arī 52. panta 1. punktu, Starptautiskā pakta par pilsoniskajām un politiskajām tiesībām, ko Apvienoto Nāciju Organizācijas Ģenerālā asambleja pieņēma 1966. gada 16. decembrī un kas stājās spēkā 1976. gada 23. martā, 17. pantu, vispārējie tiesiskās drošības, samērīguma un pašnoteikšanās informācijas jomā principi, kā arī LES 5. panta 4. punkts.

75 Prasību pamatojumam prasītāji pamatlietā būtībā apgalvo, ka 2016. gada 29. maija likuma prettiesiskums it īpaši ir saistīts ar to, ka tas pārsniedz absolūti nepieciešamā robežas un tajā nav paredzētas pietiekamas aizsardzības garantijas. Konkrētāk, ne tā noteikumi par datu saglabāšanu, ne noteikumi, kas reglamentē iestāžu piekļuvi saglabātajiem datiem, neatbilstot prasībām, kas izriet no 2014. gada 8. aprīļa sprieduma *Digital Rights Ireland* u.c. (C-293/12 un C-594/12, turpmāk tekstā – "spriedums *Digital Rights*", EU:C:2014:238), un 2016. gada 21. decembra sprieduma *Tele2* (C-203/15 un C-698/15, EU:C:2016:970). Proti, šajās tiesību normās esot ietverts risks, ka tiks izveidoti personības profili ar no tiem izrietošo iespējamo ļaunprātīgo izmantošanu no kompetento iestāžu puses, un tajās arī neesot paredzēts atbilstošs saglabāto datu nodrošināšanas un aizsardzības līmenis. Visbeidzot, šis likums attiecoties uz personām, kuras ir saistītas ar dienesta noslēpumu, kā arī uz personām, kurām ir pienākums ievērot konfidencialitāti, un tas attiecoties uz sensitīviem personas komunikācijas datiem, neparedzot īpašas garantijas šo pēdējo minēto datu aizsardzībai.

76 Iesniedzējtiesa norāda, ka dati, kuri saskaņā ar 2016. gada 29. maija likumu ir jāsaglabā telefonijas pakalpojumu sniedzējiem, tostarp internetā, piekļuves internetam un elektroniskā pasta pakalpojumu sniedzējiem, kā arī operatoriem, kuri nodrošina publiskos elektronisko komunikāciju tīklus, ir identiski datiem, kas uzskaitīti Eiropas Parlamenta un Padomes Direktīvā 2006/24/EK (2006. gada 15. marts) 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 (OV 2006, L 105, 54. lpp.), nenošķirot atkarībā no datu subjektiem vai vēlamā mērķa. Šajā pēdējā ziņā šī tiesa precizē, ka likumdevēja ar šo likumu izvirzītais mērķis ir ne tikai cīnīties pret terorismu un bērnu pornogrāfiju, bet arī izmantot saglabātos datus visdažādākajās situācijās saistībā ar kriminālizmeklēšanu. Turklāt iesniedzējtiesa konstatē, ka no minētā likuma paskaidrojuma raksta izriet, ka valsts likumdevējs uzskatīja, ka, ņemot vērā izvirzīto mērķi, nav iespējams noteikt mērķorientētu un diferencētu saglabāšanas pienākumu, un izvēlējas visaptverošam un nediferencētam saglabāšanas pienākumam pievienot stingras garantijas – gan saglabāto datu ziņā, gan piekļuves tiem ziņā, lai līdz minimumam samazinātu iejaukšanos tiesībās uz privātās dzīves neaizskaramību.

77 Iesniedzējtiesa piebilst, ka 2005. gada 13. jūnija likuma 126. panta 2. punkta 1.° un 2.° apakšpunktā, redakcijā, kas izriet no 2016. gada 29. maija likuma, ir paredzēti nosacījumi, ar kādiem attiecīgi tiesu iestādes un izlūkdienesti un drošības dienesti var saņemt piekļuvi saglabātajiem datiem, līdz ar to šī likuma tiesiskuma pārbaude, ņemot vērā Savienības tiesību prasības, būtu jāaptur līdz brīdim, kad Tiesa pasludinās nolēmumus divās tajā notiekošajās prejudiciālā nolēmuma procedūrās, kas ir saistītas ar šādu piekļuvi.

78 Visbeidzot iesniedzējtiesa norāda, ka 2016. gada 29. maija likumā ir paredzēts arī ļaut veikt efektīvu kriminālizmeklēšanu un efektīvu sodīšanu par nepilngadīgo seksuālu izmantošanu un ļaut efektīvi identificēt šāda nozieguma izdarītāju, pat tad, ja viņš ir izmantojis elektroniskās komunikācijas līdzekļus. Tajā notiekošajā tiesvedībā uzmanība šajā ziņā esot pievērsta pozitīvajiem pienākumiem, kas izriet no ECPAK 3. un 8. panta. Šie pienākumi varot izrietēt arī no attiecīgajiem Hartas noteikumiem, kas varētu ietekmēt Direktīvas 2002/58 15. panta 1. punkta interpretāciju.

79 Šādos apstākļos *Cour constitutionnelle* nolēma apturēt tiesvedību un uzdot Tiesai šādus prejudiciālus jautājumus:

“1) Vai Direktīvas [2002/58] 15. panta 1. punkts, to aplūkojot kopsakarā ar [Hartas] 6. pantā garantētajām tiesībām uz drošību un [Hartas] 7., 8. pantā un 52. panta 1. punktā garantētajām tiesībām uz personas datu aizsardzību, ir jāinterpretē tādējādi, ka tas nepieļauj tādu valsts tiesisko regulējumu kā pamatlietā aplūkotais, kurā elektronisko komunikāciju pakalpojumu sniedzējiem un operatoriem ir noteikts vispārējs pienākums saglabāt informāciju par datu plūsmu un atrašanās vietas datus Direktīvas [2002/58] izpratnē, ko tie rada vai apstrādā saistībā ar šo pakalpojumu sniegšanu, ja valsts tiesiskā regulējuma mērķis ir ne tikai nodrošināt smagu noziegumu izmeklēšanu, atklāšanu un kriminālvajāšanu par tiem, bet arī sniegt valsts drošības, teritorijas aizsardzības un sabiedrības drošības garantijas, nodrošināt citu nodarījumu, kuri nav smagi noziegumi, izmeklēšanu, atklāšanu un kriminālvajāšanu par tiem, novērst elektronisko komunikāciju sistēmu neatļautu izmantošanu vai sasniegt kādu citu mērķi, kas noteikts Regulas [2016/679] 23. panta 1. punktā, turklāt to pakļaujot šajā pašā tiesiskajā regulējumā paredzētajām garantijām datu saglabāšanas ziņā un piekļuves šiem datiem ziņā?

2) Vai Direktīvas [2002/58] 15. panta 1. punkts, to aplūkojot kopsakarā ar [Hartas] 4., 7., 8., 11. pantu un 52. panta 1. punktu, ir jāinterpretē tādējādi, ka tas nepieļauj tādu valsts tiesisko regulējumu kā pamatlietā aplūkotais, kurā elektronisko komunikāciju pakalpojumu sniedzējiem un operatoriem ir noteikts vispārējs pienākums saglabāt informāciju par datu plūsmu un atrašanās vietas datus Direktīvas [2002/58] izpratnē, ko tie rada vai apstrādā saistībā ar šo pakalpojumu sniegšanu, ja šā regulējuma mērķis tostarp ir izpildīt pozitīvos pienākumus, kas iestādei izriet no Hartas 4. un

[7]. panta un kas liek izveidot tiesisko regulējumu, kurš ļautu veikt efektīvu kriminālizmeklēšanu un efektīvu sodīšanu par nepilngadīgo seksuālu izmantošanu un ļautu efektīvi identificēt nozieguma izdarītāju, pat tad, ja tiek izmantoti elektronisko komunikāciju līdzekļi?

3) Ja, pamatojoties uz atbildēm uz pirmo vai otro prejudiciālo jautājumu, *Cour constitutionnelle* [(Konstitucionālā tiesa)] secinātu, ka ar apstrīdēto likumu ir pārkāpts viens vai vairāki pienākumi, kas izriet no šajos jautājumos minētajām tiesību normām, vai tā varētu uz laiku saglabāt [2016. gada 29. maija] likuma sekas, lai izvairītos no tiesiskās nedrošības un ļautu iepriekš savāktos un saglabātos datus joprojām izmantot likumā paredzētajiem mērķiem?"

Par tiesvedību Tiesā

80 Ar Tiesas priekšsēdētāja 2018. gada 25. septembra lēmumu lietas C-511/18 un C-512/18 tika apvienotas rakstveida un mutvārdu procesā, kā arī sprieduma taisīšanai. Ar Tiesas priekšsēdētāja 2020. gada 9. jūlija lēmumu lieta C-520/18 tika pievienota šīm lietām sprieduma taisīšanai.

Par prejudiciālajiem jautājumiem

Par pirmajiem jautājumiem lietās C-511/18 un C-512/18, kā arī par pirmo un otro jautājumu lietā C-520/18

81 Ar pirmajiem jautājumiem lietās C-511/18 un C-512/18, kā arī ar pirmo un otro jautājumu lietā C-520/18, kuri ir jāizskata kopā, iesniedzējtiesas būtībā vēlas noskaidrot, vai Direktīvas 2002/58 15. panta 1. punkts ir jāinterpretē tādējādi, ka tam ir pretrunā tāds valsts tiesiskais regulējums, kurā elektronisko komunikāciju pakalpojumu sniedzējiem šajā 15. panta 1. punktā paredzētajiem mērķiem ir jāveic informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta saglabāšana.

Ievada apsvērumi

82 No Tiesas rīcībā esošajiem lietas materiāliem izriet, ka pamatlietā aplūkotais tiesiskais regulējums attiecas uz visiem elektroniskās komunikācijas līdzekļiem un aptver visus šo līdzekļu lietotājus, šajā ziņā nepiemērojot diferenciāciju vai izņēmumus. Turklāt dati, kas saskaņā ar šo tiesisko regulējumu ir jāsaglabā elektroniskās komunikācijas pakalpojumu sniedzējiem, konkrētāk, ir tie, kas ir nepieciešami, lai atrastu komunikācijas avotu un tās galamērķi, noteiktu komunikācijas datumu, laiku, ilgumu un veidu, identificētu izmantoto komunikācijas aprīkojumu, kā arī noteiktu galaiekārtas un komunikāciju veikšanas atrašanās vietu, datus, kuros tostarp ietilpst lietotāja vārds un adrese, zvanītāja un adresāta tālruņa numuri, kā arī interneta pakalpojumu IP adrese. Savukārt minētie dati neattiecas uz attiecīgās komunikācijas saturu.

83 Tādējādi dati, kas saskaņā ar pamatlietā aplūkoto valsts tiesisko regulējumu ir jāsaglabā vienu gadu, ļauj tostarp uzzināt, ar kuru personu elektroniskās komunikācijas līdzekļa lietotājs ir sazinājies un ar kādu līdzekli šī komunikācija ir notikusi, noteikt komunikācijas un pieslēgšanās internetam datumu, laiku un ilgumu, kā arī vietu, no kuras tie ir notikuši, un uzzināt galaiekārtu atrašanās vietu, ne vienmēr pārraidot pašu komunikāciju. Turklāt tās sniedz iespēju noteikt lietotāja komunikācijas ar noteiktām personām biežumu noteiktā laikposmā. Visbeidzot, attiecībā uz valsts tiesisko regulējumu, kas aplūkots lietās C-511/18 un C-512/18, šķiet, ka tas, tā kā tas attiecas arī uz datiem par elektronisko komunikāciju pārraidīšanu tīklos, ļauj arī identificēt tiešsaistē iegūtās informācijas raksturu.

84 Attiecībā uz izvirzītajiem mērķiem ir jānorāda, ka lietās C-511/18 un C-512/18 aplūkotais tiesiskais regulējums tostarp ir vērsts uz noziedzīgu nodarījumu izmeklēšanu, atklāšanu un kriminālvajāšanu vispārēji, valsts neatkarību, teritorijas integritāti un valsts aizsardzību, ārpolitikas sevišķi svarīgām interesēm, Francijas Eiropas un starptautisko saistību izpildi, svarīgām Francijas ekonomiskajām, rūpnieciskajām un zinātniskajām interesēm, kā arī terorisma novēršanu, kaitējumu iestāžu republikāniskajai formai un pūļa vardarbības, kas nopietni apdraud sabiedrības mieru, novēršanu. Tiesiskā regulējuma, kas tiek aplūkots lietā C-520/18, mērķi tostarp ir noziedzīgu nodarījumu izmeklēšana, atklāšana un kriminālvajāšana, kā arī valsts drošības, teritorijas aizsardzības un sabiedrības drošības aizsardzība.

85 Iesniedzējtiesas it īpaši jautā par Hartas 6. pantā nostiprināto tiesību uz drošību iespējamo ietekmi uz Direktīvas 2002/58 15. panta 1. punkta interpretāciju. Tāpat tās jautā, vai par pamatotu var uzskatīt iejaukšanos Hartas 7. un 8. pantā garantētajās pamattiesībās, ko rada datu saglabāšana, kas paredzēta pamatlietās aplūkotajā tiesiskajā regulējumā, ņemot vērā, ka pastāv noteikumi, kas ierobežo valsts iestāžu piekļuvi saglabātajiem datiem. Turklāt *Conseil d'État* uzskata, ka, tā kā šis jautājums rodas kontekstā, ko raksturo nopietni un pastāvīgi draudi valsts drošībai, tas arī ir jāizvērtē, ņemot vērā LES 4. panta 2. punktu. Savukārt *Cour constitutionnelle* uzsver, ka ar lietā C-520/18 aplūkoto valsts tiesisko regulējumu tiek īstenoti arī pozitīvie pienākumi, kas izriet no Hartas 4. un 7. panta, proti, paredzēt tiesisko regulējumu, kas ļauj efektīvi sodīt par nepilngadīgo seksuālu izmantošanu.

86 Kaut arī gan *Conseil d'État*, gan *Cour constitutionnelle* pamatojas uz pieņēmumu, ka pamatlietā aplūkotie valstu tiesiskie regulējumi, kuros ir reglamentēta informācijas par datu plūsmu un atrašanās vietas datu saglabāšana, kā arī valsts iestāžu piekļuve šiem datiem Direktīvas 2002/58 15. panta 1. punktā paredzētajiem mērķiem, piemēram, valsts drošības aizsardzības nolūkā, ietilpst šīs direktīvas piemērošanas jomā, atsevišķas pamatlietas puses un dažas dalībvalstis, kas ir iesniegušas rakstveida apsvērumus Tiesai, pauž atšķirīgu viedokli šajā ziņā, īpaši saistībā ar minētās direktīvas 1. panta 3. punkta interpretāciju. Tādējādi vispirms ir jāpārbauda, vai minētie tiesiskie regulējumi ietilpst šīs pašas direktīvas piemērošanas jomā.

Par Direktīvas 2002/58 piemērošanas jomu

87 *Quadrature du Net*, *Fédération des fournisseurs d'accès à Internet associatifs*, *Igwan.net*, *Privacy International* un *Center for Democracy and Technology*, šajā ziņā atsaucoties uz Tiesas judikatūru par Direktīvas 2002/58 piemērošanas jomu, būtībā apgalvo, ka gan datu saglabāšana, gan piekļuve saglabātajiem datiem ietilpst šajā piemērošanas jomā neatkarīgi no tā, vai šī piekļuve notiek vēlāk vai reāllaikā. Tā kā valsts drošības aizsardzības mērķis ir skaidri minēts šīs direktīvas 15. panta 1. punktā, šī mērķa sasniegšana neizraisītu minētās direktīvas nepiemērojamību. Iesniedzējtiesu minētais LES 4. panta 2. punkts neietekmējot šo vērtējumu.

88 Attiecībā uz datu vākšanas pasākumiem, kurus Francijas kompetentās iestādes īsteno tieši, nereglamentējot elektronisko komunikāciju pakalpojumu sniedzēju darbību, uzliekot tiem īpašus pienākumus, *Center for Democracy and Technology* norāda, ka šie pasākumi noteikti ietilpst Direktīvas 2002/58 un Hartas piemērošanas jomā, jo tie esot uzskatāmi par atkāpēm no šīs direktīvas 5. pantā garantētā konfidencialitātes principa. Līdz ar to minētajiem pasākumiem esot jāatbilst prasībām, kas izriet no tās 15. panta 1. punkta.

89 Savukārt Francijas, Čehijas un Igaunijas valdības, Īrija, Kipras, Ungārijas, Polijas, Zviedrijas un Apvienotās Karalistes valdības būtībā apgalvo, ka Direktīva 2002/58 nav piemērojama tādiem valsts tiesiskajiem regulējumiem kā pamatlietā, jo to mērķis ir valsts drošības aizsardzība. Izlūkdienestu darbības, ciktāl tās ir saistītas ar sabiedriskās kārtības uzturēšanu, kā arī iekšējās drošības un teritoriālās integritātes nodrošināšanu, ietilpstot dalībvalstu pamatfunkcijās, un līdz ar to tās esot vienīgi dalībvalstu kompetencē, kā to apliecinot tostarp LES 4. panta 2. punkta trešais teikums.

90 Šīs valdības, kā arī Īrija turklāt atsaucas uz Direktīvas 2002/58 1. panta 3. punktu, kurā no tās piemērošanas jomas, tāpat kā jau bija paredzēts Direktīvas 95/46 3. panta 2. punkta pirmajā ievilkumā, esot izslēgtas darbības, kas saistītas ar sabiedrības drošību, aizsardzību un valsts drošību. Šajā ziņā tās balstās uz šīs pēdējās minētās tiesību normas interpretāciju, kas sniegta 2006. gada 30. maija spriedumā Parlaments/Padome un Komisija (C-317/04 un C-318/04, EU:C:2006:346).

