Zbirka odločb sodne prakse

SODBA SODIŠČA (veliki senat)

z dne 6. oktobra 2020 *

(besedilo, popravljeno s sklepom z dne 16. novembra 2020)

Kazalo

Pravni okvir 6

Pravo Unije 6

Direktiva 95/46 6

Direktiva 97/66 7

Direktiva 2000/31 7

Direktiva 2002/21 8

Direktiva 2002/58 9

Uredba št. 2016/679 13

Francosko pravo 16

Code de la sécurité intérieure (zakonik o notranji varnosti) 16

CPCE 21

Zakon št. 2004-575 z dne 21. junija 2004 o zaupanju v digitalno gospodarstvo 23

Odlok št. 2011-219 23

Belgijsko pravo 25

Spori o glavni stvari in vprašanja za predhodno odločanje 27

Zadeva C-511/18 27

Zadeva C-512/18 29

* Jezik postopka: francoščina.

Zadeva C-520/18 30

Postopek pred Sodiščem 32

Vprašanja za predhodno odločanje 32

Prvi vprašanji v zadevah C-511/18 in C-512/18 ter prvo in drugo vprašanje v zadevi C-520/18 32

Uvodne ugotovitve 32

Področje uporabe Direktive 2002/58 33

Razlaga člena 15(1) Direktive 2002/58 36

– Zakonski ukrepi, s katerimi je za zaščito nacionalne varnosti določena preventivna hramba podatkov o prometu in podatkov o lokaciji 40

– Zakonski ukrepi, s katerimi je za boj proti kriminalu in zaščito javne varnosti določena preventivna hramba podatkov o prometu in podatkov o lokaciji 41

– Zakonski ukrepi, s katerimi je za boj proti kriminalu in zaščito javne varnosti določena preventivna hramba naslovov IP in podatkov o civilni identiteti 43

– Zakonski ukrepi, s katerimi je za boj proti hudemu kriminalu določena takojšnja hramba podatkov o prometu in podatkov o lokaciji 44

Drugo in tretje vprašanje v zadevi C-511/18 46

Avtomatizirana analiza podatkov o prometu in podatkov o lokaciji 47

Zbiranje podatkov o prometu in podatkov o lokaciji v realnem času 49

Obvestitev oseb, katerih podatki so bili zbrani ali analizirani 50

Drugo vprašanje v zadevi C-512/18 51

Tretje vprašanje v zadevi C-520/18 53

Stroški 55

„Predhodno odločanje – Obdelava osebnih podatkov na področju elektronskih komunikacij – Ponudniki elektronskih komunikacijskih storitev – Ponudniki storitev gostovanja in ponudniki dostopa do interneta – Splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji – Avtomatizirana analiza podatkov – Dostop do podatkov v realnem času – Zaščita nacionalne varnosti in boj proti terorizmu – Boj proti kriminalu – Direktiva 2002/58/ES – Področje uporabe – Člen 1(3) in člen 3 – Zaupnost elektronskih komunikacij – Varstvo – Člen 5 in člen 15(1) – Direktiva 2000/31/ES – Področje uporabe – Listina Evropske unije o temeljnih pravicah – Členi 4, od 6 do 8 in 11 ter člen 52(1) – Člen 4(2) PEU“

V združenih zadevah C-511/18, C-512/18 in C-520/18,

katerih predmet so predlogi za sprejetje predhodne odločbe na podlagi člena 267 PDEU, ki sta jih vložila Conseil d'État (državni svet, Francija) z odločbama z dne 26. julija 2018, ki sta na Sodišče prispeli 3. avgusta 2018 (C-511/18 in C-512/18), in Cour constitutionnelle (ustavno sodišče, Belgija) z odločbo z dne 19. julija 2018, ki je na Sodišče prispela 2. avgusta 2018 (C-520/18), v postopkih

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

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

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

Igwan.net (C-511/18),

proti

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

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

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18), ob udeležbi

Privacy International (C-512/18),

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

ter

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

proti

Conseil des ministres,

ob udeležbi

Child Focus (C-520/18),

SODIŠČE (veliki senat)

v sestavi K. Lenaerts, predsednik, R. Silva de Lapuerta, podpredsednica, J.-C. Bonichot, A. Arabadjiev, predsednika senatov, A. Prechal, predsednica senata, M. Safjan, P. G. Xuereb, predsednika senatov, in L. S. Rossi, predsednica senata, J. Malenovský, L. Bay Larsen, T. von Danwitz (poročevalec), sodniki, C. Toader, K. Jürimäe, sodnici, C. Lycourgos in N. Piçarra, sodnika,

generalni pravobranilec: M. Campos Sánchez-Bordona,

sodna tajnica: C. Strömholm, administratorka,

na podlagi pisnega postopka in obravnave z dne 9. in 10. septembra 2019,

ob upoštevanju stališč, ki so jih predložili:

– za Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net in Center for Democracy and Technology A. Fitzjean Ò Cobhthaigh, avocat,

– za French Data Network Y. Padova, avocat,

– za Privacy International H. Roy, avocat,

– za Ordre des barreaux francophones in germanophone E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart in J.-F. Henrotte, avocats,

– za Académie Fiscale ASBL in UA J.-P. Riquet,

– za Liga voor Mensenrechten ASBL J. Vander Velpen, avocat,

– za Ligue des Droits de l'Homme ASBL R. Jespers in J. Fermon, avocats,

– za VZ, WY in XX D. Pattyn, avocat,

– za Child Focus N. Buisseret, K. De Meester in J. Van Cauter, avocats,

– za francosko vlado sprva D. Dubois, F. Alabrune, D. Colas, E. de Moustier in A.-L. Desjonquères, nato D. Dubois, F. Alabrune, E. de Moustier in A.-L. Desjonquères, agenti,