91 Šajā ziņā ir jānorāda, ka Direktīvas 2002/58 1. panta 1. punktā tostarp ir paredzēta to dalībvalstu tiesību normu saskaņošana, kas nepieciešamas, lai nodrošinātu pamattiesību un pamatbrīvību, jo īpaši tiesību uz privāto dzīvi un konfidencialitāti saistībā ar personas datu apstrādi elektronisko komunikāciju nozarē, līdzvērtīgu aizsardzības līmeni.

92 Ar šīs direktīvas 1. panta 3. punktu no tās piemērošanas jomas ir izslēgtas "valsts darbības" tajā norādītajās jomās, kuru vidū ir arī valsts darbības krimināltiesību jomā un darbības, kas attiecas uz sabiedrības drošību, aizsardzību un valsts drošību, tostarp valsts ekonomisko labklājību, ja darbības attiecas uz valsts drošības jautājumiem. Tajā par piemēru minētās darbības visos gadījumos ir valstu vai valstu iestāžu darbības, kas neietilpst privātpersonu darbības lokā (spriedums, 2018. gada 2. oktobris, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 32. punkts un tajā minētā judikatūra).

93 Turklāt Direktīvas 2002/58 3. pantā ir paredzēts, ka šī direktīva attiecas uz personas datu apstrādi saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiski pieejamos komunikāciju pakalpojumu tīklos Savienībā, tostarp publiski pieejamos komunikāciju tīklos, kuros var izmantot datu iegūšanas un identifikācijas ierīces (turpmāk tekstā – "elektronisko komunikāciju pakalpojumi"). Līdz ar to minētā direktīva ir jāuzskata par tādu, kas reglamentē šādu pakalpojumu sniedzēju darbības (spriedums, 2018. gada 2. oktobris, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 33. punkts un tajā minētā judikatūra).

94 Šajā saistībā Direktīvas 2002/58 15. panta 1. punktā dalībvalstīm ir atļauts, ievērojot tajā paredzētos nosacījumus, pieņemt "tiesību aktus, lai ierobežotu šīs direktīvas 5. un 6. pantā, 8. panta 1., 2., 3. un 4. punktā un [šīs direktīvas] 9. pantā minēto tiesību un pienākumu darbības jomu" (spriedums, 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 71. punkts).

95 Direktīvas 2002/58 15. panta 1. punktā kā obligāts priekšnosacījums ir izvirzīts, ka tajā paredzētajiem valsts tiesību aktiem ir jāietilpst šīs direktīvas piemērošanas jomā, jo tā skaidri dalībvalstīm tos pieņemt ļauj tikai tad, ja tiek ievēroti tajā paredzētie nosacījumi. Turklāt ar šādiem pasākumiem šajā tiesību normā minētajiem mērķiem tiek regulēta elektronisko komunikāciju pakalpojumu sniedzēju darbība (spriedums, 2018. gada 2. oktobris, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 34. punkts un tajā minētā judikatūra).

96 Tieši, ņemot vērā šos apsvērumus, Tiesa ir nospriedusi, ka Direktīvas 2002/58 15. panta 1. punkts, lasot kopsakarā ar tās 3. pantu, ir interpretējams tādējādi, ka šīs direktīvas piemērošanas jomā ietilpst ne tikai tādi tiesību akti, kuros elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums saglabāt informāciju par datu plūsmu un atrašanās vietas datus, bet arī tiesību akti, ar kuriem noteikts pienākums piešķirt piekļuvi šiem datiem kompetentajām valsts iestādēm. Šādi tiesību akti viennozīmīgi nosaka par pienākumu minētajiem pakalpojumu sniedzējiem apstrādāt minētos datus un, ciktāl tie reglamentē šo pašu pakalpojumu sniedzēju darbības, tie nevar tikt pielīdzināti minētās direktīvas 1. panta 3. punktā norādītajām valsts darbībām (šajā nozīmē skat. spriedumu, 2018. gada 2. oktobris, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 35. un 37. punkts, kā arī tajos minētā judikatūra).

97 Turklāt, ņemot vērā šī sprieduma 95. punktā minētos apsvērumus un Direktīvas 2002/58 vispārējo struktūru, ar tādu šīs direktīvas interpretāciju, saskaņā ar kuru tās 15. panta 1. punktā norādītie tiesību akti tiktu izslēgti no minētās direktīvas piemērošanas jomas, jo mērķi, kuriem šādiem tiesību aktiem jāatbilst, būtībā sakrīt ar šīs pašas direktīvas 1. panta 3. punktā minēto darbību mērķiem, šim 15. panta 1. punktam tiktu liegta jebkāda lietderīga iedarbība (šajā nozīmē skat. spriedumu, 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 72. un 73. punkts).

98 Tādējādi Direktīvas 2002/58 1. panta 3. punktā ietvertais jēdziens "darbības", kā to būtībā ir norādījis ģenerāladvokāts secinājumu apvienotajās lietās *La Quadrature du Net* u.c. (C-511/18 un C-512/18, EU:C:2020:6) 75. punktā, nevar tikt interpretēts kā tāds, kas attiecas uz šīs direktīvas 15. panta 1. punktā paredzētajiem tiesību aktiem.

99 LES 4. panta 2. punkta noteikumi, uz kuriem ir atsaukušās šī sprieduma 89. punktā minētās valdības, nevar atspēkot šo secinājumu. Lai gan saskaņā ar Tiesas pastāvīgo judikatūru dalībvalstīm ir kompetence noteikt to būtiskās drošības intereses un veikt pienācīgus pasākumus, lai nodrošinātu to iekšējo un ārējo drošību, tas fakts vien, ka valsts pasākums ir pieņemts valsts drošības aizsardzības nolūkos, nevar izraisīt Savienības tiesību nepiemērojamību un atbrīvot dalībvalstis no šo tiesību obligātas ievērošanas (šajā nozīmē skat. spriedumus, 2013. gada 4. jūnijs, ZZ, C-300/11, EU:C:2013:363, 38. punkts; 2018. gada 20. marts, Komisija/Austrija (Valsts drukātava), C-187/16, EU:C:2018:194, 75. un 76. punkts, kā arī 2020. gada 2. aprīlis, Komisija/Polija, Ungārija un Čehijas Republika (Starptautiskās aizsardzības pieteikuma iesniedzēju pagaidu pārcelšanas mehānisms), C-715/17, C-718/17 un C-719/17, EU:C:2020:257, 143. un 170. punkts).

100 Taisnība, ka 2006. gada 30. maija spriedumā Parlaments/Padome un Komisija (C-317/04 un C-318/04, EU:C:2006:346, 56.–59. punkts) Tiesa ir nospriedusi, ka personas datu nodošana, ko aviosabiedrības veic trešās valsts iestādēm, lai novērstu, kā arī apkarotu terorismu un citus smagus noziegumus, saskaņā ar Direktīvas 95/46 3. panta 2. punkta pirmo ievilkumu neietilpst šīs direktīvas piemērošanas jomā, jo šī nodošana ietilpst valsts varas noteiktajos ietvaros, kas attiecas uz sabiedrības drošību.

101 Tomēr, ņemot vērā šī sprieduma 93., 95. un 96. punktā ietvertos apsvērumus, šī judikatūra nav izmantojama Direktīvas 2002/58 1. panta 3. punkta interpretācijai. Kā to būtībā norādīja ģenerāladvokāts secinājumu apvienotajās lietās *La Quadrature du Net* u.c. (C-511/18 un C-512/18, EU:C:2020:6) 70.–72. punktā, ar Direktīvas 95/46, uz kuru ir atsauce minētajā judikatūrā, 3. panta 2. punkta pirmo ievilkumu no pēdējās minētās direktīvas piemērošanas jomas vispārēji ir izslēgtas "apstrādes operācijas attiecībā uz sabiedrisko drošību, aizsardzību, valsts drošību", nenošķirot atkarībā no attiecīgo datu apstrādes veicēja. Savukārt, interpretējot Direktīvas 2002/58 1. panta 3. punktu, šāda nošķiršana ir nepieciešama. Kā izriet no šī sprieduma 94.–97. punkta, visa personas datu apstrāde, ko veic elektronisko komunikāciju pakalpojumu sniedzēji, ietilpst minētās direktīvas piemērošanas jomā, tostarp arī apstrāde, kas izriet no pienākumiem, kurus tiem ir uzlikušas valsts iestādes, lai gan uz šo pēdējo minēto apstrādi attiecīgajā gadījumā varēja attiekties Direktīvas 95/46 3. panta 2. punkta pirmajā ievilkumā paredzētais izņēmums, ņemot vērā šīs tiesību normas plašāku formulējumu, kas attiecas uz visu apstrādi – neatkarīgi no tās veicēja – kuras priekšmets ir sabiedrības drošība, aizsardzība vai valsts drošība.

102 Turklāt ir jānorāda, ka Direktīva 95/46, kas tika aplūkota lietā, kurā tika pasludināts 2006. gada 30. maija spriedums Parlaments/Padome un Komisija (C-317/04 un C-318/04, EU:C:2006:346), saskaņā ar Regulas 2016/679 94. panta 1. punktu tika atcelta un aizstāta ar šo regulu no 2018. gada 25. maija. Lai gan minētās regulas 2. panta 2. punkta d) apakšpunktā ir precizēts, ka tā neattiecas uz apstrādi, ko "kompetentās iestādes" veic tostarp noziedzīgu nodarījumu novēršanas un atklāšanas nolūkā, tostarp aizsardzībai pret sabiedrības drošības apdraudējumiem un to novēršanu, no šīs pašas regulas 23. panta 1. punkta d) un h) apakšpunkta izriet, ka personas datu apstrāde, ko šiem pašiem mērķiem veic privātpersonas, ietilpst tās piemērošanas jomā. No tā ir secināms, ka iepriekš izklāstītā Direktīvas 2002/58 1. panta 3. punkta, 3. panta un 15. panta 1. punkta interpretācija atbilst Regulas 2016/679, ko šī direktīva papildina un precizē, piemērošanas jomas norobežošanai.

103 Savukārt, ja dalībvalstis tieši īsteno pasākumus, ar kuriem tiek izdarīta atkāpe no elektronisko komunikāciju konfidencialitātes, neuzliekot apstrādes pienākumus šādas komunikācijas pakalpojumu sniedzējiem, datu subjektu datu aizsardzība ir atkarīga nevis no Direktīvas 2002/58, bet gan vienīgi no valsts tiesībām, neskarot Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai

izpildītu krimināls odus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV 2016, L 119, 89. lpp.), piemērošanu, līdz ar to aplūkotajiem pasākumiem tostarp jāatbilst konstitucionāla līmeņa valsts tiesībām un ECPAK prasībām.

104 No iepriekš minētajiem apsvērumiem izriet, ka valsts tiesiskais regulējums, kurā elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums saglabāt tādu informāciju par datu plūsmu un atrašanās vietas datiem, kāda minēta pamatlietā, lai aizsargātu valsts drošību un apkarotu noziedzību, ietilpst Direktīvas 2002/58 piemērošanas jomā.

Par Direktīvas 2002/58 15. panta 1. punkta interpretāciju

105 Vispirms ir jāatgādina, ka saskaņā ar Tiesas pastāvīgo judikatūru, interpretējot Savienības tiesību normu, ir jāņem vērā ne tikai tās teksts, bet arī tās konteksts un šo normu ietverošā tiesiskā regulējuma mērķi un tostarp šī tiesiskā regulējuma izstrādāšanas vēsture (šajā nozīmē skat. spriedumu, 2018. gada 17. aprīlis, *Egenberger*, C-414/16, EU:C:2018:257, 44. punkts).

106 Direktīvas 2002/58 mērķis, kā tas tostarp izriet no tās 6. un 7. apsvēruma, ir vērsts uz to, lai aizsargātu elektronisko komunikāciju pakalpojumu lietotājus pret riskiem personas datiem un privātajai dzīvei, kas izriet no jaunajām tehnoloģijām un arvien lielākas jaudas datu automatizētai glabāšanai un apstrādei. Minētā direktīva, kā tas ir norādīts tās 2. apsvērumā, jo īpaši pilnībā nodrošina tiesības, kas izklāstītas Hartas 7. un 8. pantā. Šajā ziņā no priekšlikuma Eiropas Parlamenta un Padomes Direktīvai par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (COM(2000) 385, galīgā redakcija), kas ir Direktīvas 2002/58 pamatā, paskaidrojuma raksta izriet, ka Savienības likumdevējs ir vēlējies "rīkoties tādējādi, lai joprojām tiktu nodrošināts augsts personas datu un privātās dzīves aizsardzības līmenis attiecībā uz visiem elektroniskās komunikācijas pakalpojumiem neatkarīgi no izmantotās tehnoloģijas".

107 Šajā ziņā Direktīvas 2002/58 5. panta 1. punktā ir nostiprināts gan elektronisko komunikāciju, gan ar tām saistītās informācijas par datu plūsmu konfidencialitātes princips, un tajā tostarp ir paredzēts aizliegums principā visām personām, kas nav lietotāji, bez viņu piekrišanas uzglabāt šīs komunikācijas un šo informāciju.

108 It īpaši attiecībā uz informācijas par datu plūsmu apstrādi un uzglabāšanu, ko veic elektronisko komunikāciju pakalpojumu sniedzēji, no Direktīvas 2002/58 6. panta, kā arī 22. un 26. apsvēruma izriet, ka šāda apstrāde ir atļauta tikai tik lielā mērā un tik ilgi, cik nepieciešams pakalpojumu tirdzniecībai, rēķinu sagatavošanai par tiem un pievienotās vērtības pakalpojumu sniegšanai. Pēc šī laikposma beigām apstrādātie un uzglabātie dati ir jāizdzēš vai jāpadara anonīmi. Attiecībā uz atrašanās vietas datiem, kas nav informācija par datu plūsmu, minētās direktīvas 9. panta 1. punktā ir paredzēts, ka šos datus var apstrādāt tikai, ja izpildīti konkrēti nosacījumi, kad tie ir padarīti anonīmi, vai arī ar lietotāju vai abonentu piekrišanu (spriedums, 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 86. punkts un tajā minētā judikatūra).

109 Tādējādi, pieņemot šo direktīvu, Savienības likumdevējs ir konkretizējis Hartas 7. un 8. pantā paredzētās tiesības tādējādi, ka elektronisko komunikāciju līdzekļu lietotājiem principā ir tiesības sagaidīt, ka viņu komunikācijas un ar tām saistītie dati, ja nav viņu piekrišanas, paliek anonīmi un nevar tikt reģistrēti.

110 Tomēr Direktīvas 2002/58 15. panta 1. punktā dalībvalstīm ir atļauts ieviest izņēmumus no šīs direktīvas 5. panta 1. punktā paredzētā principa nodrošināt personas datu konfidencialitāti, kā arī no attiecīgajiem pienākumiem, kas it īpaši minēti minētās direktīvas 6. un 9. pantā, ja šāds ierobežojums ir nepieciešams, atbilstošs un samērīgs pasākums demokrātiskā sabiedrībā, lai garantētu valsts drošību, aizsardzību, sabiedrības drošību vai krimināl pārkāpumu vai elektroniskās komunikāciju sistēmas

nevēlamas izmantošanas novēršanu, izmeklēšanu, atklāšanu un kriminālvajāšanu. Šim nolūkam dalībvalstis tostarp var pieņemt tiesību aktus, paredzot datu saglabāšanu ierobežotā laikposmā, ja tas ir pamatots ar kādu no šiem iemesliem.

111 To paturot prātā, tiesības atkāpties no Direktīvas 2002/58 5., 6. un 9. pantā paredzētajām tiesībām un pienākumiem nevar pamatot to, ka par normu kļūst atkāpe no principiālā pienākuma nodrošināt elektronisko komunikāciju un ar tām saistīto datu konfidencialitāti un, it īpaši, atkāpe no aizlieguma uzglabāt šos datus, kas tieši paredzēts šīs direktīvas 5. pantā (šajā nozīmē skat. spriedumu, 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 89. un 104. punkts).

112 Saistībā ar mērķiem, kas var pamatot Direktīvas 2002/58 5., 6. un 9. pantā paredzēto tiesību un pienākumu ierobežojumu, Tiesa jau ir nospriedusi, ka šīs direktīvas 15. panta 1. punkta pirmajā teikumā ietvertais mērķu uzskaitījums ir izsmeļošs un tādēļ tiesību aktam, kas ir pieņemts atbilstoši šai normai, patiešām un stingri ir jāatbilst kādam no šiem mērķiem (šajā nozīmē skat. spriedumu, 2018. gada 2. oktobris, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 52. punkts un tajā minētā judikatūra).

113 Turklāt no Direktīvas 2002/58 15. panta 1. punkta trešā teikuma izriet, ka dalībvalstīm ir atļauts pieņemt tiesību aktus, lai ierobežotu šīs direktīvas 5., 6. un 9. pantā minēto tiesību un pienākumu apjomu, tikai, ievērojot Savienības tiesību vispārējos principus, tostarp samērīguma principu un Hartā garantētās pamattiesības. Šajā ziņā Tiesa jau ir nospriedusi, ka dalībvalsts ar valsts tiesisko regulējumu noteiktais pienākums elektronisko komunikāciju pakalpojumu sniedzējiem saglabāt informāciju par datu plūsmu, lai to vajadzības gadījumā padarītu pieejamu kompetentajām valsts iestādēm, izraisa jautājumus ne tikai par Hartas 7. un 8. panta ievērošanu, kuri attiecīgi ir saistīti ar privātās dzīves, kā arī ar personas datu aizsardzību, bet arī par Hartas 11. pantā garantēto vārda brīvību (šajā nozīmē skat. spriedumus, 2014. gada 8. aprīlis, *Digital Rights*, C-293/12 un C-594/12, EU:C:2014:238, 25. un 70. punkts, kā arī 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 91. un 92. punkts, kā arī tajos minētā judikatūra).

114 Tātad, interpretējot Direktīvas 2002/58 15. panta 1. punktu, ir jāņem vērā gan Hartas 7. pantā garantēto tiesību uz privātās dzīves neaizskaramību, gan arī tās 8. pantā garantēto tiesību uz personas datu aizsardzību nozīmīgums, kāds tas izriet no Tiesas judikatūras, kā arī vārda brīvības nozīmīgums – šīs pamattiesības, kas garantētas Hartas 11. pantā, veido vienu no demokrātiskas un plurālistiskas sabiedrības būtiskajiem pamatiem, kas ir starp tām vērtībām, uz kurām pamatojoties, saskaņā ar LES 2. pantu ir dibināta Savienība (šajā nozīmē skat. spriedumus, 2001. gada 6. marts, *Connolly*/Komisija, C-274/99 P, EU:C:2001:127, 39. punkts, kā arī 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 93. punkts un tajā minētā judikatūra).

115 Šajā ziņā ir jāprecizē, ka pati informācijas par datu plūsmu un atrašanās vietas datu saglabāšana, pirmkārt, ir atkāpe no Direktīvas 2002/58 5. panta 1. punktā paredzētā aizlieguma jebkurai personai, kas nav lietotājs, glabāt šos datus, un, otrkārt, iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās uz privātās dzīves neaizskaramību un personas datu aizsardzību, un nav nozīmes tam, vai attiecīgajai informācijai par privāto dzīvi ir vai nav sensitīvs raksturs un vai ieinteresētajām personām ir vai nav radītas neērtības šīs iejaukšanās dēļ (šajā nozīmē skat. atzinumu 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 124. un 126. punkts, kā arī tajos minētā judikatūra; pēc analoģijas attiecībā uz ECPAK 8. pantu skat. ECT, 2020. gada 30. janvāris, *Breyer* pret Vāciju, CE:ECHR:2020:0130JUD005000112, 81. punkts).

116 Tāpat nav nozīmes tam, vai saglabātie dati vēlāk tiek vai netiek izmantoti (pēc analoģijas attiecībā uz ECPAK 8. pantu skat. ECT, 2000. gada 16. februāris, *Amann* pret Šveici, CE:ECHR:2000:0216JUD002779895, 69. punkts, kā arī 2020. gada 13. februāris, *Trjakovski* un *Chipovski* pret Ziemeļmaķedoniju, CE:ECHR:2020:0213JUD005320513, 51. punkts), jo piekļuve šādiem

datiem neatkarīgi no tā, kā tie tiek izmantoti vēlāk, ir atsevišķa iejaukšanās iepriekšējā punktā minētajās pamattiesībās (šajā nozīmē skat. atzinumu 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 124. un 126. punkts).

117 Šis secinājums vēl jo vairāk šķiet pamatots tāpēc, ka informācija par datu plūsmu un atrašanās vietas dati var atklāt informāciju par datu subjektu būtisku privātās dzīves aspektu skaitu, ieskaitot sensitīvu informāciju, piemēram, seksuālo orientāciju, politiskajiem uzskatiem, reliģisko, filozofisko, sabiedrisko vai citu pārliecību, kā arī veselības stāvokli, lai gan šādi dati turklāt ir īpaši aizsargāti Savienības tiesībās. Minētie dati kopumā var ļaut izdarīt ļoti precīzus secinājumus par personu, kuru dati tikuši saglabāti, privāto dzīvi, proti, ikdienas paradumiem, pastāvīgajām vai pagaidu uzturēšanās vietām, ikdienas vai citām gaitām, veiktajām darbībām, šo personu sociālajiem kontaktiem un aprindām, kurās tās mēdz uzturēties. It īpaši šie dati sniedz iespējas noteikt attiecīgo personu profilu, kas tiesību uz privātās dzīves neaizskaramību kontekstā ir tikpat sensitīva informācija kā pats šīs komunikācijas saturs (šajā nozīmē skat. spriedumus, 2014. gada 8. aprīlis, *Digital Rights*, C-293/12 un C-594/12, EU:C:2014:238, 27. punkts, kā arī 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 99. punkts).

118 Līdz ar to, pirmkārt, informācijas par datu plūsmu un atrašanās vietas datu saglabāšana tiesībaizsardzības mērķiem pati par sevi var apdraudēt Hartas 7. pantā nostiprinātās tiesības uz saziņas neaizskaramību, un tas elektroniskās komunikācijas līdzekļu izmantotājus var atturēt izmantot savu vārda brīvību, kas ir garantēta tās 11. pantā (šajā nozīmē skat. spriedumus, 2014. gada 8. aprīlis, *Digital Rights*, C-293/12 un C-594/12, EU:C:2014:238, 28. punkts, kā arī 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 101. punkts). Šāda atturoša iedarbība it īpaši var ietekmēt personas, uz kuru saziņu saskaņā ar valsts tiesību aktiem attiecas dienesta noslēpums, kā arī trauksmes cēlējus, kuru darbības ir aizsargātas ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2019/1937 (2019. gada 23. oktobris) par to personu aizsardzību, kas ziņo par Savienības tiesību pārkāpumiem (OV 2019, L 305, 17. lpp.). Turklāt šī ietekme ir vēl jo būtiskāka lielā saglabāto datu apjoma un to daudzveidības dēļ.

119 Otrkārt, ņemot vērā informācijas par datu plūsmu un atrašanās vietas datu, kurus var pastāvīgi saglabāt ar visaptverošu un nediferencētu saglabāšanas pasākumu, ievērojamo apjomu, kā arī informācijas, ko šie dati var sniegt, sensitīvo raksturu, pati minēto datu saglabāšana, ko veic elektronisko komunikāciju pakalpojumu sniedzēji, ietver ļaunprātīgas izmantošanas un prettiesiskas piekļuves risku.

120 To ņemot vērā, ciktāl ar to dalībvalstīm ir atļauts ieviest šī sprieduma 110. punktā norādītas atkāpes, Direktīvas 2002/58 15. panta 1. punkts atspoguļo apstākli, ka Hartas 7., 8. un 11. pantā ietvertās tiesības nav uztveramas kā absolūtas prerogatīvas, bet gan jāaplūko saistībā ar to funkciju sabiedrībā (šajā nozīmē skat. spriedumu, 2020. gada 16. jūlijs, *Facebook Ireland* un *Schrems*, C-311/18, EU:C:2020:559, 172. punkts, kā arī tajā minētā judikatūra).

121 Kā izriet no Hartas 52. panta 1. punkta, tā pieļauj, ka šādām tiesībām var tikt noteikti izmantošanas ierobežojumi, ciktāl šie ierobežojumi ir paredzēti tiesību aktos, ar tiem tiek respektēta šo tiesību būtība un, ievērojot samērīguma principu, tie ir nepieciešami un patiešām atbilst vispārējo interešu mērķiem, ko atzinusi Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības.

122 Tādējādi, interpretējot Direktīvas 2002/58 15. panta 1. punktu Hartas kontekstā, ir jāņem vērā arī Hartas 3., 4., 6. un 7. pantā garantēto tiesību nozīmīgums un valsts drošības un smagu noziegumu apkarošanas mērķi, veicinot citu personu tiesību un brīvību aizsardzību.

123 Šajā ziņā Hartas 6. pantā, uz kuru atsaucas *Conseil d'État* un *Cour constitutionnelle*, ir nostiprinātas ne tikai ikvienas personas tiesības uz brīvību, bet arī uz drošību, un garantētas tiesības, kuras atbilst ECPAK 5. pantā noteiktajām tiesībām (šajā nozīmē skat. spriedumus, 2016. gada 15. februāris, *N.*,

C-601/15 PPU, EU:C:2016:84, 47. punkts; 2016. gada 28. jūlijs, *JZ*, C-294/16 PPU, EU:C:2016:610, 48. punkts, kā arī 2019. gada 19. septembris, *Rayonna prokuratura Lom*, C-467/18, EU:C:2019:765, 42. punkts un tajā minētā judikatūra).

124 Turklāt ir jāatgādina, ka Hartas 52. panta 3. punkta mērķis ir nodrošināt nepieciešamo saskaņotību starp tajā ietvertajām tiesībām un atbilstošajām ECPAK garantētajām tiesībām, tomēr negatīvi neietekmējot Savienības tiesību un Eiropas Savienības Tiesas autonomiju. Līdz ar to, interpretējot Hartu, kā minimālās aizsardzības robeža ir jāņem vērā atbilstošās ECPAK tiesības (šajā nozīmē skat. spriedumus, 2019. gada 12. februāris, *TC*, C-492/18 PPU, EU:C:2019:108, 57. punkts, kā arī 2019. gada 21. maijs, Komisija/Ungārija (Lauksaimniecības zemes lietojuma tiesības), C-235/17, EU:C:2019:432, 72. punkts un tajā minētā judikatūra).

125 Attiecībā uz ECPAK, tā 5. panta, kurā ir nostiprinātas "tiesības uz brīvību" un "tiesības uz drošību", mērķis saskaņā ar Eiropas Cilvēktiesību tiesas judikatūru ir aizsargāt indivīdu no jebkādas patvaļīgas vai nepamatotas brīvības atņemšanas (šajā nozīmē skat. ECT, 2008. gada 18. marts, *Ladent* pret Poliju, CE:ECHR:2008:0318JUD001103603, 45. un 46. punkts; 2010. gada 29. marts, *Medvedyev* un citi pret Franciju, CE:ECHR:2010:0329JUD000339403, 76. un 77. punkts, kā arī 2012. gada 13. decembris, *El-Masri* pret Bijušo Dienvidslāvijas Maķedonijas Republiku, CE:ECHR:2012:1213JUD003963009, 239. punkts). Tomēr, ciktāl šī tiesību norma attiecas uz valsts iestādes veiktu brīvības atņemšanu, Hartas 6. pants nevar tikt interpretēts tādējādi, ka ar to valsts iestādēm ir noteikts pienākums veikt īpašus pasākumus, lai sodītu par noteiktiem noziedzīgiem nodarījumiem.

126 Savukārt, kas attiecas it īpaši uz *Cour constitutionnelle* minēto efektīvo cīņu pret noziedzīgiem nodarījumiem, kuros tostarp ir cietušas nepilngadīgas personas un citas neaizsargātas personas, ir jāuzsver, ka pozitīvi pienākumi, kas uzlikti valsts iestādēm, var izrietēt no Hartas 7. panta, lai veiktu juridiskus pasākumus privātās un ģimenes dzīves aizsardzībai (šajā nozīmē skat. spriedumu, 2020. gada 18. jūnijs, Komisija/Ungārija (Biedrošanās pārskatāmība), C-78/18, EU:C:2020:476, 123. punkts un minētā Eiropas Cilvēktiesību tiesas judikatūra). Šādi pienākumi var izrietēt arī no minētā 7. panta attiecībā uz mājokļa un saziņas aizsardzību, kā arī no 3. un 4. panta attiecībā uz personu fiziskās un garīgās integritātes aizsardzību, kā arī no spīdzināšanas un necilvēcīgas vai pazemojošas izturēšanās aizlieguma.

127 Ņemot vērā šos dažādos pozitīvos pienākumus, ir jāveic attiecīgo dažādo aplūkoto interešu un tiesību nepieciešamā saskaņošana.

128 Eiropas Cilvēktiesību tiesa ir nospriedusi, ka pozitīvie pienākumi, kas izriet no ECPAK 3. un 8. panta, kuru atbilstošās garantijas ir ietvertas Hartas 4. un 7. pantā, tostarp nozīmē materiālo un procesuālo tiesību normu pieņemšanu, kā arī praktisku pasākumu noteikšanu, kas ļauj efektīvi apkarot noziedzīgus nodarījumus pret personām, veicot efektīvu izmeklēšanu un kriminālvajāšanu, un šis pienākums ir vēl jo svarīgāks, ja tiek apdraudēta bērna fiziskā un garīgā labklājība. To paturot prātā, pasākumos, kas ir jāveic kompetentajām iestādēm, ir pilnībā jāievēro tiesiskie līdzekļi un citas garantijas, kas var ierobežot krimināllizmeklēšanas pilnvaru apjomu, kā arī citas brīvības un tiesības. It īpaši šī tiesa uzskata, ka ir jāievieš tiesiskais regulējums, kas ļauj saskaņot dažādās intereses un aizsargājamās tiesības (ECT, 1998. gada 28. oktobris, *Osman* pret Apvienoto Karalisti, CE:ECHR:1998:1028JUD002345294, 115. un 116. punkts; 2004. gada 4. marts, *M.C.* pret Bulgāriju, CE:ECHR:2003:1204JUD003927298, 151. punkts; 2004. gada 24. jūnijs, *Von Hannover* pret Vāciju, CE:ECHR:2004:0624JUD005932000, 57. un 58. punkts, kā arī 2008. gada 2. decembris, K.U. pret Somiju, CE:ECHR:2008:1202JUD000287202, 46., 48. un 49. punkts).

129 Attiecībā uz samērīguma principa ievērošanu Direktīvas 2002/58 15. panta 1. punkta pirmajā teikumā ir noteikts, ka dalībvalstis var veikt pasākumu, atkāpjoties no komunikāciju un ar to saistītās informācijas par datu plūsmu konfidencialitātes principa, ja šis pasākums ir "nepieciešam[s], atbilstīg[s]

un samērīg[s] [..] demokrātiskā sabiedrībā", ņemot vērā šajā tiesību normā paredzētos mērķus. Šīs direktīvas 11. apsvērumā ir precizēts, ka šādam tiesību aktam ir jābūt "stingri" samērīgam ar paredzēto nolūku.

130 Šajā ziņā ir jāatgādina, ka pamattiesību uz privātās dzīves neaizskaramību aizsardzība atbilstoši Tiesas pastāvīgajai judikatūrai nozīmē, ka atkāpes no personas datu aizsardzības un tās ierobežojumi ir jāīsteno absolūti nepieciešamā ietvaros. Turklāt vispārējo interešu mērķi nevar sasniegt, neņemot vērā to, ka tas ir jāsaskaņo ar pamattiesībām, uz kurām attiecas pasākums, līdzsvarojot vispārējo interešu mērķi, no vienas puses, ar attiecīgajām tiesībām, no otras puses (šajā nozīmē skat. spriedumus, 2008. gada 16. decembris, *Satakunnan Markkinapörssi* un *Satamedia*, C-73/07, EU:C:2008:727, 56. punkts; 2010. gada 9. novembris, *Volker und Markus Schecke* un *Eifert*, C-92/09 un C-93/09, EU:C:2010:662, 76., 77. un 86. punkts, kā arī 2014. gada 8. aprīlis, *Digital Rights*, C-293/12 un C-594/12, EU:C:2014:238, 52. punkts; atzinums 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 140. punkts).

131 Konkrētāk, no Tiesas judikatūras izriet, ka iespēja dalībvalstīm pamatot tostarp Direktīvas 2002/58 5., 6. un 9. pantā paredzēto tiesību un pienākumu ierobežojumus ir jāizvērtē, izsverot iejaukšanās, ko rada šāds ierobežojums, smagumu, un pārbaudot, vai vispārējo interešu mērķa nozīmīgums, kas ir šī ierobežojuma pamats, ir atbilstošs šim smagumam (šajā nozīmē skat. spriedumu, 2018. gada 2. oktobris, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 55. punkts un tajā minētā judikatūra).

132 Lai izpildītu samērīguma prasību, tiesiskajā regulējumā 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, būtu pietiekamas garantijas, kas ļautu šos datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku. Šim tiesiskajam regulējumam ir jābūt juridiski saistošam valsts tiesībās un tajā it īpaši ir jānorāda, kādos apstākļos un saskaņā ar kādiem nosacījumiem var īstenot pasākumu, kas ietver šādu datu apstrādi, tādējādi garantējot, ka šāda iejaukšanās notiek tikai absolūti nepieciešamajā apmērā. Šādu garantiju sniegšanas nepieciešamība ir vēl jo svarīgāka tādēļ, ka personas dati tiek apstrādāti automātiski un pastāv ievērojams nelikumīgas piekļuves risks šiem datiem. Šie apsvērumi ir it īpaši svarīgi, ja runa ir par tādas kategorijas personas datu aizsardzību kā sensitīvi dati (šajā nozīmē skat. spriedumus, 2014. gada 8. aprīlis, *Digital Rights*, C-293/12 un C-594/12, EU:C:2014:238, 54. un 55. punkts, kā arī 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 117. punkts; atzinums 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 141. punkts).

133 Tādējādi tiesiskajam regulējumam, kurā ir paredzēta personas datu saglabāšana, vienmēr ir jāatbilst objektīviem kritērijiem, kas veido saikni starp saglabājamajiem datiem un sasniedzamo mērķi (šajā nozīmē skat. atzinumu 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 191. punkts un tajā minētā judikatūra, kā arī spriedumu, 2019. gada 3. oktobris, *A* u.c., C-70/18, EU:C:2019:823, 63. punkts).

– Par tiesību aktiem, kas paredz informācijas par datu plūsmu un atrašanās vietas datu preventīvu saglabāšanu valsts drošības aizsardzības nolūkā

134 Jānorāda, ka valsts drošības aizsardzības mērķi, uz ko atsaukušās iesniedzējtiesas un valdības, kas iesniegušas apsvērumus, Tiesa vēl nav īpaši izvērtējusi savos spriedumos, ar kuriem tiek interpretēta Direktīva 2002/58.

135 Šajā ziņā vispirms ir jānorāda, ka LES 4. panta 2. punktā ir noteikts, ka valsts drošība paliek vienīgi katras dalībvalsts atbildībā. Šī atbildība atbilst primārajām interesēm aizsargāt valsts pamatfunkcijas un sabiedrības pamatintereses un ietver tādu darbību novēršanu un apkarošanu, kas var nopietni destabilizēt valsts konstitucionālās, politiskās, ekonomiskās vai sociālās pamatstruktūras un it īpaši tieši apdraudēt pašu sabiedrību, iedzīvotājus vai valsti, kā, piemēram, terorisma darbības.