– za belgijsko vlado J.-C. Halleux, P. Cottin in C. Pochet, agenti, skupaj z J. Vanpraetom, Y. Peetersom, S. Depréjem in E. de Lophemom, avocats,

– za češko vlado M. Smolek, J. Vláčil in O. Serdula, agenti,

– za dansko vlado sprva J. Nymann-Lindegren, M. Wolff in P. Ngo, nato J. Nymann-Lindegren in M. Wolff, agenti,

– za nemško vlado sprva J. Möller, M. Hellmann, E. Lankenau, R. Kanitz in T. Henze, nato J. Möller, M. Hellmann, E. Lankenau in R. Kanitz, agenti,

– za estonsko vlado N. Grünberg in A. Kalbus, agentki,

– za irsko vlado A. Joyce, M. Browne in G. Hodge, agenti, skupaj z D. Fennellyem, BL,

– za špansko vlado sprva L. Aguilera Ruiz in A. Rubio González, nato L. Aguilera Ruiz, agenta,

– za ciprsko vlado E. Neofytou, agentka,

– za latvijsko vlado V. Soņeca, agentka,

– za madžarsko vlado sprva M. Z. Fehér in Z. Wagner, nato M. Z. Fehér, agenta,

– za nizozemsko vlado M. K. Bulterman in A. M. de Ree, agenta,

– za poljsko vlado B. Majczyna, J. Sawicka in M. Pawlicka, agenti,

– za švedsko vlado sprva H. Shev, H. Eklinder, C. Meyer-Seitz in A. Falk, nato H. Shev, H. Eklinder, C. Meyer-Seitz in J. Lundberg, agenti,

– za vlado Združenega kraljestva S. Brandon, agent, skupaj z G. Facenno, QC, in C. Knightom, barrister,

– [alinea, izbrisana s sklepom z dne 16. novembra 2020]

– za Evropsko komisijo sprva H. Kranenborg, M. Wasmeier in P. Costa de Oliveira, nato H. Kranenborg in M. Wasmeier, agenti,

– za Evropskega nadzornika za varstvo podatkov T. Zerdick in A. Buchta, agenta,

po predstavitvi sklepnih predlogov generalnega pravobranilca na obravnavi 15. januarja 2020

izreka naslednjo

Sodbo

1 Predlogi za sprejetje predhodne odločbe se nanašajo na razlago, prvič, člena 15(1) Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514), kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 (UL 2009, L 337, str. 11) (v nadaljevanju: Direktiva 2002/58), in drugič, členov od 12 do 15 Direktive 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 25, str. 399) v povezavi s členi 4, od 6 do 8 in 11 ter členom 52(1) Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina) ter členom 4(2) PEU.

2 Predlog v zadevi C-511/18 je bil vložen v okviru sporov med organizacijami Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs in Igwan.net na eni strani ter Premier ministre (predsednik vlade, Francija), Garde des Sceaux, ministre de la Justice (minister za pravosodje, Francija), ministre de l'Intérieur (minister za notranje zadeve, Francija) in ministre des Armées (minister za obrambo, Francija) na drugi strani glede zakonitosti décret no 2015-1185, du 28 septembre 2015, portant désignation des services spécialisés de renseignement (odlok št. 2015-1185 z dne 28. septembra 2015 o imenovanju posebnih obveščevalnih služb) (JORF z dne 29. septembra 2015, besedilo 1 od 97, v nadaljevanju: odlok št. 2015-1185), décret no 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 (odlok št. 2015-1211 z dne 1. oktobra 2015 o sporih glede izvajanja obveščevalnih metod, za katere je potrebno dovoljenje, in datotek, ki zadevajo državno varnost) (JORF z dne 2. oktobra 2015, besedilo 7 od 108, v nadaljevanju: odlok št. 2015-1211),

décret no 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 (odlok št. 2015-1639 z dne 11. decembra 2015 o imenovanju služb, ki niso posebne obveščevalne službe in ki lahko uporabljajo metode, navedene pod naslovom V knjige VIII zakonika o notranji varnosti, ki je bil sprejet na podlagi člena L. 811-4 zakonika o notranji varnosti) (JORF z dne 12. decembra 2015, besedilo 28 od 127, v nadaljevanju: odlok št. 2015-1639) in décret no 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement (odlok št. 2016-67 z dne 29. januarja 2016 o metodah zbiranja informacij) (JORF z dne 31. januarja 2016, besedilo 2 od 113, v nadaljevanju: odlok št. 2016-67).

3 Predlog v zadevi C-512/18 je bil vložen v okviru sporov med organizacijami French Data Network, la Quadrature du Net in Fédération des fournisseurs d'accès à Internet associatifs na eni strani ter Premier ministre (predsednik vlade, Francija) in Garde des Sceaux, ministre de la Justice (minister za pravosodje, Francija) na drugi strani glede zakonitosti člena R. 10-13 code des postes et des communications électroniques (zakonik o pošti in elektronskih komunikacijah) (v nadaljevanju: CPCE) in décret no 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 (odlok št. 2011-219 z dne 25. februarja 2011 o hrambi in posredovanju podatkov, na podlagi katerih je mogoče identificirati vsako osebo, ki je sodelovala pri ustvarjanju vsebine, dane na splet) (JORF z dne 1. marca 2011, besedilo 32 od 170, v nadaljevanju: odlok št. 2011-219).