136 Valsts drošības aizsardzības mērķa, lasot to kopā ar LES 4. panta 2. punktu, nozīmīgums pārsniedz citu Direktīvas 2002/58 15. panta 1. punktā paredzēto mērķu nozīmīgumu, it īpaši vispārējus noziedzības apkarošanas mērķus, pat ja noziedzība ir smaga, kā arī sabiedrības drošības aizsardzību. Tādi draudi, kādi ir minēti iepriekšējā punktā, pēc sava rakstura un īpašā smaguma atšķiras no vispārējās valsts drošības spriedzes vai traucējumu, pat nopietnu, rašanās riska. Ar nosacījumu, ka tiek ievērotas citas Hartas 52. panta 1. punktā paredzētās prasības, valsts drošības aizsardzības mērķis līdz ar to var attaisnot pasākumus, kas ietver smagāku iejaukšanos pamattiesībās nekā tā, kas varētu attaisnot šos pārējos mērķus.

137 Tādējādi tādās situācijās, kādas ir aprakstītas šī sprieduma 135. un 136. punktā, Direktīvas 2002/58 15. panta 1. punktam, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, principā nav pretrunā tāds tiesību akts, ar kuru kompetentajām iestādēm ir atļauts uzdot elektronisko komunikāciju pakalpojumu sniedzējiem saglabāt informāciju par datu plūsmu un atrašanās vietas datus par visiem elektronisko komunikāciju līdzekļu lietotājiem ierobežotā laikposmā, ja pastāv pietiekami konkrēti apstākļi, kas ļauj uzskatīt, ka attiecīgajā dalībvalstī pastāv nopietns valsts drošības apdraudējums, kāds ir norādīts šī sprieduma 135. un 136. punktā, kurš šķiet patiess un faktisks vai paredzams. Pat ja šāds pasākums vienādi attiecas uz visiem elektronisko komunikāciju līdzekļu lietotājiem, kuri sākotnēji nešķiet esam saistīti ar draudiem šīs dalībvalsts drošībai šī sprieduma 133. punktā minētās judikatūras izpratnē, tomēr ir jāuzskata, ka šādu draudu esamība pati par sevi var radīt šādu saikni.

138 Rīkojums, kurā paredzēta visu elektronisko komunikāciju līdzekļu lietotāju datu preventīva saglabāšana, tomēr laika ziņā nedrīkst pārsniegt absolūti nepieciešamo. Lai gan nevar izslēgt, ka elektronisko komunikāciju pakalpojumu sniedzējiem noteiktais rīkojums saglabāt datus šāda apdraudējuma turpināšanās dēļ var tikt pagarināts, katra rīkojuma termiņš nevar pārsniegt paredzamo laika posmu. Turklāt šādai datu saglabāšanai ir jābūt pakļautai ierobežojumiem un to reglamentē stingras garantijas, kas ļauj efektīvi aizsargāt datu subjektu personas datus pret ļaunprātīgas izmantošanas risku. Tādējādi šai saglabāšanai nevar būt sistemātisks raksturs.

139 Ņemot vērā no šāda visaptverošas un nediferencētas datu saglabāšanas pasākuma izrietošās iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās smagumu, ir jānodrošina, lai tā izmantošana patiešām attiektos tikai uz situācijām, kurās pastāv nopietns apdraudējums valsts drošībai, kādas ir minētas šī sprieduma 135. un 136. punktā. Šajā ziņā ir būtiski, lai lēmumu, ar kuru elektronisko komunikāciju pakalpojumu sniedzējiem tiek uzdots veikt šādu datu saglabāšanu, varētu efektīvi kontrolēt vai nu tiesa, vai arī neatkarīga administratīva iestāde, kuras lēmumam ir saistoša iedarbība, lai pārbaudītu, vai pastāv šāda situācija, kā arī, vai ir ievēroti paredzētie nosacījumi un garantijas.

– Par tiesību aktiem, kas paredz informācijas par datu plūsmu un atrašanās vietas datu preventīvu saglabāšanu, lai apkarotu noziedzību un aizsargātu valsts drošību

140 Attiecībā uz noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķi saskaņā ar samērīguma principu vienīgi smagu noziegumu apkarošana un nopietnu valsts drošības apdraudējumu novēršana var pamatot tādu nopietnu iejaukšanos Hartas 7. un 8. pantā noteiktajās pamattiesībās, par kādu ir uzskatāma informācijas par datu plūsmu un atrašanās vietas datu saglabāšana. Tādējādi vienīgi tāda iejaukšanās minētajās pamattiesībās, kas nav smaga, var tikt attaisnota ar vispārīgu noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķi (šajā nozīmē skat. spriedumu, 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 102. punkts, kā arī 2018. gada 2. oktobris, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 56. un 57. punkts; atzinums 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 149. punkts).

141 Valsts tiesiskais regulējums, kas paredz visaptveroši un nediferencēti saglabāt informāciju par datu plūsmu un atrašanās vietas datus smagu noziegumu apkarošanas nolūkā, pārsniedz to, kas ir absolūti nepieciešams, un nevar tikt uzskatīts par pamatotu demokrātiskā sabiedrībā, kā to prasa arī Direktīvas 2002/58 15. panta 1. punkts, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā (šajā nozīmē skat. spriedumu, 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 107. punkts).

142 Ņemot vērā tādas informācijas sensitīvo raksturu, ko var sniegt informācija par datu plūsmu un atrašanās vietas datiem, tās konfidencialitāte ir būtiska attiecībā uz tiesībām uz privātās dzīves neaizskaramību. Tādējādi, ņemot vērā, pirmkārt, šī sprieduma 118. punktā minēto atturošo iedarbību uz Hartas 7. un 11. pantā paredzēto pamattiesību īstenošanu, ko var izraisīt šo datu saglabāšana, un, otrkārt, šādas saglabāšanas radītās iejaukšanās smagumu demokrātiskā sabiedrībā, ir svarīgi, lai tā, kā tas ir paredzēts ar Direktīvu 2002/58 izveidotajā sistēmā, būtu izņēmums, nevis norma, un lai šos datus nevarētu saglabāt sistemātiski un nepārtraukti. Šis secinājums attiecas pat uz mērķiem apkarot smagus noziegumus un novērst nopietnus draudus valsts drošībai, kā arī attiecībā uz nozīmīgumu, kas tiem ir jāpiešķir.

143 Turklāt Tiesa ir uzsvērusi, ka tiesiskais regulējums, kurā ir paredzēta informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta saglabāšana, attiecas uz gandrīz visu iedzīvotāju elektroniskajām komunikācijām, neparedzot nekādu diferenciāciju, ierobežojumus vai izņēmumus atkarībā no sasniedzamā mērķa. Šāds tiesiskais regulējums, pretēji šī sprieduma 133. punktā atgādinātajai prasībai, vispārēji attiecas uz visām personām, kuras izmanto elektronisko komunikāciju pakalpojumus, lai gan šīs personas pat netieši neatrodas situācijā, kurā var tikt veikta krimināltiesvedība. Tādējādi tas ir piemērojams pat attiecībā uz personām, par kurām nepastāv nekādas norādes, kas ļautu uzskatīt, ka to rīcībai varētu būtu kaut netieša vai attālināta saikne ar šo mērķi apkarot smagas noziedzīgas darbības, un, it īpaši, neparedzot saikni starp datiem, kurus ir paredzēts saglabāt, un draudiem valsts drošībai (šajā nozīmē skat. spriedumus, 2014. gada 8. aprīlis, *Digital Rights*, C-293/12 un C-594/12, EU:C:2014:238, 57. un 58. punkts, kā arī 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 105. punkts).

144 Konkrētāk, kā Tiesa jau ir nospriedusi, šādā tiesiskajā regulējumā nav paredzēta vienīgi ierobežota saglabāšana, kas attiecas vai nu uz datiem saistībā ar kādu laikposmu un/vai ģeogrāfisku teritoriju un/vai personu loku, kuras var vienā vai otrā veidā būt iesaistītas smagā noziegumā, vai arī uz personām, kuru datu saglabāšana citu iemeslu dēļ varētu palīdzēt smagu noziegumu apkarošanai (šajā nozīmē skat. spriedumus, 2014. gada 8. aprīlis, *Digital Rights*, C-293/12 un C-594/12, EU:C:2014:238, 59. punkts, un 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 106. punkts).

145 Pat dalībvalstu pozitīvie pienākumi, kas attiecīgā gadījumā var izrietēt no Hartas 3., 4. un 7. panta un kuri, kā tas ir norādīts šī sprieduma 126. un 128. punktā, attiecas uz tādu noteikumu ieviešanu, kas ļauj efektīvi apkarot noziedzīgus nodarījumus, nevar attaisnot tik nopietnu iejaukšanos, kas ietverta tiesiskajā regulējumā, kurā ir paredzēta informācijas par datu plūsmu un atrašanās vietas datu saglabāšana, gandrīz visas sabiedrības Hartas 7. un 8. pantā garantētajās pamattiesībās, ja attiecīgo personu dati nevar norādīt uz saikni, vismaz netiešu, ar vēlamo mērķi.

146 Savukārt saskaņā ar šī sprieduma 142.–144. punktā norādīto un, ņemot vērā nepieciešamo attiecīgo tiesību un interešu saskaņošanu, smagu noziegumu apkarošanas, nopietna sabiedrības drošības apdraudējuma novēršanas un, *a fortiori*, valsts drošības aizsardzības mērķi, ņemot vērā to nozīmīgumu, ievērojot iepriekšējā punktā atgādinātos pozitīvos pienākumus, uz kuriem tostarp ir atsaukusies *Cour constitutionnelle* (Konstitucionālā tiesa), var attaisnot īpaši smagu iejaukšanos, ko rada mērķtiecīga informācijas par datu plūsmu un atrašanās vietas datiem saglabāšana.

147 Tādējādi, kā Tiesa jau ir nospriedusi, Direktīvas 2002/58 15. panta 1. punkts, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, nav pretrunā tam, ka dalībvalsts pieņem tiesisku regulējumu, ar ko preventīvi atļauta informācijas par datu plūsmu un atrašanās vietas datu

mērķorientēta saglabāšana smagu noziegumu apkarošanas un nopietnu draudu sabiedrības drošībai novēršanas nolūkā, kā arī valsts drošības aizsardzībai, ar nosacījumu, ka šāda saglabāšana attiecībā uz saglabājamo datu kategorijām, attiecīgajiem komunikācijas līdzekļiem, datu subjektiem, kā arī noteikto saglabāšanas ilgumu aprobežojas tikai ar tam absolūti nepieciešamo (šajā nozīmē skat. spriedumu, 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 108. punkts).

148 Aprobežošanu, kas jāveic ar attiecībā uz šādu informācijas saglabāšanas pasākumu, var noteikt atkarībā no datu subjektu kategorijām, jo Direktīvas 2002/58 15. panta 1. punktam nav pretrunā tiesiskais regulējums, kura pamatā ir objektīvi apstākļi, kas ļauj definēt personas, kuru informācijai par datu plūsmu un atrašanās vietas datiem var būt kaut vai netieša saikne ar smagiem noziegumiem, vienā vai otrā veidā veicinot smagu noziegumu apkarošanu vai būtiska riska sabiedrības drošībai vai arī valsts drošībai novēršanu (šajā nozīmē skat. spriedumu, 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 111. punkts).

149 Šajā ziņā ir jāprecizē, ka šādi minētās personas tostarp var būt personas, kuras piemērojamās valsts procedūrās un pamatojoties uz objektīviem apstākļiem iepriekš ir identificētas kā tādas, kas apdraud attiecīgās dalībvalsts sabiedrības drošību vai valsts drošību.

150 Pasākuma, ar kuru ir paredzēta informācijas par datu plūsmu un atrašanās vietas datu saglabāšana, aprobežošanas pamatā var būt arī ģeogrāfisks kritērijs, kad kompetentās valsts iestādes, pamatojoties uz objektīviem un nediskriminējošiem elementiem, uzskata, ka vienā vai vairākās ģeogrāfiskajās zonās pastāv augsts risks saistībā ar sagatavošanos smagiem noziegumiem vai to izdarīšanu (šajā nozīmē skat. spriedumu, 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 111. punkts). Šīs teritorijas tostarp var būt vietas, kurās ir raksturīgs liels smagu noziegumu skaits, vietas, kas ir īpaši pakļautas smagu noziegumu izdarīšanai, piemēram, vietas vai infrastruktūra, ko regulāri apmeklē ļoti liels personu skaits, vai arī stratēģiskas vietas, piemēram, lidostas, dzelzceļa stacijas vai autoceļu nodevas iekasēšanas vietas.

151 Lai nodrošinātu, ka iejaukšanās, ko rada šī sprieduma 147.–150. punktā aprakstītie mērķorientētie aizsardzības pasākumi, atbilst samērīguma principam, to ilgums nevar pārsniegt to, kas ir absolūti nepieciešams izvirzītajam mērķim, kā arī tos pamatojošos apstākļus, saglabājot iespēju tos pagarināt šādas saglabāšanas nepieciešamības turpināšanās dēļ.

– Par tiesību aktiem, kas paredz IP adrešu un personas identitātes datu preventīvu saglabāšanu, lai apkarotu noziedzību un aizsargātu sabiedrības drošību

152 Jānorāda, ka IP adreses, lai gan tās ir daļa no informācijas par datu plūsmu, tiek radītas, nebūdamas saistītas ar noteiktu komunikāciju, un galvenokārt ir paredzētas, lai ar elektronisko komunikāciju pakalpojumu sniedzēju starpniecību identificētu fizisku personu, kurai pieder galaiekārta, no kuras tiek veikta komunikācija ar interneta starpniecību. Tādējādi elektroniskā pasta, kā arī interneta telefonijas jomā, ciktāl tiek saglabātas vienīgi komunikācijas avota, nevis adresāta IP adreses, šīs adreses pašas par sevi neatklāj nekādu informāciju par trešajām personām, kuras ir sazinājušās ar personu, kura ir iniciējusi komunikāciju. Šīs kategorijas dati tātad ir mazāk jutīgi nekā cita informācija par datu plūsmu.

153 Tomēr, tā kā IP adreses var tikt izmantotas, lai tostarp veiktu izsmeļošu interneta lietotāja navigācijas maršruta un līdz ar to tā darbību tiešsaistē izsekošanu, šie dati ļauj noteikt interneta lietotāja detalizētu profilu. Tādējādi minēto IP adrešu saglabāšana un analīze, kas prasa šādu izsekošanu, ir nopietna iejaukšanās Hartas 7. un 8. pantā garantētajās interneta lietotāja pamattiesībās, kurai var būt tāda atturoša iedarbība kā šī sprieduma 118. punktā minētā.

154 Lai nodrošinātu nepieciešamo attiecīgo tiesību un interešu saskaņošanu, kā tas ir prasīts šī sprieduma 130. punktā minētajā judikatūrā, ir jāņem vērā, ka tiešsaistē izdarīta noziedzīga nodarījuma gadījumā IP adrese var būt vienīgais izmeklēšanas līdzeklis, kas ļauj identificēt personu, kurai šī adrese ir piešķirta šī noziedzīgā nodarījuma izdarīšanas brīdī. Papildus tam ir jāņem vērā tas, ka IP adrešu saglabāšana, ko veic elektroniskās komunikācijas pakalpojumu sniedzēji pēc šo datu piešķiršanas beigām, principā nav nepieciešama, izrakstot rēķinus par attiecīgajiem pakalpojumiem, tādējādi šī iemesla dēļ, kā to norādīja vairākas valdības savos Tiesā iesniegtajos apsvērumos, tiešsaistē izdarīto noziegumu atklāšana var izrādīties neiespējama, neizmantojot tiesību aktus, kas pieņemti, pamatojoties uz Direktīvas 2002/58 15. panta 1. punktu. Kā apgalvo šīs valdības, tā tas tostarp ir īpaši smagu noziedzīgu nodarījumu gadījumā bērnu pornogrāfijas jomā, piemēram bērnu pornogrāfijas iegādāšanās, izplatīšanas vai ievietošanas tiešsaistē gadījumos Eiropas Parlamenta un Padomes Direktīvas 2011/93/ES (2011. gada 13. decembris) par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu, un ar kuru aizstāj Padomes Pamatlēmumu 2004/68/TI (OV 2011, L 335, 1. lpp.), 2. panta c) punkta izpratnē.

155 Šādos apstākļos, lai gan ir taisnība, ka tiesību akts, kurā ir paredzēta visu to fizisko personu IP adrešu saglabāšana, kurām pieder tāda galaiekārta, no kuras var tikt sniegta piekļuve internetam, attiektos uz personām, kurām šī sprieduma 133. punktā minētās judikatūras izpratnē pirmšķietami nav tiešas saiknes ar sasniedzamajiem mērķiem, un ka interneta lietotājiem atbilstoši šī sprieduma 109. punktā konstatētajam saskaņā ar Hartas 7. un 8. pantu ir tiesības sagaidīt, ka principā to identitāte netiks atklāta, tāds tiesību akts, kurā ir paredzēta visaptveroša un nediferencēta vienīgi to IP adrešu saglabāšana, kas ir piešķirtas savienojuma avotam, principā nav pretrunā Direktīvas 2002/58 15. panta 1. punktam, to lasot Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, ja šī iespēja ir pakļauta stingrai materiāltiesisko un tādu procesuālo nosacījumu ievērošanai, kam jāreglamentē šo datu izmantošana.

156 Ņemot vērā iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās smago raksturu, ko rada šāda saglabāšana, šo iejaukšanos var pamatot vienīgi smagu noziegumu apkarošana un nopietnu sabiedrības drošības draudu novēršana, kā arī valsts drošības aizsardzība. Turklāt glabāšanas ilgums nedrīkst pārsniegt to, kas ir absolūti nepieciešams izvirzītā mērķa sasniegšanai. Visbeidzot, šāda veida pasākumā ir jāparedz stingri nosacījumi un garantijas attiecībā uz šo datu izmantošanu, it īpaši veicot datu subjektu tiešsaistes komunikāciju un darbību izsekošanu.

157 Visbeidzot, attiecībā uz datiem par elektronisko komunikāciju līdzekļu lietotāju identitāti, jānorāda, ka šie dati paši par sevi neļauj uzzināt veikto komunikāciju datumu, laiku, ilgumu un adresātus, ne arī vietas, kur šī saziņa ir notikusi, vai to biežumu ar noteiktām personām noteiktā laika posmā, tādējādi tie nesniedz šo personu kontaktinformāciju, kā, piemēram, viņu adreses, nekādu informāciju par veiktajām komunikācijām un, līdz ar to, viņu privāto dzīvi. Tādējādi, principā iejaukšanos, ko rada šo datu saglabāšana, nevar kvalificēt kā smagu (šajā nozīmē skat. spriedumu, 2018. gada 2. oktobris, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 59. un 60. punkts).

158 No tā izriet, ka atbilstoši tam, kas tika norādīts šī sprieduma 140. punktā, tiesību aktus saistībā ar pašu šo datu apstrādi, tostarp to saglabāšanu un piekļuvi tiem vienīgi ar nolūku identificēt attiecīgo lietotāju, ja nav iespējas minētos datus sasaistīt ar informāciju par veikto komunikāciju, var pamatot noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķi vispārīgā veidā, uz kuriem ir norāde Direktīvas 2002/58 15. panta 1. punkta pirmajā teikumā (šajā nozīmē skat. spriedumu, 2018. gada 2. oktobris, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 62. punkts).

159 Šādos apstākļos, ņemot vērā nepieciešamību saskaņot attiecīgās tiesības un intereses un šī sprieduma 131. un 158. punktā minēto iemeslu dēļ, ir jāuzskata, ka, pat nepastāvot saiknei starp visiem elektronisko komunikāciju līdzekļu lietotājiem un sasniedzamajiem mērķiem, Direktīvas 2002/58 15. panta 1. punktam, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, nav pretrunā tiesību akts, ar ko, nenosakot konkrētu termiņu, elektronisko komunikāciju pakalpojumu sniedzējiem tiek noteikts pienākums saglabāt visus ar elektronisko komunikāciju līdzekļu

lietotāju identitāti saistītos datus noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķim, kā arī sabiedrības drošības aizsardzībai, un nav nepieciešams, lai noziedzīgie nodarījumi vai draudi, vai kaitējums sabiedrības drošībai būtu smags.

– Par tiesību aktiem, kas paredz informācijas par datu plūsmu un atrašanās vietas datu operatīvu saglabāšanu smagu noziegumu apkarošanai

160 Attiecībā uz informāciju par datu plūsmu un atrašanās vietas datiem, ko elektronisko komunikāciju pakalpojumu sniedzēji apstrādā un glabā, pamatojoties uz Direktīvas 2002/58 5., 6. un 9. pantu, vai, pamatojoties uz tiesību aktiem, kas pieņemti saskaņā ar tās 15. panta 1. punktu, kas aprakstīti šī sprieduma 134.–159. punktā, ir jānorāda, ka šie dati principā atkarībā no konkrētā gadījuma ir jādzēš vai jāpadara anonīmi, beidzoties termiņam, kas šīs direktīvas transponēšanai pieņemtajos tiesību aktos ir noteikts to apstrādei un uzglabāšanai.

161 Tomēr šīs apstrādes un uzglabāšanas laikā var rasties situācijas, kurās ir nepieciešams uzglabāt minētos datus pēc šiem termiņiem, lai atklātu smagus noziedzīgus nodarījumus vai valsts drošības apdraudējumu, un tas var notikt gan situācijā, kad šie noziedzīgie nodarījumi vai šis apdraudējums jau ir ticis atklāts, gan gadījumā, kad par to esamību pēc visu atbilstošo apstākļu objektīvas pārbaudes var rasties pamatotas aizdomas.

162 Šajā ziņā ir jānorāda, ka 2001. gada 23. novembra Eiropas Padomes Konvencijas par kibernoziegumiem (Eiropas līgumu sērija – Nr. 185), kuru ir parakstījušas 27 dalībvalstis un ratificējušas 25 no tām un kuras mērķis ir atvieglot tādu noziedzīgu nodarījumu apkarošanu, kas izdarīti, izmantojot datortīklus, 14. pantā ir paredzēts, ka līgumslēdzējas puses izmeklēšanas vai kriminālprocesa konkrētiem mērķiem veic noteiktus pasākumus, kas attiecas uz jau uzkrātu informāciju par datu plūsmu, piemēram, šādu datu operatīvu saglabāšanu. It īpaši šīs konvencijas 16. panta 1. punktā ir noteikts, ka līgumslēdzējas puses pieņem tiesību aktus, kas ir nepieciešami, lai ļautu to kompetentajām iestādēm dot rīkojumu vai līdzīgi nodrošināt operatīvu informācijas par datu plūsmu saglabāšanu, kas tikusi uzglabāta ar datorsistēmas palīdzību, īpaši, ja ir pamats uzskatīt, ka dati ir īpaši jutīgi pret nozaudēšanu vai izmainīšanu.

163 Tādā situācijā kā šī sprieduma 161. punktā minētā, dalībvalstis, ņemot vērā šī sprieduma 130. punktā minēto nepieciešamību saskaņot attiecīgās tiesības un intereses, var saskaņā ar Direktīvas 2002/58 15. panta 1. punktu pieņemtajos tiesību aktos paredzēt iespēju ar kompetentās iestādes lēmumu, kas ir pakļauts efektīvai pārbaudei tiesā, uzdot elektronisko komunikāciju pakalpojumu sniedzējiem uz noteiktu laiku operatīvi saglabāt to rīcībā esošo informāciju par datu plūsmu un atrašanās vietas datus.

164 Ciktāl šādas operatīvas saglabāšanas mērķis vairs neatbilst mērķiem, kādiem sākotnēji tikuši vākti un saglabāti dati, un ciktāl jebkurai datu apstrādei saskaņā ar Hartas 8. panta 2. punktu ir jāatbilst noteiktiem mērķiem, dalībvalstīm savos tiesību aktos ir jāprecizē mērķis, kādam var notikt datu operatīva saglabāšana. Ņemot vērā iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās smago raksturu, ko var ietvert šāda saglabāšana, vienīgi smagu noziegumu apkarošana un, *a fortiori*, valsts drošības aizsardzība var pamatot šo iejaukšanos. Turklāt, lai nodrošinātu, ka iejaukšanās, ko rada šāda veida pasākums, ir ierobežota ar absolūti nepieciešamo, pirmkārt, saglabāšanas pienākumam ir jāattiecas vienīgi uz to informāciju par datu plūsmu un atrašanās vietas datiem, kas var sekmēt smaga noziedzīga nodarījuma vai attiecīgā valsts drošības apdraudējuma atklāšanu. Otrkārt, datu uzglabāšanas ilgums ir jāierobežo līdz absolūti nepieciešamajam, bet tas tomēr var tikt pagarināts, ja to pamato minētā pasākuma izvirzītais mērķis un apstākļi.

165 Šajā ziņā ir jāprecizē, ka šāda operatīva uzglabāšana nav jāattiecina tikai uz to personu datiem, kuras konkrēti tiek turētas aizdomās par noziedzīga nodarījuma izdarīšanu vai valsts drošības apdraudējumu. Ievērojot Direktīvas 2002/58 15. panta 1. punktā, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta

1. punkta kontekstā, noteiktos ietvarus un ņemot vērā šī sprieduma 133. punktā minētos apsvērumus, šāds pasākums, atkarībā no likumdevēja izvēles un ievērojot absolūti nepieciešamā robežas, var tikt attiecināts arī uz informāciju par datu plūsmu un atrašanās vietas datiem, kas ir saistīti ar personām, kas nav tās, kuras tiek turētas aizdomās par to, ka tās ir plānojušas vai izdarījušas smagu noziedzīgu nodarījumu vai veikušas valsts drošības apdraudējumu, ciktāl šie dati, pamatojoties uz objektīviem un nediskriminējošiem apstākļiem, var veicināt šāda noziedzīga nodarījuma vai šāda valsts drošības apdraudējuma atklāšanu, piemēram, cietušo dati, sociālā vai profesionālā loka vai arī noteiktu ģeogrāfisko zonu dati, piemēram, attiecīgā noziedzīgā nodarījuma vai valsts drošības apdraudējuma sagatavošanas un izdarīšanas vietas dati. Turklāt kompetento iestāžu piekļuvei šādi saglabātajiem datiem ir jāatbilst nosacījumiem, kas izriet no judikatūras, kurā ir interpretēta Direktīva 2002/58 (šajā nozīmē skat. spriedumu, 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 118.–121. punkts un tajos minētā judikatūra).

166 Vēl ir jāpiebilst, kā tas it īpaši izriet no šī sprieduma 115. un 133. punkta, ka piekļuvi informācijai par datu plūsmu un atrašanās vietas datiem, ko pakalpojumu sniedzēji saglabā, piemērojot saskaņā ar Direktīvas 2002/58 15. panta 1. punktu pieņemtu tiesību aktu, principā var pamatot vienīgi ar vispārējo interešu mērķi, kura dēļ pakalpojumu sniedzējiem ir ticis uzdots veikt šādu saglabāšanu. No tā it īpaši izriet, ka piekļuvi šādiem datiem, lai veiktu kriminālvajāšanu un sodītu par parastu noziedzīgu nodarījumu, nekādā gadījumā nevar piešķirt, ja to saglabāšana ir pamatota ar smagu noziegumu apkarošanas vai, *a fortiori*, ar valsts drošības aizsardzības mērķi. Savukārt saskaņā ar samērīguma principu, kāds tas ir precizēts šī sprieduma 131. punktā, piekļuvi saglabātajiem datiem, lai apkarotu smagus noziegumus, ar nosacījumu, ka tiek ievēroti iepriekšējā punktā minētie šādas piekļuves materiāltiesiskie un procesuālie nosacījumi, var pamatot ar valsts drošības aizsardzības mērķi.

167 Šajā ziņā dalībvalstis savos tiesību aktos var paredzēt, ka piekļuve informācijai par datu plūsmu un atrašanās vietas datiem, ievērojot šos pašus materiāltiesiskos un procesuālos nosacījumus, var notikt, lai apkarotu smagus noziegumus vai aizsargātu valsts drošību, ja pakalpojumu sniedzējs minētos datus glabā veidā, kas atbilst Direktīvas 2002/58 5., 6. un 9. pantam vai arī 15. panta 1. punktam.

168 Ņemot vērā visus iepriekš minētos apsvērumus, uz pirmajiem jautājumiem lietās C-511/18 un C-512/18, kā arī uz pirmo un otro jautājumu lietā C-520/18 ir jāatbild, ka Direktīvas 2002/58 15. panta 1. punkts, lasot to kopā ar Hartas 7., 8. un 11. pantu, kā arī 52. panta 1. punktu, ir jāinterpretē tādējādi, ka tam ir pretrunā tādi tiesību akti, ar kuriem 15. panta 1. punktā paredzētajiem mērķiem preventīvi ir paredzēta informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta saglabāšana. Savukārt minētajam 15. panta 1. punktam, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, nav pretrunā tādi tiesību akti,

– ar kuriem, gadījumā, ja elektronisko komunikāciju pakalpojumu sniedzējiem ir izdots rīkojums veikt visaptverošu un nediferencētu informācijas par datu plūsmu un atrašanās vietas datu saglabāšanu situācijās, kad attiecīgā dalībvalsts sastopas ar nopietniem draudiem valsts drošībai, kuri izrādās patiesi un faktiski vai paredzami, valsts drošības aizsardzības nolūkā ir atļauts pieņemt lēmumu, kurā ir paredzēts, ka šis rīkojums var tikt pakļauts efektīvai pārbaudei tiesā vai arī neatkarīgā administratīvā iestādē, kuras nolēmumam ir saistoša iedarbība, lai pārbaudītu šādas situācijas esamību, kā arī paredzēto nosacījumu un garantiju ievērošanu, un minēto rīkojumu var izdot vienīgi uz absolūti nepieciešamo laiku, tomēr šo termiņu var pagarināt, ja šāds apdraudējums saglabājas;

– kas, lai aizsargātu valsts drošību, apkarotu smagus noziegumus un novērstu nopietnus draudus sabiedrības drošībai, paredz informācijas par datu plūsmu un atrašanās vietas datu mērķorientētu saglabāšanu, kura, pamatojoties uz objektīviem un nediskriminējošiem elementiem, tiek ierobežota atkarībā no attiecīgo personu kategorijām vai pamatojoties uz ģeogrāfisku kritēriju, uz laiku, kas nepārsniedz absolūti nepieciešamo, kuru tomēr var pagarināt;

– kas, lai aizsargātu valsts drošību, apkarotu smagus noziegumus un novērstu nopietnus draudus sabiedrības drošībai, paredz visaptveroši un nediferencēti saglabāt savienojuma avotam piešķirtās IP adreses uz laiku, kas nepārsniedz absolūti nepieciešamo;

– kas, lai aizsargātu valsts drošību, apkarotu smagus noziegumus un novērstu nopietnus draudus sabiedrības drošībai, paredz visaptverošu un nediferencētu elektronisko komunikāciju līdzekļu lietotāju identitātes datu saglabāšanu un,

– kas, lai apkarotu smagus noziegumus un *a fortiori* aizsargātu valsts drošību, ļauj ar kompetentās iestādes lēmumu, kas ir pakļauts efektīvai pārbaudei tiesā, izdot rīkojumu elektronisko komunikāciju pakalpojumu sniedzējiem uz noteiktu laiku operatīvi saglabāt šo pakalpojumu sniedzēju rīcībā esošo informāciju par datu plūsmu un atrašanās vietas datus,

ja ar šiem pasākumiem ar skaidriem un precīziem noteikumiem tiek nodrošināts, ka attiecīgo datu saglabāšana notiek atbilstoši tai paredzētajiem materiāltiesiskajiem un procesuālajiem nosacījumiem un ka datu subjektiem ir efektīvas garantijas pret ļaunprātīgas izmantošanas risku.

Par otro un trešo jautājumu lietā C-511/18

169 Ar otro un trešo jautājumu lietā C-511/18 iesniedzējtiesa būtībā jautā, vai Direktīvas 2002/58 15. panta 1. punkts, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, ir jāinterpretē tādējādi, ka tam ir pretrunā tāds valsts tiesiskais regulējums, kurā elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums īstenot pasākumus to tīklos, kas ļauj veikt, pirmkārt, informācijas par datu plūsmu un atrašanās vietas datu automatizētu analīzi, kā arī to vākšanu reāllaikā, un, otrkārt, tehnisko datu par izmantoto galaiekārtu atrašanās vietu vākšanu reāllaikā, neparedzot šīs apstrādes un vākšanas datu subjektu informēšanu.

170 Iesniedzējtiesa precizē, ka IDK L. 851-2. līdz L. 851-4. pantā paredzētās izlūkdatu vākšanas metodes elektronisko komunikāciju pakalpojumu sniedzējiem nerada īpašu prasību saglabāt informāciju par datu plūsmu un atrašanās vietas datus. It īpaši attiecībā uz IDK L. 851-3. pantā paredzēto automatizēto analīzi šī tiesa norāda, ka šīs apstrādes mērķis ir saskaņā ar šim nolūkam noteiktiem kritērijiem atklāt saiknes, kas var atklāt terorisma draudus. Attiecībā uz IDK L. 851-2. pantā paredzēto vākšanu reāllaikā minētā tiesa konstatē, ka tā attiecas tikai uz vienu vai vairākām personām, kuras iepriekš ir identificētas kā tādas, kas varētu būt saistītas ar terorisma draudiem. Šī pati tiesa uzskata, ka šīs divas metodes var tikt īstenotas tikai, lai novērstu terorismu, un tās attiecas uz IDK L. 851-1. un R. 851-5. pantā minētajiem datiem.

171 Vispirms ir jāprecizē, ka apstāklis, ka saskaņā ar IDK L. 851-3. pantu tajā paredzētā automatizētā analīze pati par sevi neļauj identificēt lietotājus, kuru dati tiek pakļauti šai analīzei, nav šķērslis, lai šādus datus kvalificētu par "personas datiem". Tā kā šīs pašas tiesību normas IV punktā paredzētā procedūra vēlāk ļauj identificēt datu subjektu vai subjektus, kuru datu automatizētā analīze ir atklājusi, ka tās varētu būt saistītas ar terorisma draudiem, visas personas, kuru dati ir pakļauti automatizētai analīzei, ir identificējamas, pamatojoties uz šiem datiem. Saskaņā ar Regulas 2016/679 4. panta 1. punktā ietverto personas datu definīciju šādi dati ir informācija, kas tostarp attiecas uz identificējamu personu.

Par informācijas par datu plūsmu un atrašanās vietas datu automatizēto analīzi

172 No IDK L. 851-3. panta izriet, ka tajā paredzētā automatizētā analīze būtībā ir tās informācijas par datu plūsmu un atrašanās vietas datu kopuma filtrēšana, ko saglabā elektronisko komunikāciju pakalpojumu sniedzēji pēc kompetento valsts iestāžu pieprasījuma un piemērojot to noteiktos parametrus. No tā izriet, ka visi elektronisko komunikācijas līdzekļu lietotāju dati tiek pārbaudīti, vai tie atbilst šiem

parametriem. Līdz ar to šāda automatizēta analīze ir jāuzskata par tādu, kas nozīmē, ka attiecīgie elektronisko komunikāciju pakalpojumu sniedzēji kompetentās iestādes vārdā veic visaptverošu un nediferencētu apstrādi, kas izpaužas kā automatizētu līdzekļu izmantošana Regulas 2016/679 4. panta 2. punkta izpratnē, kas aptver visu elektroniskās komunikācijas līdzekļu lietotāju informāciju par datu plūsmu un atrašanās vietas datus. Šī apstrāde ir neatkarīga no vēlākas datu par personām, kuras ir identificētas pēc automatizētās analīzes, vākšanas, kas ir atļauta, pamatojoties uz IDK L. 851-3. panta IV punktu.