4 Predlog v zadevi C-520/18 je bil vložen v okviru sporov med Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY in XX na eni strani ter Conseil des ministres (svet ministrov, Belgija) na drugi strani glede zakonitosti loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (zakon z dne 29. maja 2016 o zbiranju in hrambi podatkov na področju elektronskih komunikacij) (Moniteur belge z dne 18. julija 2016, str. 44717, v nadaljevanju: zakon z dne 29. maja 2016).

Pravni okvir

Pravo Unije

Direktiva 95/46

5 Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 15, str. 355) je bila z učinkom od 25. maja 2018 razveljavljena z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (UL 2016, L 119, str. 1). Člen 3(2) Direktive 95/46 je določal:

„Ta direktiva se ne uporablja za obdelavo osebnih podatkov:

– med dejavnostjo, ki ne sodi na področje uporabe zakonodaje Skupnosti, kot so tiste, opredeljene v naslovih V in VI Pogodbe o Evropski uniji, in v vsakem primeru v postopkih obdelave v zvezi z javno varnostjo, obrambo, državno varnostjo (vključno z gospodarsko blaginjo države, kadar se postopek obdelave nanaša na zadeve državne varnosti) in pri dejavnostih države na področju kazenskega prava,

– s strani fizične osebe med potekom popolnoma osebne ali domače dejavnosti."

6 Člen 22 Direktive 95/46 iz poglavja III, naslovljenega „Pravna sredstva, odgovornost in sankcije“, je določal:

„Brez poseganja v upravnopravna pravna sredstva pred predložitvijo zadeve sodnemu organu, ki jih je možno med drugim predvideti pred nadzornim organom iz člena 28, države članice zagotovijo, da ima vsaka oseba v primeru kršitve pravic, zagotovljenih z nacionalno zakonodajo, ki se nanaša na zadevno obdelavo, pravico vložiti pravno sredstvo na sodišču.“

Direktiva 97/66

7 Člen 5 Direktive 97/66/ES Evropskega parlamenta in Sveta z dne 15. decembra 1997 o obdelavi osebnih podatkov in varstvu zasebnosti na področju telekomunikacij (UL 1997, L 24, str. 1), naslovljen „Zaupnost sporočil“, je določal:

„1. Države članice z nacionalnimi predpisi zagotovijo zaupnost sporočil, ki se pošiljajo prek javnega telekomunikacijskega omrežja ali javno dostopnih telekomunikacijskih storitev. Zlasti prepovejo vsem osebam razen uporabnikom, da brez privolitve zadevnih uporabnikov poslušajo, prisluškujejo, shranjujejo ali na druge načine prestrezajo ali nadzirajo sporočila, razen kadar je to zakonsko dovoljeno v skladu s členom 14(1).

2. Odstavek 1 ne vpliva na zakonsko dovoljeno zapisovanje/snemanje sporočil/komunikacij, če se to izvaja v okviru zakonite poslovne prakse z namenom, da se zagotovi dokaz o tržni transakciji ali kateri koli drugi poslovni komunikaciji.“

Direktiva 2000/31

8 V uvodnih izjavah 14 in 15 Direktive 2000/31 je navedeno:

„(14) Varstvo posameznikov v zvezi z obdelavo osebnih podatkov urejata izključno Direktiva [95/46] ter Direktiva [97/66], ki se v celoti uporabljata za storitve informacijske družbe; ker direktivi že oblikujeta pravni okvir Skupnosti na področju osebnih podatkov, tega vprašanja zaradi zagotavljanja nemotenega delovanja notranjega trga in predvsem prostega pretoka osebnih podatkov med državami članicami ni treba obravnavati v tej direktivi; njeno izvajanje in uporaba bi morala biti popolnoma usklajena z načeli o varstvu osebnih podatkov, predvsem glede nepovabljenih komercialnih sporočil in odgovornosti posrednikov; ta direktiva ne more prepovedati anonimne rabe odprtih omrežij, npr. interneta;

(15) Člen 5 Direktive [97/66] zagotavlja zaupnost sporočil; države članice morajo skladno s to direktivo prepovedati, da bi tisti, ki ni pošiljatelj ali prejemnik, prestregel ali nadzoroval sporočilo, razen če je to z zakonom dovoljeno“.

9 Člen 1 Direktive 2000/31 določa:

„1. Cilj te direktive je prispevati k pravilnemu delovanju notranjega trga z zagotavljanjem prostega pretoka storitev informacijske družbe med državami članicami.

2. Ta direktiva usklajuje, kolikor je to potrebno za dosego ciljev iz odstavka 1, nekatere nacionalne določbe o storitvah informacijske družbe glede notranjega trga, sedeža ponudnikov storitev, komercialnih sporočil, elektronskih pogodb, odgovornosti posrednikov, kodeksov ravnanja, izvensodnih poravnav sporov, sodnega varstva in sodelovanja med državami članicami.

3. Ta direktiva dopolnjuje pravo Skupnosti, ki se uporablja za storitve informacijske družbe, in ne posega v stopnjo zaščite, še posebno ne javnega zdravja in varstva interesov potrošnikov, kakor izhaja iz pravnih aktov Skupnosti in nacionalne zakonodaje za njihovo izvajanje, če to ne omejuje svobode zagotavljanja storitev informacijske družbe.