173 Valsts tiesiskais regulējums, kas atļauj šādu informācijas par datu plūsmu un atrašanās vietas datu automatizētu analīzi, ir atkāpe no Direktīvas 2002/58 5. pantā noteiktā principiālā pienākuma nodrošināt elektroniskās komunikācijas un ar to saistīto datu konfidencialitāti. Šāds tiesiskais regulējums arī rada iejaukšanos Hartas 7. un 8. pantā garantētajās pamattiesībās, lai arī kāda būtu šo datu vēlāka izmantošana. Visbeidzot, saskaņā ar šī sprieduma 118. punktā minēto judikatūru minētajam tiesiskajam regulējumam var būt atturoša ietekme uz Hartas 11. pantā nostiprinātās vārda brīvības īstenošanu.

174 Turklāt iejaukšanās, kas izriet no informācijas par datu plūsmu un atrašanās vietas datu automatizētas analīzes, kāda tiek aplūkota pamatlietā, ir īpaši smaga, jo tā visaptveroši un nediferencēti attiecas uz to personu datiem, kuras izmanto elektronisko komunikāciju līdzekļus. Šis konstatējums ir vēl jo vairāk attiecināms, ja, kā izriet no pamatlietā aplūkotā valsts tiesiskā regulējuma, automatizēti analizētie dati var atklāt tiešsaistē iegūtās informācijas raksturu. Turklāt šāda automatizēta analīze ir vispārīgi piemērojama visām personām, kas izmanto elektroniskās komunikācijas līdzekļus, un līdz ar to arī tām, par kurām nav nekādu norāžu, kas ļautu uzskatīt, ka to rīcībai varētu būt kaut netieša vai attāla saikne ar terorisma darbībām.

175 Attiecībā uz šādas iejaukšanās pamatojumu ir jāprecizē, ka Hartas 52. panta 1. punktā ietvertā prasība, saskaņā ar kuru jebkuram pamattiesību izmantošanas ierobežojumam ir jābūt noteiktam tiesību aktos, nozīmē, ka pašā juridiskajā pamatā ir jānosaka attiecīgo tiesību īstenošanas ierobežojuma apjoms (šajā nozīmē skat. spriedumu, 2020. gada 16. jūlijs, *Facebook Ireland* un *Schrems*, C-311/18, EU:C:2020:559, 175. punkts, kā arī tajā minētā judikatūra).

176 Turklāt, lai izpildītu šī sprieduma 130. un 131. punktā atgādināto samērīguma prasību, saskaņā ar kuru atkāpes no personas datu aizsardzības un tās ierobežojumi ir jāīsteno absolūti nepieciešamā robežās, valsts tiesiskajam regulējumam, kas reglamentē kompetento iestāžu piekļuvi saglabātajai informācijai par datu plūsmu un atrašanās vietas datiem, ir jāatbilst prasībām, kas izriet no šī sprieduma 132. punktā minētās judikatūras. It īpaši šāds tiesiskais regulējums nevar aprobežoties ar prasību, lai iestāžu piekļuve datiem atbilstu šī tiesiskā regulējuma mērķim, bet tajā ir arī jāparedz materiāltiesiskie un procesuālie nosacījumi, kas regulē šo izmantošanu (pēc analoģijas skat. atzinumu 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 192. punkts un tajā minētā judikatūra).

177 Šajā ziņā ir jāatgādina, ka īpaši smaga iejaukšanās, ko rada informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta saglabāšana, kas minēta šī sprieduma 134.–139. punktā ietvertajos apsvērumos, kā arī īpaši smaga iejaukšanās, ko rada to automatizētā analīze, var atbilst samērīguma prasībai tikai situācijās, kad dalībvalsts saskaras ar nopietniem draudiem valsts drošībai, kas izrādās patiesi un faktiski vai paredzami, un ar nosacījumu, ka šīs glabāšanas ilgums ir ierobežots ar absolūti nepieciešamo.

178 Tādās situācijās, kādas ir minētas iepriekšējā punktā, visu elektronisko komunikāciju līdzekļu lietotāju informācijas par datu plūsmu un atrašanās vietas datu automatizētas analīzes īstenošana stingri ierobežotā laikposmā var tikt uzskatīta par pamatotu, ņemot vērā prasības, kas izriet no Direktīvas 2002/58 15. panta 1. punkta, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā.

179 To ņemot vērā, lai nodrošinātu, ka šāda pasākuma izmantošana patiešām ir ierobežota ar to, kas ir absolūti nepieciešams valsts drošības aizsardzībai un it īpaši terorisma novēršanai, saskaņā ar šī sprieduma 139. punktā konstatēto ir būtiski, lai lēmumu, ar kuru tiek atļauta automatizēta analīze, varētu efektīvi pārbaudīt vai nu tiesa, vai arī neatkarīga administratīva iestāde, kuras lēmumam ir saistoša iedarbība, lai pārliecinātos, vai pastāv situācija, kas pamato minēto pasākumu, kā arī, vai ir ievēroti paredzētie nosacījumi un garantijas.

180 Šajā ziņā ir jāprecizē, ka iepriekš noteiktajiem modeļiem un kritērijiem, uz kuriem ir balstīta šāda veida datu apstrāde, ir jābūt, pirmkārt, specifiskiem un ticamiem, kas ļauj sasniegt rezultātus, ar kuriem tiek identificētas personas, par kurām varētu rasties pamatotas aizdomas par dalību teroristiskos nodarījumos, un, otrkārt, nediskriminējošiem (šajā nozīmē skat. atzinumu 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 172. punkts).

181 Turklāt ir jāatgādina, ka jebkāda automatizēta analīze, kas tiek veikta atkarībā no modeļiem un kritērijiem, kuri ir balstīti uz pieņēmumu, ka rase vai etniskā izcelsme, politiskie uzskati, reliģiskā vai filozofiskā pārliecība, personas piederība arodbiedrībām, veselības stāvoklis vai dzimumdzīve pati par sevi un neatkarīgi no šīs personas individuālās rīcības varētu būt nozīmīga saistībā ar terorisma novēršanu, pārkāptu Hartas 7. un 8. pantā, skatot tos kopsakarā ar Hartas 21. pantu, garantētās tiesības. Tādējādi iepriekš noteikti modeļi un kritēriji automatizētas analīzes nolūkā novērst terorisma darbības, kas nopietni apdraud valsts drošību, nevar tikt balstīti tikai uz šiem sensitīvajiem datiem (šajā nozīmē skat. atzinumu 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 165. punkts).

182 Turklāt informācijas par datu plūsmu un atrašanās vietas datu automatizēta analīze noteikti ietver zināmu kļūdu īpatsvaru, un jebkurš pozitīvs rezultāts, kas iegūts pēc automatizētas apstrādes, ir individuāli jāpārskata ar neautomatizētiem līdzekļiem, pirms tiek noteikts individuāls pasākums, kas datu subjektiem rada nelabvēlīgas sekas, kā, piemēram, vēlāka informācijas par datu plūsmu un atrašanās vietas datu vākšana reāllaikā, jo šāds pasākums nevar tikt izšķiroši pamatots tikai ar rezultātu, kas izriet no automatizētas apstrādes. Tāpat, lai praksē nodrošinātu, ka iepriekš noteikti izmantotie modeļi un kritēriji, kā arī izmantotās datu bāzes nav diskriminējošas un ir ierobežotas ar absolūti nepieciešamo, ņemot vērā mērķi novērst terorisma darbības, kas nopietni apdraud valsts drošību, šo iepriekš noteikto modeļu un kritēriju, kā arī izmantotās datu bāzes uzticamība un aktualitāte ir regulāri jāpārbauda (šajā nozīmē skat. atzinumu 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 173. un 174. punkts).

Par informācijas par datu plūsmu un atrašanās vietas datu vākšanu reāllaikā

183 Attiecībā uz IDK L. 851-2. pantā paredzēto informācijas par datu plūsmu un atrašanās vietas datu vākšanu reāllaikā ir jānorāda, ka tā var tikt individuāli atļauta attiecībā uz "iepriekš identificētu personu, kas var būt saistīta ar [terorisma] draudiem". Tāpat saskaņā ar šo tiesību normu, "ja ir nopietni iemesli uzskatīt, ka viena vai vairākas personas, kas ietilpst attiecīgās personas, uz kuru attiecas atļauja, lokā, var sniegt informāciju atbilstoši atļaujas mērķim, to var piešķirt arī par katru no šīm personām individuāli".

184 Dati, uz kuriem attiecas šāda veida pasākums, ļauj kompetentajām valsts iestādēm atļaujas darbības laikā nepārtraukti un reāllaikā uzraudzīt sarunu partnerus, ar kuriem datu subjekti sazinās, viņu izmantotos līdzekļus, viņu komunikācijas ilgumu, kā arī viņu uzturēšanās vietas un pārvietošanos. Tāpat tie, šķiet, var atklāt tādas informācijas raksturu, ar kuru iepazīstas tiešsaistē. Kopumā šie dati, kā izriet no šī sprieduma 117. punkta, ļauj izdarīt ļoti precīzus secinājumus par datu subjektu privāto dzīvi un nodrošina līdzekļus, lai noteiktu to profilu – šāda informācija no tiesību uz privātās dzīves neaizskaramību viedokļa ir tikpat sensitīva kā pats komunikāciju saturs.

185 Attiecībā uz IDK L. 851-4. pantā paredzēto datu vākšanu reāllaikā šajā tiesību normā ir atļauts vākt tehniskos datus par galaiekārtu atrašanās vietu un tos reāllaikā nodot premjerministra dienestam. Šķiet, ka šādi dati ļauj kompetentajam dienestam jebkurā brīdī atļaujas darbības laikā nepārtraukti un reāllaikā noteikt izmantoto galaiekārtu, piemēram, mobilo tālruņu, atrašanās vietu.

186 Valsts tiesiskais regulējums, kas atļauj šādu vākšanu reāllaikā, tāpat kā tas, kas atļauj datu automatizētu analīzi, veido atkāpi no Direktīvas 2002/58 5. pantā noteiktā principiālā pienākuma nodrošināt elektronisko komunikāciju un ar to saistīto datu konfidencialitāti. Tādējādi arī tas ir iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās un tam var būt atturoša ietekme uz Hartas 11. pantā garantētās vārda brīvības īstenošanu.

187 Ir jāuzsver, ka iejaukšanās, ko rada datu vākšana reāllaikā, kas ļauj noteikt galaiekārtas atrašanās vietu, ir īpaši smaga, jo šie dati kompetentajām valsts iestādēm sniedz veidu, kā precīzi un pastāvīgi uzraudzīt mobilo tālruņu lietotāju pārvietošanos. Ciktāl šie dati tādējādi ir jāuzskata par īpaši sensitīviem, kompetento iestāžu piekļuve šādiem datiem reāllaikā ir jānošķir no piekļuves šiem datiem vēlāk, jo pirmā rada lielāku iejaukšanos, ciktāl ar to ir iespējama gandrīz pilnīga šo lietotāju uzraudzība (pēc analoģijas attiecībā uz ECPAK 8. pantu skat. ECT spriedumu, 2018. gada 8. februāris, *Ben Faiza* pret Franciju, CE:ECHR:2018:0208JUD003144612, 74. punkts). Šīs iejaukšanās intensitāte turklāt pastiprinās, ja vākšana reāllaikā attiecas arī uz informāciju par datu subjektu datu plūsmu.

188 Lai gan pamatlietā aplūkotajā valsts tiesiskajā regulējumā izvirzītais terorisma novēršanas mērķis, ņemot vērā tā nozīmīgumu, var pamatot iejaukšanos, ko rada informācijas par datu plūsmu un atrašanās vietas datu vākšana reāllaikā, šāds pasākums, ņemot vērā tā īpaši aizskarošo raksturu, var tikt īstenots tikai attiecībā uz personām, attiecībā uz kurām ir pamatots iemesls aizdomām, ka tās kaut kādā veidā ir iesaistītas terorisma darbībās. Šajā kategorijā neietilpstošo personu datiem var piekļūt tikai vēlāk, jo saskaņā ar Tiesas judikatūru tiem var piekļūt tikai īpašās situācijās, piemēram, tad, kad runa ir par teroristiskām darbībām un ja pastāv objektīvi apstākļi, kas ļauj uzskatīt, ka šie dati konkrētajā gadījumā varētu sniegt efektīvu ieguldījumu cīņā pret terorismu (šajā nozīmē skat. spriedumu, 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 119. punkts un tajā minētā judikatūra).

189 Turklāt lēmumam, ar kuru atļauj reāllaikā vākt informāciju par datu plūsmu un atrašanās vietas datus, ir jābūt pamatotam ar valsts tiesību aktos paredzētiem objektīviem kritērijiem. It īpaši šajos tiesību aktos saskaņā ar šī sprieduma 176. punktā minēto judikatūru ir jānosaka apstākļi un nosacījumi, kādos šāda vākšana var tikt atļauta, un jāparedz, kā tas ir precizēts iepriekšējā punktā, ka tā var skart vienīgi personas, kurām ir saikne ar terorisma novēršanas mērķi. Turklāt lēmumam, ar kuru atļauj reāllaikā vākt informāciju par datu plūsmu un atrašanās vietas datus, ir jābūt pamatotam ar valsts tiesību aktos paredzētiem objektīviem un nediskriminējošiem kritērijiem. Lai praksē nodrošinātu šo nosacījumu ievērošanu, ir būtiski, lai pasākuma, ar kuru atļauta vākšana reāllaikā, īstenošana būtu pakļauta iepriekšējai pārbaudei, ko veic tiesa vai neatkarīga administratīva iestāde, kuras lēmumam ir saistoša iedarbība, un ka šai tiesai vai šai iestādei turklāt ir jāpārliecinās, ka šāda vākšana reāllaikā tiek atļauta vienīgi absolūti nepieciešamā robežās (šajā nozīmē skat. spriedumu, 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 120. punkts). Pienācīgi pamatotos neatliekamības gadījumos pārbaude jāveic īsā laikā.

Par to personu informēšanu, kuru dati tiek vākti vai analizēti

190 Ir būtiski, lai kompetentās valsts iestādes, kuras veic informācijas par datu plūsmu un atrašanās vietas datu vākšanu reāllaikā, par to informētu datu subjektus atbilstoši piemērojamajām valsts procesuālajām normām tiktāl un no brīža, kad šī informēšana vairs nevar traucēt šo iestāžu uzdevumu izpildei. Šī informēšana faktiski ir nepieciešama, lai ļautu šīm personām īstenot to tiesības, kas izriet no Hartas 7. un 8. panta, lūgt piekļuvi saviem personas datiem, kas ir šo pasākumu priekšmets, un vajadzības gadījumā panāktu to labošanu vai dzēšanu, kā arī saskaņā ar Hartas 47. panta pirmo daļu

izmantotu tiesības par efektīvu tiesību aizsardzību tiesā, turklāt šādas tiesības ir skaidri garantētas Direktīvas 2002/58 15. panta 2. punktā, to lasot kopā ar Regulas 2016/679 79. panta 1. punktu (šajā nozīmē skat. spriedumu, 2016. gada 21. decembris, *Tele2*, C-203/15 un C-698/15, EU:C:2016:970, 121. punkts un tajā minētā judikatūra, kā arī atzinumu 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 219. un 220. punkts).

191 Attiecībā uz informēšanu, kas tiek prasīta informācijas par datu plūsmu un atrašanās vietas datu automatizētas analīzes kontekstā, jānorāda, ka kompetentajai valsts iestādei ir jāpublicē vispārēja rakstura informācija par šo analīzi, taču tai nav pienākuma individuāli informēt datu subjektus. Savukārt gadījumā, ja dati atbilst pasākumā, ar ko atļauta automatizētā analīze precizētajiem parametriem, un ja šī iestāde identificē datu subjektu, lai padziļināti analizētu datus, kas uz viņu attiecas, ir nepieciešams šo personu informēt individuāli. Tomēr šāda informācija ir jāsniedz tikai un vienīgi tādā apmērā un no tā brīža, kad tā nevar apdraudēt minētajai iestādei uzticēto uzdevumu izpildi (pēc analoģijas skat. atzinumu 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs, EU:C:2017:592, 222.–224. punkts).

192 Ņemot vērā visus iepriekš izklāstītos apsvērumus, uz otro un trešo jautājumu lietā C-511/18 ir jāatbild, ka Direktīvas 2002/58 15. panta 1. punkts, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, ir jāinterpretē tādējādi, ka tam nav pretrunā tāds valsts tiesiskais regulējums, ar kuru elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums veikt, pirmkārt, tostarp informācijas par datu plūsmu un atrašanās vietas datu automatizētu analīzi un vākšanu reāllaikā, un, otrkārt, tehnisko datu par izmanto galaiekārtu izmantošanu vākšanu reāllaikā, ja

– automatizētas analīzes izmantošana 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, lai pārliecinātos par tādas situācijas esamību, kas pamato minēto pasākumu, kā arī par to, vai ir ievēroti paredzētie nosacījumi un garantijas, un

– informācijas par datu plūsmu un atrašanās vietas datu vākšana 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, lai pārliecinātos, ka šāda vākšana reāllaikā ir atļauta vienīgi absolūti nepieciešamā apmērā. Pienācīgi pamatotos neatliekamības gadījumos pārbaude ir jāveic īsā laikā.