[…]

5. Ta direktiva se ne uporablja za:

[…]

(b) vprašanja v zvezi s storitvami informacijske družbe, ki jih zajemata Direktivi [95/46] in [97/66];

[…]“

10 Člen 2 Direktive 2000/31 določa:

„Za namene te direktive imajo posamezni izrazi, uporabljeni v tej direktivi, naslednji pomen:

(a) ‚storitve informacijske družbe‘: storitve v smislu člena 1(2) Direktive 98/34/ES [Evropskega parlamenta in Sveta z dne 22. junija 1998 o določitvi postopka za zbiranje informacij na področju tehničnih standardov in tehničnih predpisov o storitvah informacijske družbe (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 20, str. 337)], spremenjene z Direktivo 98/48/ES [Evropskega parlamenta in Sveta z dne 20. julija 1998 (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 21, str. 8)];

[…]“

11 Člen 15 Direktive 2000/31 določa:

„1. Države članice ponudnikom glede opravljanja storitev iz členov 12, 13 in 14 ne predpišejo splošne obveznosti za nadzor podatkov pri njihovem prenosu ali shranjevanju, pa tudi ne za dejavno raziskovanje okoliščin, na podlagi katerih se domneva, da gre za nezakonito dejavnost.

2. Države članice lahko določijo, da morajo ponudniki storitev informacijske družbe nemudoma obvestiti pristojne organe o domnevnih nezakonitih dejavnostih ali podatkih prejemnikov njihove storitve ali da morajo pristojnim organom na zahtevo sporočiti podatke, na podlagi katerih je možno identificirati prejemnike njihove storitve, s katerimi so sklenili dogovore o shranjevanju.“

Direktiva 2002/21

12 V uvodni izjavi 10 Direktive Evropskega parlamenta in Sveta 2002/21/ES z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve (okvirna direktiva) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 349) je navedeno:

„Opredelitev ‚storitve informacijske družbe‘ v členu 1 Direktive [98/34, kakor je bila spremenjena z Direktivo 98/48,] obsega široko področje gospodarskih dejavnosti, ki potekajo sprotno (on-line). Večina teh dejavnosti ni vključena v področje uporabe te direktive, ker dejavnosti niso v celoti ali pretežno sestavljene iz prenosa signalov po elektronskih komunikacijskih omrežjih. Storitve prenosa govorne telefonije in elektronske pošte so vključene v to direktivo. Eno podjetje, na primer ponudnik internetnih storitev, lahko ponudi elektronsko komunikacijsko storitev, kot je dostop do interneta, in storitve, ki niso zajete v tej direktivi, kot je zagotavljanje internetnih vsebin.“

13 Člen 2 Direktive 2002/21 določa:

„Za namene te direktive:

[…]

(c) ‚elektronska komunikacijska storitev' pomeni storitev, ki se navadno opravlja za plačilo in je v celoti ali pretežno sestavljena iz prenosa signalov po elektronskih komunikacijskih omrežjih ter vključuje telekomunikacijske storitve in storitve prenosa po omrežjih, ki se uporabljajo za radiodifuzijo, izključuje pa storitve, s katerimi se zagotavljajo vsebine ali izvaja redakcijski nadzor nad vsebinami, ki se pošiljajo po elektronskih komunikacijskih omrežjih in z elektronskimi komunikacijskimi storitvami; ne vključuje storitev informacijske družbe, opredeljenih v členu 1 Direktive [98/34], ki niso v celoti ali pretežno sestavljene iz prenosa signalov po elektronskih komunikacijskih omrežjih;

[…]"

Direktiva 2002/58

14 V uvodnih izjavah 2, 6, 7, 11, 22, 26 in 30 Direktive 2002/58 je navedeno:

„(2) Ta direktiva uveljavlja spoštovanje temeljnih pravic in upošteva načela, priznana zlasti z [Listino]. Zlasti pa želi ta direktiva zagotoviti popolno spoštovanje pravic, določenih v členih 7 in 8 navedene listine.

[…]

(6) Internet spreminja tradicionalne tržne strukture, ker ponuja skupno, globalno infrastrukturo za dobavo široke izbire elektronskih komunikacijskih storitev. Javno dostopne elektronske komunikacijske storitve prek interneta odpirajo nove možnosti uporabnikom, pa tudi nova tveganja za njihove osebne podatke in zasebnost.

(7) V primeru javnih komunikacijskih omrežij je treba sprejeti posebne zakone in druge predpise, s katerimi se zavarujejo temeljne pravice in svoboščine fizičnih oseb ter zakoniti interesi pravnih oseb, zlasti v zvezi s čedalje večjo zmogljivostjo samodejnega shranjevanja in obdelave podatkov, ki se nanašajo na naročnike in uporabnike.

[…]

(11) Ta direktiva, tako kot Direktiva [95/46], ne obravnava vprašanj varstva temeljnih pravic in svoboščin, povezanih z dejavnostmi, ki jih ne ureja pravni red [Unije]. Zato ne spreminja obstoječega ravnotežja med posameznikovo pravico do zasebnosti in možnostjo držav članic, da sprejmejo ukrepe iz člena 15(1) te direktive, potrebne za zaščito javne varnosti, obrambe, državne varnosti (vključno z gospodarsko blaginjo države, kadar se dejavnosti nanašajo na zadeve državne varnosti) in izvajanje kazenske zakonodaje. Ta direktiva torej ne vpliva na zmožnost držav članic, da zakonito prestrezajo elektronska sporočila ali da sprejmejo druge ukrepe, če so potrebni iz katerega koli od teh namenov ter v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin[, podpisano v Rimu 4. novembra 1950], kakor jo razlaga Evropsko sodišče za človekove pravice v svojih sodbah. Taki ukrepi morajo biti ustrezni, dosledno sorazmerni z namenom in potrebni v demokratični družbi ter predmet primernih zaščitnih ukrepov v skladu z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin.