Par otro jautājumu lietā C-512/18

193 Ar otro jautājumu lietā C-512/18 iesniedzējtiesa būtībā vēlas noskaidrot, vai Direktīvas 2000/31 tiesību normas, lasot tās Hartas 6.–8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, ir jāinterpretē tādējādi, ka tām ir pretrunā valsts tiesiskais regulējums, ar kuru piekļuves publiskiem tiešsaistes komunikāciju pakalpojumiem sniedzējiem un mitināšanas pakalpojumu sniedzējiem ir noteikts pienākums veikt visaptverošu un nediferencētu ar šiem pakalpojumiem saistītu personas datu saglabāšanu.

194 Uzskatot, ka šādi pakalpojumi ietilpst Direktīvas 2000/31, nevis Direktīvas 2002/58 piemērošanas jomā, iesniedzējtiesa domā, ka Direktīvas 2000/31 15. panta 1. un 2. punkts, lasot tos kopā ar tās 12. un 14. pantu, paši par sevi nerada principiālu aizliegumu saglabāt datus par satura radīšanu, no kura varētu atkāpties tikai izņēmuma kārtā. Šī tiesa tomēr jautā, vai šis vērtējums ir atbalstāms, ņemot vērā nepieciešamību ievērot Hartas 6.–8. un 11. pantā nostiprinātās pamattiesības.

195 Turklāt iesniedzējtiesa precizē, ka tās jautājums attiecas uz *LCEN* 6. pantā, lasot to kopā ar Dekrētu Nr. 2011-219, paredzēto saglabāšanas pienākumu. Dati, kuri šajā ziņā ir jāsaglabā attiecīgajiem pakalpojumu sniedzējiem, ietver tostarp datus par to personu identitāti, kuras ir izmantojušas šos pakalpojumus, piemēram, viņu vārdu, uzvārdu, piesaistītās pasta adreses, elektroniskā pasta adreses vai piesaistīto kontu adreses, paroles un, ja līguma vai konta parakstīšana ir par maksu, izmantoto maksāšanas veidu, maksājuma references numuru, summu, kā arī darījuma datumu un laiku.

196 Tāpat dati, uz kuriem attiecas saglabāšanas pienākums, ietver abonentu, pieslēguma un izmantoto galaiekārtu identifikatorus, satura identifikatorus, pieslēgumu un darbību sākuma un beigu datumus un laikus, kā arī protokolu veidus, kas tiek izmantoti, lai pieslēgtos pakalpojumam un pārsūtītu saturu. Piekļuve šiem datiem, kuru glabāšanas ilgums ir viens gads, var tikt lūgta krimināprocesā un civilprocesā, lai ievērotu noteikumus par civiltiesisko vai krimināatbildību, kā arī saistībā ar izlūkdatu vākšanas pasākumiem, kuriem ir piemērojams IDK L. 851-1. pants.

197 Šajā ziņā ir jānorāda, ka saskaņā ar Direktīvas 2000/31 1. panta 2. punktu tā saskaņo konkrētus valsts noteikumus par informācijas sabiedrības pakalpojumiem, kas norādīti tās 2. panta a) punktā.

198 Šādi pakalpojumi, protams, ietver pakalpojumus, kuri tiek sniegti no attāluma ar elektroniskām iekārtām datu apstrādei un uzglabāšanai pēc pakalpojuma saņēmēja individuāla pieprasījuma un parasti pret atlīdzību, piemēram, piekļuves internetam vai komunikāciju tīkla pakalpojumi, kā arī mitināšanas pakalpojumi (šajā nozīmē skat. spriedumus, 2011. gada 24. novembris, *Scarlet Extended*, C-70/10, EU:C:2011:771, 40. punkts; 2012. gada 16. februāris, *SABAM*, C-360/10, EU:C:2012:85, 34. punkts; 2016. gada 15. septembris, *Mc Fadden*, C-484/14, EU:C:2016:689, 55. punkts, kā arī 2018. gada 7. augusts, *SNB-REACT*, C-521/17, EU:C:2018:639, 42. punkts un minētā judikatūra).

199 Tomēr Direktīvas 2000/31 1. panta 5. punktā ir noteikts, ka tā nav piemērojama jautājumiem, kuri attiecas uz informācijas sabiedrības pakalpojumiem un kuri ietverti direktīvās 95/46 un 97/66. Šajā ziņā no Direktīvas 2000/31 14. un 15. apsvēruma izriet, ka komunikācijas konfidencialitātes aizsardzību, kā arī fizisko personu aizsardzību attiecībā uz personas datu apstrādi informācijas sabiedrības pakalpojumu ietvaros reglamentē vienīgi Direktīvas 95/46 un 97/66, un Direktīvas 97/66 5. pantā komunikācijas konfidencialitātes mērķiem ir aizliegta jebkāda veida saziņas aizturēšana vai pārraudzība.

200 Līdz ar to jautājumi saistībā ar komunikāciju konfidencialitātes un personas datu aizsardzību ir jānovērtē Direktīvas 2002/58 un Regulas 2016/679 kontekstā, ar kurām ir aizstātas attiecīgi Direktīva 97/66 un Direktīva 95/46, precizējot, ka aizsardzība, kuras nodrošināšana ir Direktīvas 2000/31 mērķis, katrā ziņā nevar apdraudēt prasības, kas izriet no Direktīvas 2002/58 un Regulas 2016/679 (šajā nozīmē skat. spriedumu, 2008. gada 29. janvāris, *Promusicae*, C-275/06, EU:C:2008:54, 57. punkts).

201 Šī sprieduma 195. punktā minētajā valsts tiesiskajā regulējumā noteiktais pienākums piekļuves publiskiem tiešsaistes komunikāciju pakalpojumiem sniedzējiem un mitināšanas pakalpojumu sniedzējiem saglabāt ar šiem pakalpojumiem saistītos personas datus, līdz ar to, kā to būtībā ir norādījis ģenerāladvokāts secinājumu apvienotajās lietās *La Quadrature du Net* u.c. (C-511/18 un C-512/18, EU:C:2020:6) 141. punktā, ir jāizvērtē, ņemot vērā Direktīvu 2002/58 vai Regulu 2016/679.

202 Tādējādi atkarībā no tā, vai pakalpojumu sniegšana, uz kuriem attiecas šis valsts tiesiskais regulējums, ietilpst vai neietilpst Direktīvas 2002/58 piemērošanas jomā, to reglamentēs vai nu pēdējā minētā direktīva, it īpaši tās 15. panta 1. punkts, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, vai Regula 2016/679, it īpaši minētās regulas 23. panta 1. punkts, lasot to šo pašu Hartas noteikumu kontekstā.

203 Šajā gadījumā, kā savos rakstveida apsvērumos norāda Eiropas Komisija, nevar izslēgt, ka daži no pakalpojumiem, kuriem ir piemērojams šī sprieduma 195. punktā minētais valsts tiesiskais regulējums, ir elektronisko komunikāciju pakalpojumi Direktīvas 2002/58 izpratnē, un tas ir jāpārbauda iesniedzējtiesai.

204 Šajā ziņā ir jānorāda, ka Direktīva 2002/58 attiecas uz elektronisko komunikāciju pakalpojumiem, kas atbilst Direktīvas 2002/21 2. panta c) punktā norādītajiem nosacījumiem, uz kuriem ir atsauce Direktīvas 2002/58 2. pantā un kurā elektronisko komunikāciju pakalpojums ir definēts kā "pakalpojum[s], ko parasti nodrošina par atlīdzību un kas pilnīgi vai galvenokārt sastāv no signālu pārraidīšanas elektronisko komunikāciju tīklos, ietverot telekomunikāciju pakalpojumus un pārraidīšanas pakalpojumus tīklos, ko izmanto apraidei". Šī sprieduma 197. un 198. punktā norādītie un Direktīvā 2000/31 ietvertie informācijas sabiedrības pakalpojumi ir uzskatāmi par elektronisko komunikāciju pakalpojumiem, ja tie pilnībā vai galvenokārt sastāv no signālu pārraidīšanas elektronisko komunikāciju tīklos (šajā nozīmē skat. spriedumu, 2019. gada 5. jūnijs, *Skype Communications*, C-142/18, EU:C:2019:460, 47. un 48. punkts).

205 Līdz ar to interneta piekļuves pakalpojumi, uz kuriem, kā šķiet, attiecas šī sprieduma 195. punktā norādītais valsts tiesiskais regulējums, kā tas ir apstiprināts Direktīvas 2002/21 10. apsvērumā, ir uzskatāmi par elektronisko komunikāciju pakalpojumiem šīs direktīvas izpratnē (šajā nozīmē skat. spriedumu, 2019. gada 5. jūnijs, *Skype Communications*, C-142/18, EU:C:2019:460, 37. punkts). Tā tas ir arī interneta ziņapmaiņas pakalpojumu sniegšanas gadījumā, jo nešķiet, ka būtu izslēgts tas, ka arī tiem ir piemērojams šis valsts tiesiskais regulējums, jo tehniskā ziņā tie pilnībā vai galvenokārt sastāv no signālu pārraidīšanas elektronisko komunikāciju tīklos (šajā nozīmē skat. spriedumu, 2019. gada 13. jūnijs, *Google*, C-193/18, EU:C:2019:498, 35. un 38. punkts).

206 Attiecībā uz prasībām, kas izriet no Direktīvas 2002/58 15. panta 1. punkta, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, ir jāatsaucas uz visiem konstatējumiem un vērtējumiem, kas veikti, atbildot uz pirmajiem jautājumiem lietās C-511/18 un C-512/18, kā arī uz pirmo un otro jautājumu lietā C-520/18.

207 Attiecībā uz prasībām, kas izriet no Regulas 2016/679, jāatgādina, ka tās mērķis, kā izriet no tās 10. apsvēruma, tostarp ir nodrošināt augsta līmeņa aizsardzību fiziskām personām Savienībā un šai nolūkā nodrošināt noteikumu par fiziskas personas pamattiesību un pamatbrīvību aizsardzību attiecībā uz personas datu apstrādi vienveidīgu piemērošanu visā Savienībā (šajā nozīmē skat. spriedumu, 2020. gada 16. jūlijs, *Facebook Ireland* un *Schrems*, C-311/18, EU:C:2020:559, 101. punkts).

208 Šajā nolūkā jebkurai personas datu apstrādei, ievērojot Regulas 2016/679 23. pantā pieļautās atkāpes, ir jāatbilst principiem, kas reglamentē personas datu apstrādi, kā arī datu subjekta tiesības, kas noteiktas attiecīgi šīs regulas II un III nodaļā. Konkrētāk, jebkurai personas datu apstrādei, pirmkārt, ir jāatbilst minētās regulas 5. pantā noteiktajiem principiem un, otrkārt, jāatbilst šīs pašas regulas 6. pantā uzskaitītajiem likumības nosacījumiem (pēc analoģijas attiecībā uz Direktīvu 95/46 skat. spriedumu, 2013. gada 30. maijs, *Worten*, C-342/12, EU:C:2013:355, 33. punkts un tajā minētā judikatūra).

209 Konkrētāk, attiecībā uz Regulas 2016/679 23. panta 1. punktu ir jānorāda, ka tajā, tāpat kā tas ir paredzēts Direktīvas 2002/58 15. panta 1. punktā, dalībvalstīm ir atļauts, ņemot vērā tajā paredzētos mērķus un izmantojot tiesību aktus, ierobežot tajā paredzēto pienākumu un tiesību apjomu, "ja ar šādu ierobežojumu tiek ievērota pamattiesību un pamatbrīvību būtība un tas demokrātiskā sabiedrībā ir nepieciešams un samērīgs, lai garantētu" izraudzīto mērķi. Jebkurā tiesību aktā, kas pieņemts uz šī pamata, it īpaši ir jāievēro šīs regulas 23. panta 2. punktā noteiktās īpašās prasības.

210 Tādējādi Regulas 2016/679 23. panta 1. un 2. punkts nevar tikt interpretēti tādējādi, ka ar tiem dalībvalstīm tiek piešķirtas pilnvaras apdraudēt privātās dzīves neaizskaramību, neievērojot Hartas 7. pantu, kā arī citas tajā paredzētās garantijas (pēc analoģijas attiecībā uz Direktīvu 95/46 skat. spriedumu, 2003. gada 20. maijs, *Österreichischer Rundfunk* u.c., C-465/00, C-138/01 un C-139/01,

EU:C:2003:294, 91. punkts). Konkrētāk, tāpat kā attiecībā uz Direktīvas 2002/58 15. panta 1. punktu, pilnvaras, kas ar Regulas 2016/679 23. panta 1. punktu piešķirtas dalībvalstīm, var tikt īstenotas, vienīgi ievērojot samērīguma prasību, saskaņā ar kuru atkāpes no personas datu aizsardzības un tās ierobežojumi ir jāīsteno tikai, ciktāl tas ir absolūti nepieciešams (pēc analoģijas attiecībā uz Direktīvu 95/46 skat. spriedumu, 2013. gada 7. novembris, *IPI*, C-473/12, EU:C:2013:715, 39. punkts un tajā minētā judikatūra).

211 No tā izriet, ka konstatējumi un vērtējumi, kas veikti, atbildot uz pirmajiem jautājumiem lietās C-511/18 un C-512/18, kā arī uz pirmo un otro jautājumu lietā C-520/18, *mutatis mutandis* ir piemērojami Regulas 2016/679 23. pantam.

212 Ņemot vērā iepriekš minētos apsvērumus, uz otro jautājumu lietā C-512/18 ir jāatbild, ka Direktīva 2000/31 ir jāinterpretē tādējādi, ka tā nav piemērojama komunikāciju konfidencialitātes un fizisko personu aizsardzības jomā attiecībā uz personas datu apstrādi informācijas sabiedrības pakalpojumu ietvaros, jo šo aizsardzību atkarībā no gadījuma reglamentē Direktīva 2002/58 vai Regula 2016/679. Regulas 2016/679 23. panta 1. punkts, to lasot Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, ir jāinterpretē tādējādi, ka tas nepieļauj tādu valsts tiesisko regulējumu, kurā piekļuves publiskiem tiešsaistes komunikāciju pakalpojumiem sniedzējiem un mitināšanas pakalpojumu sniedzējiem ir noteikts pienākums veikt visaptverošu un nediferencētu ar šiem pakalpojumiem saistīto personas datu saglabāšanu.

Par trešo jautājumu lietā C-520/18

213 Ar trešo jautājumu lietā C-520/18 iesniedzējtiesa būtībā vēlas noskaidrot, vai valsts tiesa var piemērot savas valsts tiesību normu, ar kuru tā ir pilnvarota ierobežot laikā tāda konstatējuma par prettiesiskumu, kurš izriet no šo tiesību aktu nesaderības ar Direktīvas 2002/58 15. panta 1. punktu, to lasot Hartas 7., 8. un 11. panta, kā arī Hartas 52. panta 1. punkta kontekstā, iedarbību laikā, kas tai saskaņā ar šīm tiesībām ir jānosaka attiecībā uz valsts tiesību aktiem, ar kuriem elektronisko komunikāciju pakalpojumu sniedzējiem tiek noteikts pienākums – tostarp, lai sasniegtu valsts drošības aizsardzības un noziedzības apkarošanas mērķus, – veikt visaptverošu un nediferencētu informācijas par datu plūsmu un atrašanās vietas datu saglabāšanu.

214 Ar Savienības tiesību pārākuma principu tiek nostiprināta Savienības tiesību prioritāte pār dalībvalstu tiesībām. Tādējādi šis princips uzliek par pienākumu visām dalībvalstu iestādēm nodrošināt dažādo Savienības normu pilnīgu iedarbību, jo dalībvalstu tiesības nevar ietekmēt iedarbību, kura šīm dažādajām normām ir atzīta minēto valstu teritorijā (spriedumi, 1964. gada 15. jūlijs, *Costa*, 6/64, EU:C:1964:66, 1159. un 1160. punkts, kā arī 2019. gada 19. novembris, A. K. u.c. (Augstākās tiesas Disciplinārlietu palātas neatkarība), C-585/18, C-624/18 un C-625/18, EU:C:2019:982, 157. un 158. punkts un tajā minētā judikatūra).

215 Saskaņā ar pārākuma principu gadījumā, ja valsts tiesisko regulējumu nav iespējams interpretēt atbilstīgi Savienības tiesību prasībām, valsts tiesai, kurai ir pienākums savas kompetences ietvaros piemērot Savienības tiesību normas, ir uzdevums nodrošināt šo normu pilnīgu iedarbību, pēc savas ierosmes vajadzības gadījumā atstājot bez piemērošanas jebkuru tām pretrunā esošu valsts tiesību normu, pat vēlāk pieņemtu, un nav nepieciešams lūgt vai gaidīt, lai tā vispirms tiktu atcelta likumdošanas kārtībā vai ar kādu citu konstitūcijā paredzētu metodi (spriedumi, 2010. gada 22. jūnijs, *Melki* un *Abdeli*, C-188/10 un C-189/10, EU:C:2010:363, 43. punkts un tajā minētā judikatūra; 2019. gada 24. jūnijs, *Popławski*, C-573/17, EU:C:2019:530, 58. punkts, kā arī 2019. gada 19. novembris, A. K. u.c. (Augstākās tiesas Disciplinārlietu palātas neatkarība), C-585/18, C-624/18 un C-625/18, EU:C:2019:982, 160. punkts).