[…]

(22) Prepoved shranjevanja sporočil in s tem povezanih podatkov o prometu osebam, ki niso uporabniki ali ki nimajo privolitve uporabnikov, ni namenjena prepovedi vsakega samodejnega, vmesnega in prehodnega shranjevanja teh podatkov, dokler se to dogaja samo zaradi izvedbe prenosa v omrežju elektronskih komunikacij in pod pogojem, da podatki niso shranjeni dlje, kot je to potrebno za prenos in upravljanje prometa in da zaupnost podatkov ostane zagotovljena v času njihovega hranjenja. […]

[…]

(26) Podatki o naročnikih, ki se obdelajo v elektronskih komunikacijskih omrežjih zaradi vzpostavitve povezav in prenosa podatkov, vsebujejo podatke o zasebnem življenju fizičnih oseb in zadevajo pravico do spoštovanja njihove korespondence ali legitimne interese pravnih oseb. Takšni podatki se lahko shranijo le v obsegu, potrebnem za izvedbo storitve, za namen zaračunavanja in plačila medsebojnih povezav ter za določen čas. Vsaka nadaljnja obdelava takih podatkov […] je dovoljena samo takrat, kadar naročnik v to privoli na podlagi točnih in popolnih podatkov, ki jih dobi od ponudnika javno razpoložljivih elektronskih komunikacijskih storitev o vrsti nadaljnje obdelave, ki jo ta namerava izvajati, in o naročnikovi pravici, da ne da privolitve za tako obdelavo ali da jo umakne. Podatke o prometu, uporabljene za trženje komunikacijskih storitev […], je […] treba izbrisati ali napraviti anonimne. […]

[…]

(30) Sistemi za zagotavljanje elektronskih komunikacijskih omrežij in storitev morajo biti zasnovani tako, da omejijo količino potrebnih osebnih podatkov na strogi minimum. […]“

15 Člen 1 Direktive 2002/58, naslovljen „Področje in cilj“, določa:

„1. Ta direktiva določa uskladitev [harmonizacijo] določb držav članic, ki je potrebna za zagotovitev enakovredne ravni varstva temeljnih pravic in svoboščin ter zlasti pravice do zasebnosti in zaupnosti v zvezi z obdelavo osebnih podatkov na področju elektronskih komunikacij in za zagotovitev prostega pretoka takih podatkov ter elektronske komunikacijske opreme in storitev v [Evropski uniji].

2. Določbe te direktive podrobno opredeljujejo in dopolnjujejo Direktivo [95/46] za namene, navedene v odstavku 1. Razen tega predvidevajo varstvo zakonitih interesov naročnikov, ki so pravne osebe.

3. Ta direktiva se ne uporablja za dejavnosti, ki so zunaj obsega [PDEU], kot na primer tiste, zajete v Oddelkih V in VI Pogodbe o Evropski uniji in v vsakem primeru za dejavnosti v zvezi z javno varnostjo, obrambo, državno varnostjo (vključno gospodarsko blaginjo države, kadar se dejavnosti nanašajo na zadeve v zvezi z državno varnostjo) ter dejavnosti države na področju kazenskega prava.“

16 Člen 2 Direktive 2002/58, naslovljen „Opredelitve“, določa:

„Razen če je drugače določeno, se uporabijo opredelitve pojmov iz Direktive [95/46] in Direktive [2002/21].

Uporabijo se tudi naslednje opredelitve pojmov:

(a) ‚uporabnik‘ pomeni vsako fizično osebo, ki uporablja javno razpoložljivo elektronsko komunikacijsko storitev v zasebne ali poslovne namene, pri čemer ni nujno naročena na to storitev;

(b) ‚podatki o prometu' pomenijo katere koli podatke, obdelane za namen prenosa sporočila po elektronskem komunikacijskem omrežju ali zaradi zaračunavanja tega sporočila;

(c) ‚podatki o lokaciji' pomenijo vsakršne podatke, obdelane v elektronskem komunikacijskem omrežju ali v okviru elektronske komunikacijske storitve, ki razkrivajo zemljepisni položaj terminalske opreme uporabnika javno razpoložljive elektronske komunikacijske storitve;

(d) ‚sporočilo' (komunikacija) pomeni vsak podatek, ki se izmenjuje ali prenaša med končnim številom strank s pomočjo javno razpoložljive elektronske komunikacijske storitve. To ne vključuje nobenih podatkov, prenesenih javnosti kot del radiodifuzijske storitve prek elektronskega komunikacijskega omrežja, razen v obsegu, v katerem se da podatek povezati s prepoznavnim naročnikom ali uporabnikom, ki ga prejme;

[…]"

17 Člen 3 Direktive 2002/58, naslovljen „Storitve", določa:

„Ta direktiva se uporablja za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v Skupnosti, vključno z javnimi komunikacijskimi omrežji, ki podpirajo zbiranje podatkov in identifikacijske naprave."

18 Člen 5 Direktive 2002/58, naslovljen „Zaupnost sporočil", določa:

„1. Države članice s svojo nacionalno zakonodajo zagotovijo zaupnost sporočil in s tem povezanih podatkov o prometu, ki se pošiljajo prek javnega komunikacijskega omrežja in javno razpoložljivih elektronskih komunikacijskih storitev. Zlasti prepovejo vsem osebam razen uporabnikom, da poslušajo, prisluškujejo, shranjujejo ali na druge načine prestrezajo ali nadzirajo komunikacije (sporočila) in z njimi povezane podatke o prometu, brez privolitve zadevnih uporabnikov, razen kadar je to zakonsko dovoljeno v skladu s členom 15(1). Ta odstavek ne preprečuje tehničnega shranjevanja, ki je potrebno za prenos sporočila, brez vpliva na načelo zaupnosti.

[…]

3. Države članice zagotovijo, da je shranjevanje podatkov ali pridobivanje dostopa do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika, dovoljeno samo pod pogojem, da je zadevni naročnik ali uporabnik v to privolil po tem, ko je bil jasno in izčrpno obveščen v skladu z Direktivo [95/46], med drugim o namenih obdelave. To ne prepreči nobenega tehničnega shranjevanja ali dostopa izključno za namen opravljanja prenosa sporočila prek elektronskega komunikacijskega omrežja, ali, če je nujno potrebno, da ponudnik zagotovi storitve informacijske družbe, ki jo naročnik ali uporabnik izrecno zahtevata."

19 Člen 6 Direktive 2002/58, naslovljen „Podatki o prometu", določa:

„1. Podatki o prometu, ki se nanašajo na naročnike in uporabnike in ki jih je ponudnik javnega komunikacijskega omrežja ali javno razpoložljive elektronske komunikacijske storitve obdelal in shranil, morajo biti izbrisani ali predelani v anonimne, potem ko niso več potrebni za namen prenosa sporočila, kar ne vpliva na odstavke 2, 3 in 5 tega člena in člena 15(1).

2. Podatki o prometu, potrebni za namene zaračunavanja naročnikom in plačil za medsebojne povezave, se lahko obdelujejo. Taka obdelava je dovoljena samo do poteka obdobja, med katerim se lahko obračun zakonito izpodbija ali sprožijo postopki za pridobitev plačila.

3. Za namen trženja elektronskih komunikacijskih storitev ali zagotovitve storitev z dodano vrednostjo lahko ponudnik javno razpoložljive elektronske komunikacijske storitve obdela podatke iz odstavka 1 v obsegu in trajanju, ki sta potrebna za takšne storitve ali trženje, če naročnik ali uporabnik, na katerega se podatki nanašajo, v to prej privoli. Uporabnikom ali naročnikom je dana možnost, da kadar koli umaknejo privolitev v obdelavo podatkov o prometu.

[…]

5. Obdelava podatkov o prometu mora biti v skladu z odstavki 1, 2, 3 in 4 omejena na osebe, ki delujejo pod nadzorom ponudnikov javnih komunikacijskih omrežij in javno razpoložljivih elektronskih komunikacijskih storitev in ki skrbijo za zaračunavanje ali upravljanje prometa, se odzivajo na povpraševanje porabnikov, odkrivajo prevare, tržijo elektronske komunikacijske storitve ali zagotavljajo storitve z dodano vrednostjo, pri čemer mora biti ta obdelava omejena na to, kar je potrebno za namene takšnih dejavnosti.“

20 Člen 9 te direktive, naslovljen „Podatki o lokaciji razen podatkov o prometu“, v odstavku 1 določa:

„Kadar se podatki o lokaciji, razen podatkov o prometu, ki se nanašajo na uporabnike ali naročnike javnih komunikacijskih omrežij ali javno razpoložljivih elektronskih komunikacijskih storitev, dajo obdelovati, se smejo takšni podatki obdelati šele potem, ko postanejo anonimni ali s privolitvijo uporabnikov ali naročnikov in to v obsegu in trajanju, ki sta potrebna za izvedbo storitve z dodano vrednostjo. Ponudnik storitve mora pred pridobitvijo njihove privolitve obvestiti uporabnike ali naročnike o vrsti podatkov v zvezi z lokacijo, razen podatkov o prometu, ki bodo obdelani, o namenih in trajanju obdelave in ali bodo podatki poslani tretji osebi za namen izvedbe storitve z dodano vrednostjo. […]“

21 Člen 15 navedene direktive, naslovljen „Uporaba nekaterih določb Direktive [95/46]“, določa:

„1. Države članice lahko sprejmejo zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, določenih v členu 5, členu 6, členu 8(1), (2), (3) in (4) ter členu 9 te direktive, kadar takšna omejitev pomeni potreben, primeren in ustrezen [sorazmeren] ukrep znotraj demokratične družbe za zaščito državne [nacionalne] varnosti (to je Državne varnosti), obrambe, javne varnosti in preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih [kaznivih] dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema iz člena 13(1) Direktive [95/46]. V ta namen lahko države članice med drugim sprejmejo zakonske ukrepe, ki določajo zadrževanje podatkov za določeno obdobje, upravičeno iz razlogov iz tega odstavka. Vsi ukrepi iz tega odstavka so v skladu s splošnimi načeli zakonodaje [Unije], vključno s tistimi iz člena 6(1) in (2) Pogodbe o Evropski uniji.

[…]

2. Določbe poglavja III o pravnih sredstvih, odgovornosti in sankcijah Direktive [95/46] se uporabijo v zvezi z nacionalnimi predpisi, sprejetimi v skladu s to direktivo in posameznimi pravicami, izhajajočimi iz te direktive.

[…]“

Uredba št. 2016/679

22 V uvodni izjavi 10 Uredbe št. 2016/679 je navedeno:

„Za zagotovitev dosledne in visoke ravni varstva posameznikov ter odstranitev ovir za prenos osebnih podatkov v Uniji bi morala biti raven varstva pravic in svoboščin posameznikov pri obdelavi osebnih podatkov enaka v vseh državah članicah. V vsej Uniji bi bilo treba zagotoviti dosledno in enotno uporabo pravil za varstvo temeljnih pravic in svoboščin posameznikov pri obdelavi osebnih podatkov. […]“

23 Člen 2 te uredbe določa:

„1. Ta uredba se uporablja za obdelavo osebnih podatkov v celoti ali delno z avtomatiziranimi sredstvi in za drugačno obdelavo kakor z avtomatiziranimi sredstvi za osebne podatke, ki so del zbirke ali so namenjeni oblikovanju dela zbirke.