216 Vienīgi Tiesa izņēmuma kārtā un primāro tiesiskās drošības apsvērumu dēļ var noteikt nepiemērošanas seku – kādas rada Savienības tiesību normas piemērošana tai pretrunā esošām valsts tiesībām – īslaicīgu apturēšanu. Šādas Tiesas interpretācijas iedarbības laikā ierobežojums ir pieļaujams tikai spriedumā, kurā ir lemts par pieprasīto interpretāciju (šajā nozīmē skat. spriedumus, 2012. gada 23. oktobris, *Nelson* u.c., C-581/10 un C-629/10, EU:C:2012:657, 89. un 91. punkts; 2020. gada 23. aprīlis, *Herst*, C-401/18, EU:C:2020:295, 56. un 57. punkts, kā arī 2020. gada 25. jūnijs, A u.c. (Vējturbīnas Ālterā un Nēvelē), C-24/19, EU:C:2020:503, 84. punkts un tajā minētā judikatūra).

217 Savienības tiesību pārākums un vienveidīga piemērošana tiktu apdraudēti, ja valsts tiesām būtu pilnvaras piešķirt valsts tiesību normām pārākumu pār Savienības tiesībām, kurām šīs tiesību normas ir pretrunā, pat ja tas būtu tikai uz laiku (šajā nozīmē skat. spriedumu, 2019. gada 29. jūlijs, *Inter-Environnement Wallonie* un *Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU:C:2019:622, 177. punkts, kā arī tajā minētā judikatūra).

218 Tomēr lietā, kurā tika aplūkots tādu pasākumu tiesiskums, kas noteikti, neievērojot Savienības tiesībās noteiktu pienākumu veikt iepriekšēju projekta ietekmes uz vidi un uz aizsargājamo teritoriju novērtējumu, Tiesa nosprieda, ka valsts tiesa, ja tas ir atļauts valsts tiesībās, izņēmuma kārtā var paturēt spēkā šādu pasākumu sekas, ja šo paturēšanu spēkā pamato primāri apsvērumi, kas saistīti ar nepieciešamību novērst reālus un nopietnus attiecīgās dalībvalsts elektroapgādes traucējumu draudus, kurus nevar novērst ar citiem līdzekļiem un alternatīvām, it īpaši iekšējā tirgū, tomēr minētā paturēšana spēkā var attiekties tikai uz laiku, kas noteikti nepieciešams šī prettiesiskuma novēršanai (šajā nozīmē skat. spriedumu, 2019. gada 29. jūlijs, *Inter-Environnement Wallonie* un *Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU:C:2019:622, 175., 176., 179. un 181. punkts).

219 Pretēji tāda procesuālā pienākuma kā iepriekšēja projekta ietekmes uz konkrētu vides aizsardzības jomu neizpildei Direktīvas 2002/58 15. panta 1. punkta, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, neizpilde nevar tikt novērsta, izmantojot procedūru, kas ir pielīdzināma iepriekšējā punktā minētajai. Proti, tāda valsts tiesiskā regulējuma kā pamatlietā aplūkotais seku saglabāšana nozīmētu, ka ar šo tiesisko regulējumu elektronisko komunikāciju pakalpojumu sniedzējiem joprojām tiek noteikti pienākumi, kas ir pretrunā Savienības tiesībām un kas ietver nopietnu iejaukšanos to personu pamattiesībās, kuru dati ir tikuši saglabāti.

220 Līdz ar to iesniedzējtiesa nevar piemērot valsts tiesību normu, ar kuru tai ir piešķirtas tiesības ierobežot laikā tāda konstatējuma par prettiesiskumu sekas, kurš tai saskaņā ar šīm tiesībām jāveic attiecībā uz pamatlietā aplūkotajiem valsts tiesību aktiem.

221 To ņemot vērā, Tiesai iesniegtajos apsvērumos VZ, WY un XX apgalvo, ka trešais jautājums netieši, bet noteikti ir par to, vai Savienības tiesībām ir pretrunā tādas informācijas un pierādījumu izmantošana kriminālprocesā, kuri – pretrunā šīm tiesībām – iegūti, visaptveroši un nediferencēti saglabājot informāciju par datu plūsmu un atrašanās vietas datus.

222 Šajā ziņā, lai sniegtu iesniedzējtiesai lietderīgu atbildi, ir jāatgādina, ka saskaņā ar pašreiz spēkā esošajām Savienības tiesībām principā vienīgi valsts tiesībās ir jāparedz noteikumi par informācijas un pierādījumu, kas iegūti, veicot šādu datu saglabāšanu, kura ir pretrunā Savienības tiesībām, pieļaujamību un izvērtēšanu kriminālprocesā, kas uzsākts pret personām, kuras tiek turētas aizdomās par smaga nozieguma izdarīšanu.

223 Saskaņā ar pastāvīgo judikatūru, ja attiecīgajā jomā nav Savienības noteikumu, katras dalībvalsts tiesību sistēmā saskaņā ar to procesuālās autonomijas principu ir jānosaka tiesvedības procesuālie noteikumi, kam jānodrošina to tiesību aizsardzība, kuras attiecīgajām personām piešķirtas Savienības tiesībās, tomēr ar nosacījumu, ka šie noteikumi nedrīkst būt mazāk labvēlīgi par tiem, kas attiecas uz līdzīgām iekšēja rakstura prasībām (līdzvērtības princips), un tie nedrīkst padarīt praktiski neiespējamu vai pārmērīgi grūtu to tiesību īstenošanu, kas piešķirtas Savienības tiesību sistēmā (efektivitātes princips) (šajā nozīmē skat. spriedumus, 2015. gada 6. oktobris, *Târşia*, C-69/14, EU:C:2015:662, 26. un

27. punkts; 2018. gada 24. oktobris, XC u.c., C-234/17, EU:C:2018:853, 21. un 22. punkts, kā arī tajos minētā judikatūra, un 2019. gada 19. decembris, *Deutsche Umwelthilfe*, C-752/18, EU:C:2019:1114, 33. punkts).

224 Attiecībā uz līdzvērtības principu valsts tiesai, kas izskata krimināllietu, pamatojoties uz informāciju vai pierādījumiem, kas iegūti, neievērojot no Direktīvas 2002/58 izrietošās prasības, ir jāpārbauda, vai valsts tiesībās, kas reglamentē šo procedūru, ir paredzēti mazāk labvēlīgi noteikumi šādas informācijas un šādu pierādījumu pieļaujamībai un izmantošanai nekā noteikumi, kas reglamentē informāciju un pierādījumus, kuri iegūti, pārkāpjot valsts tiesības.

225 Attiecībā uz efektivitātes principu ir jānorāda, ka valsts tiesību normu par informācijas un pierādījumu pieļaujamību un izmantošanu mērķis atbilstoši valsts tiesībās izdarītajām izvēlēm ir izvairīties no tā, ka prettiesiski iegūta informācija un pierādījumi nepamatoti kaitē personai, kas tiek turēta aizdomās par noziedzīgu nodarījumu izdarīšanu. Tomēr saskaņā ar valsts tiesībām šis mērķis var tikt sasniegts ne tikai ar aizliegumu izmantot šādu informāciju un pierādījumus, bet arī ar valsts noteikumiem un praksi, kas reglamentē informācijas un pierādījumu izvērtēšanu un līdzsvarošanu, vai pat ar to, ka, nosakot sodu, tiek ņemts vērā to prettiesiskais raksturs.

226 To ņemot vērā, no Tiesas judikatūras izriet, ka nepieciešamība izslēgt informāciju un pierādījumus, kas iegūti, neievērojot Savienības tiesību prasības, ir jāizvērtē, tostarp ņemot vērā risku, ko šādas informācijas un pierādījumu pieņemamība rada sacīkstes principa ievērošanai un līdz ar to – tiesībām uz lietas taisnīgu izskatīšanu (šajā nozīmē skat. spriedumu, 2003. gada 10. aprīlis, *Steffensen*, C-276/01, EU:C:2003:228, 76. un 77. punkts). Tiesai, kas uzskata, ka lietas dalībnieks nevar efektīvi paust nostāju par pierādījumu, kas izriet no jomas, kura nav zināma tiesām un kas var būtiski ietekmēt faktu vērtējumu, ir jākonstatē tiesību uz lietas taisnīgu izskatīšanu pārkāpums un jāizslēdz šis pierādīšanas līdzeklis, lai izvairītos no šāda pārkāpuma (šajā nozīmē skat. spriedumu, 2003. gada 10. aprīlis, *Steffensen*, C-276/01, EU:C:2003:228, 78. un 79. punkts).

227 Līdz ar to efektivitātes princips valsts krimināllietu tiesai nosaka pienākumu neņemt vērā informāciju un pierādījumus, kas – pretrunā Savienības tiesībām – ir iegūti, visaptveroši un nediferencēti saglabājot informāciju par datu plūsmu un atrašanās vietas datus, kriminālprocesā, kas uzsākts pret personām, kuras tiek turētas aizdomās par noziegumiem, ja šīs personas nespēj efektīvi paust nostāju par šo informāciju un šiem pierādījumiem, kuru jomu tiesas nepārzina un kuri var būtiski ietekmēt faktu vērtējumu.

228 Ņemot vērā iepriekš minētos apsvērumus, uz trešo jautājumu lietā C-520/18 ir jāatbild, ka valsts tiesa nevar piemērot valsts tiesību normu, ar kuru tā ir pilnvarota ierobežot laikā tāda konstatējuma par prettiesiskumu iedarbību laikā, kas tai saskaņā ar šīm tiesībām ir jāveic attiecībā uz valsts tiesību aktiem, ar kuriem elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums – tostarp, ņemot vērā valsts drošības aizsardzību un noziedzības apkarošanu, – veikt visaptverošu un nediferencētu informācijas par datu plūsmu un atrašanās vietas datu saglabāšanu, kas nav saderīga ar Direktīvas 2002/58 15. panta 1. punktu, to lasot Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā. Šajā 15. panta 1. punktā, to interpretējot atbilstoši efektivitātes principam, valsts krimināltiesai ir noteikts pienākums neņemt vērā informāciju un pierādījumus, kas – pretrunā Savienības tiesībām – ir iegūti, visaptveroši un nediferencēti saglabājot informāciju par datu plūsmu un atrašanās vietas datus, krimināllietā, kas ierosināta pret personām, kuras tiek turētas aizdomās par noziegumu, ja šīs personas nevar efektīvi paust nostāju par šo informāciju un šiem pierādījumiem, kuru jomu tiesas nepārzina un kuri var būtiski ietekmēt faktu vērtējumu.

Par tiesāšanās izdevumiem

229 Attiecībā uz pamatlietu pusēm šī tiesvedība ir stadija procesā, kuru izskata iesniedzējtiesas, un tās lemj par tiesāšanās izdevumiem. Izdevumi, kas radušies, iesniedzot apsvērumus Tiesai, un kas nav minēto pušu izdevumi, nav atlīdzināmi.

Ar šādu pamatojumu Tiesa (virspalāta) nospriež:

1) **Eiropas Parlamenta un Padomes Direktīvas 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privātās dzīves aizsardzību un elektroniskajām komunikācijām), kurā grozījumi ir izdarīti ar Eiropas Parlamenta un Padomes Direktīvu 2009/136/EK (2009. gada 25. novembris), 15. panta 1. punkts, lasot to Eiropas Savienības Pamattiesību hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, ir jāinterpretē tādējādi, ka tam pretrunā ir tādi tiesību akti, ar kuriem 15. panta 1. punktā paredzētajiem mērķiem preventīvi ir paredzēta informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta saglabāšana. Turpretī Direktīvas 2002/58 15. panta 1. punktam, kas grozīts ar Direktīvu 2009/136, to lasot Pamattiesību hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, nav pretrunā tiesību akti,**

   – **ar kuriem – gadījumā, ja elektronisko komunikāciju pakalpojumu sniedzējiem ir izdots rīkojums veikt visaptverošu un nediferencētu informācijas par datu plūsmu un atrašanās vietas datu saglabāšanu situācijās, kad attiecīgā dalībvalsts sastopas ar nopietniem draudiem valsts drošībai, kuri izrādās patiesi un faktiski vai paredzami, – valsts drošības aizsardzības nolūkā ir atļauts pieņemt lēmumu, kurā ir paredzēts, ka šis rīkojums var tikt pakļauts efektīvai pārbaudei tiesā vai arī neatkarīgā administratīvā iestādē, kuras nolēmumam ir saistoša iedarbība, lai pārbaudītu šādas situācijas esamību, kā arī paredzēto nosacījumu un garantiju ievērošanu, un minēto rīkojumu var izdot vienīgi uz absolūti nepieciešamo laiku, tomēr šo termiņu var pagarināt, ja šāds apdraudējums saglabājas;**

   – **kas, lai aizsargātu valsts drošību, apkarotu smagus noziegumus un novērstu nopietnus draudus sabiedrības drošībai, paredz informācijas par datu plūsmu un atrašanās vietas datu mērķorientētu saglabāšanu, kura, pamatojoties uz objektīviem un nediskriminējošiem elementiem, tiek ierobežota atkarībā no attiecīgo personu kategorijām vai pamatojoties uz ģeogrāfisku kritēriju, uz laiku, kas nepārsniedz absolūti nepieciešamo, kuru tomēr var pagarināt;**

   – **kas, lai aizsargātu valsts drošību, apkarotu smagus noziegumus un novērstu nopietnus draudus sabiedrības drošībai, paredz visaptveroši un nediferencēti saglabāt savienojuma avotam piešķirtās IP adreses uz laiku, kas nepārsniedz absolūti nepieciešamo;**

   – **kas, lai aizsargātu valsts drošību, apkarotu smagus noziegumus un novērstu nopietnus draudus sabiedrības drošībai, paredz visaptverošu un nediferencētu elektronisko komunikāciju līdzekļu lietotāju identitātes datu saglabāšanu un,**

   – **kas, lai apkarotu smagus noziegumus un *a fortiori* aizsargātu valsts drošību, ļauj ar kompetentās iestādes lēmumu, kurš ir pakļauts efektīvai pārbaudei tiesā, izdot rīkojumu elektronisko komunikāciju pakalpojumu sniedzējiem uz noteiktu laiku operatīvi saglabāt šo pakalpojumu sniedzēju rīcībā esošo informāciju par datu plūsmu un atrašanās vietas datus,**

ja ar šiem pasākumiem ar skaidriem un precīziem noteikumiem tiek nodrošināts, ka attiecīgo datu saglabāšana notiek atbilstoši tai paredzētajiem materiāltiesiskajiem un procesuālajiem nosacījumiem un ka datu subjektiem ir efektīvas garantijas pret ļaunprātīgas izmantošanas risku.

2) **Direktīvas 2002/58 15. panta 1. punkts, kas grozīts ar Direktīvu 2009/136, to lasot Pamattiesību hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, ir jāinterpretē tādējādi, ka tam nav pretrunā tāds valsts tiesiskais regulējums, ar kuru elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums veikt, pirmkārt, tostarp informācijas par datu plūsmu un atrašanās vietas datu automatizētu analīzi un vākšanu reāllaikā, un, otrkārt, tehnisko datu par izmanto galaiekārtu izmantošanu vākšanu reāllaikā, ja**

   – **automatizētas analīzes izmantošana 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, lai pārliecinātos par tādas situācijas esamību, kas pamato minēto pasākumu, kā arī par to, vai ir ievēroti paredzētie nosacījumi un garantijas, un**

   – **informācijas par datu plūsmu un atrašanās vietas datu vākšana 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, lai pārliecinātos, ka šāda vākšana reāllaikā ir atļauta vienīgi absolūti nepieciešamā apmērā. Pienācīgi pamatotos neatliekamības gadījumos pārbaude ir jāveic īsā laikā.**

3) **Eiropas Parlamenta un Padomes Direktīva 2000/31/EK (2000. gada 8. jūnijs) par dažiem informācijas sabiedrības pakalpojumu tiesiskiem aspektiem, jo īpaši elektronisko tirdzniecību, iekšējā tirgū (Direktīva par elektronisko tirdzniecību) ir jāinterpretē tādējādi, ka tā nav piemērojama komunikāciju konfidencialitātes un fizisko personu aizsardzības jomā attiecībā uz personas datu apstrādi informācijas sabiedrības pakalpojumu ietvaros, jo šo aizsardzību atkarībā no gadījuma reglamentē Direktīva 2002/58, kas grozīta ar Direktīvu 2009/136, vai Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46. Regulas 2016/679 23. panta 1. punkts, to lasot Pamattiesību hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā, ir jāinterpretē tādējādi, ka tas nepieļauj tādu valsts tiesisko regulējumu, kurā piekļuves publiskiem tiešsaistes komunikāciju pakalpojumiem sniedzējiem un mitināšanas pakalpojumu sniedzējiem ir noteikts pienākums veikt visaptverošu un nediferencētu ar šiem pakalpojumiem saistīto personas datu saglabāšanu.**

4) **Valsts tiesa nevar piemērot valsts tiesību normu, ar kuru tā ir pilnvarota ierobežot laikā tāda konstatējuma par prettiesiskumu iedarbību laikā, kas tai saskaņā ar šīm tiesībām ir jāveic attiecībā uz valsts tiesību aktiem, ar kuriem elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums – tostarp, ņemot vērā valsts drošības aizsardzību un noziedzības apkarošanu, – veikt visaptverošu un nediferencētu informācijas par datu plūsmu un atrašanās vietas datu saglabāšanu, kas nav saderīga ar Direktīvas 2002/58, kas grozīta ar Direktīvu 2009/136, 15. panta 1. punktu, to lasot Pamattiesību hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta kontekstā. Šajā 15. panta 1. punktā, to interpretējot atbilstoši efektivitātes principam, valsts krimināltiesai ir noteikts pienākums neņemt vērā informāciju un pierādījumus, kas – pretrunā Savienības tiesībām – ir iegūti, visaptveroši un nediferencēti saglabājot informāciju par datu plūsmu un atrašanās vietas datus, kriminālllietā, kas ierosināta**

pret personām, kuras tiek turētas aizdomās par noziegumu, ja šīs personas nevar efektīvi paust nostāju par šo informāciju un šiem pierādījumiem, kuru jomu tiesas nepārzina un kuri var būtiski ietekmēt faktu vērtējumu.

[Paraksti]