2. Ta uredba se ne uporablja za obdelavo osebnih podatkov:

(a) v okviru dejavnosti zunaj področja uporabe prava Unije;

(b) s strani držav članic, kadar izvajajo dejavnosti, ki spadajo na področje uporabe poglavja 2 naslova V PEU;

[…]

(d) s strani pristojnih organov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem.

[…]

4. Ta uredba ne posega v uporabo Direktive [2000/31], zlasti v uporabo pravil o odgovornosti posrednih ponudnikov storitev iz členov 12 do 15 navedene direktive.“

24 Člen 4 navedene uredbe določa:

„V tej uredbi:

(1) ‚osebni podatki‘ pomeni katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;

(2) ‚obdelava‘ pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;

[…]“

25 Člen 5 Uredbe št. 2016/679 določa:

„1. Osebni podatki so:

(a) obdelani zakonito, pošteno in na pregleden način v zvezi s posameznikom, na katerega se nanašajo osebni podatki (‚zakonitost, pravičnost in preglednost‘);

(b) zbrani za določene, izrecne in zakonite namene ter se ne smejo nadalje obdelovati na način, ki ni združljiv s temi nameni; nadaljnja obdelava v namene arhiviranja v javnem interesu, v znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene v skladu s členom 89(1) ne velja za nezdružljivo s prvotnimi nameni (‚omejitev namena‘);

(c) ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo (‚najmanjši obseg podatkov‘);

(d) točni in, kadar je to potrebo, posodobljeni; sprejeti je treba vse razumne ukrepe za zagotovitev, da se netočni osebni podatki brez odlašanja izbrišejo ali popravijo ob upoštevanju namenov, za katere se obdelujejo (‚točnost‘);

(e) hranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo; osebni podatki se lahko shranjujejo za daljše obdobje, če bodo obdelani zgolj za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene v skladu s členom 89(1), pri čemer je treba izvajati ustrezne tehnične in organizacijske ukrepe iz te uredbe, da se zaščitijo pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki (‚omejitev shranjevanja‘);

(f) obdelujejo se na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo z ustreznimi tehničnimi ali organizacijskimi ukrepi (‚celovitost in zaupnost‘).

[…]“

26 Člen 6 te uredbe določa:

„1. Obdelava je zakonita le in kolikor je izpolnjen vsaj eden od naslednjih pogojev:

[…]

(c) obdelava je potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca;

[…]

3. Podlaga za obdelavo iz točk (c) in (e) odstavka 1 je določena v skladu s:

(a) pravom Unije; ali

(b) pravom države članice, ki velja za upravljavca.

Namen obdelave se določi v navedeni pravni podlagi […]. Navedena pravna podlaga lahko vključuje posebne določbe, s katerimi se prilagodi uporaba pravil iz te uredbe, med drugim: splošne pogoje, ki urejajo zakonitost obdelave podatkov s strani upravljavca; vrste podatkov, ki se obdelujejo; zadevne posameznike, na katere se nanašajo osebni podatki; subjekte, katerim se osebni podatki lahko razkrijejo, in namene, za katere se lahko razkrijejo; omejitve namena; obdobja hrambe; ter dejanja

obdelave in postopke obdelave, vključno z ukrepi za zagotovitev zakonite in poštene obdelave, kot tiste za druge posebne primere obdelave iz poglavja IX. Pravo Unije ali pravo države članice izpolnjuje cilj javnega interesa in je sorazmerno z zakonitim ciljem, za katerega si prizadeva.

[…]“

27 Člen 23 navedene uredbe določa:

„1. Pravo Unije ali pravo države članice, ki velja za upravljavca ali obdelovalca podatkov, lahko z zakonodajnim ukrepom omeji obseg obveznosti in pravic iz členov 12 do 22 in člena 34, pa tudi člena 5, kolikor njegove določbe ustrezajo pravicam in obveznostim iz členov 12 do 22, če taka omejitev spoštuje bistvo temeljnih pravic in svoboščin ter je potreben in sorazmeren ukrep v demokratični družbi za zagotavljanje:

(a) državne varnosti;

(b) obrambe;

(c) javne varnosti;

(d) preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem;

(e) drugih pomembnih ciljev v splošnem javnem interesu Unije ali države članice, zlasti pomembnega gospodarskega ali finančnega interesa Unije ali države članice, vključno z denarnimi, proračunskimi in davčnimi zadevami, javnim zdravjem in socialno varnostjo;

(f) varstva neodvisnosti sodstva in sodnega postopka;

(g) preprečevanja, preiskovanja, odkrivanja in pregona kršitev etike v zakonsko urejenih poklicih;

(h) spremljanja, pregledovanja ali urejanja, povezanega, lahko tudi zgolj občasno, z izvajanjem javne oblasti v primerih iz točk (a) do (e) in (g);

(i) varstva posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih;

(j) uveljavljanja civilnopravnih zahtevkov.

2. Zlasti vsak zakonodajni ukrep iz odstavka 1 vsebuje posebne določbe vsaj, kjer je ustrezno, glede:

(a) namenov obdelave ali vrst obdelave;

(b) vrst osebnih podatkov;

(c) obsega uvedenih omejitev;

(d) zaščitnih ukrepov za preprečitev zlorab ali nezakonitega dostopa ali prenosa;

(e) natančnejše ureditve upravljavca ali vrst upravljavcev;

(f) obdobij hrambe in veljavnih zaščitnih ukrepov, pri čemer se upoštevajo narava, obseg in nameni obdelave ali vrste obdelave;

(g) tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, ter

(h) pravice posameznikov, na katere se nanašajo osebni podatki, da so obveščeni o omejitvi, razen če bi to posegalo v namen omejitve.“

28 Člen 79(1) navedene uredbe določa:

„Brez poseganja v katero koli razpoložljivo upravno ali izvensodno sredstvo, vključno s pravico do vložitve pritožbe pri nadzornem organu na podlagi člena 77, ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico do učinkovitega pravnega sredstva, kadar meni, da so bile njegove pravice iz te uredbe kršene zaradi obdelave njegovih osebnih podatkov, ki ni bila v skladu s to uredbo.“

29 Člen 94 Uredbe št. 2016/679 določa:

„1. Direktiva [95/46] se razveljavi z učinkom od 25. maja 2018.

2. Sklicevanja na razveljavljeno direktivo se štejejo kot sklicevanja na to uredbo. Sklicevanja na Delovno skupino za varstvo posameznikov pri obdelavi osebnih podatkov, ustanovljeno s členom 29 Direktive [95/46], se štejejo kot sklicevanja na Evropski odbor za varstvo podatkov, ustanovljen s to uredbo.“

30 Člen 95 te uredbe določa:

„Ta uredba ne uvaja dodatnih obveznosti za fizične ali pravne osebe v zvezi z obdelavo, povezano z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v Uniji v povezavi z zadevami, za katere veljajo posebne obveznosti z istim ciljem iz Direktive [2002/58].“

Francosko pravo

Code de la sécurité intérieure (zakonik o notranji varnosti)

31 Knjiga VIII zakonodajnega dela zakonika o notranji varnosti (v nadaljevanju: CSI) v členih od L. 801-1 do L. 898-1 določa pravila o obveščevalni dejavnosti.

32 Člen L. 811-3 CSI določa:

„Posebne obveščevalne službe lahko zgolj za izvajanje svojih nalog uporabljajo metode, navedene v naslovu V te knjige, za zbiranje informacij v zvezi z varnostjo in spodbujanjem naslednjih temeljnih državnih interesov:

1. državna neodvisnost, ozemeljska celovitost in nacionalna obramba;

2. pomembni interesi zunanje politike, uresničevanje evropskih in mednarodnih zavez Francije ter preprečevanje kakršne koli oblike tujega vmešavanja;

3. pomembni gospodarski, industrijski in znanstveni interesi Francije;

4. preprečevanje terorizma;

5. preprečevanje:
   (a) posegov v republikansko obliko institucij;

(b) dejanj, katerih namen je ohranjanje ali ponovno izoblikovanje skupin, razpuščenih v skladu s členom L. 212-1;
(c) kolektivnega nasilja, ki lahko resno ogrozi javni mir;

6. preprečevanje organiziranega kriminala in prestopništva;

7. preprečevanje širjenja orožja za množično uničevanje.“

33 Člen L. 811-4 CSI določa:

„Z odlokom Conseil d'État (državni svet), sprejetim po mnenju Commission nationale de contrôle des techniques de renseignement (nacionalna komisija za nadzor nad obveščevalnimi metodami), se imenujejo službe, ki niso posebne obveščevalne službe ter spadajo v pristojnost ministrov za obrambo, notranje zadeve in pravosodje ter ministrov, pristojnih za gospodarstvo, proračun in carino, ki jim je dovoljena uporaba metod, navedenih v naslovu V te knjige, pod pogoji, določenimi v isti knjigi. V tem odloku se za vsako službo navedejo cilji iz člena L. 811-3 in metode, za katere je mogoče dati dovoljenje.“

34 Člen L. 821-1, prvi odstavek, CSI določa:

„Za izvajanje metod zbiranja informacij iz poglavij od I do IV naslova V te knjige na nacionalnem ozemlju je potrebno predhodno dovoljenje predsednika vlade, izdano po mnenju nacionalne komisije za nadzor nad obveščevalnimi metodami.“

35 Člen L. 821-2 CSI določa:

„Dovoljenje iz člena L. 821-1 se izda na pisno in obrazloženo zahtevo ministra za obrambo, ministra za notranje zadeve, ministra za pravosodje ali ministrov, pristojnih za gospodarstvo, proračun ali carine. Vsak od ministrov lahko to pristojnost posamično prenese zgolj na neposredne sodelavce, pooblaščene za vpogled v tajne podatke s področja nacionalne obrambe.

V zahtevi se navedejo:

1. metoda ali metode, ki jih je treba izvesti;

2. služba, za katero je predložena;

3. zastavljeni namen ali nameni;

4. razlog ali razlogi za ukrepe;

5. rok veljavnosti dovoljenja;

6. oseba(-e), kraj(i) ali vozila, na katere se nanaša.

Za uporabo točke 6 je mogoče osebe, katerih identiteta ni znana, opredeliti z identifikatorji ali statusom, kraje ali vozila pa je mogoče opredeliti s sklicevanjem na osebe, na katere se zahteva nanaša.

[…]“

36 Člen L. 821-3, prvi odstavek, CSI določa:

„Zahteva se predloži predsedniku ali – če to ni mogoče – enemu od članov nacionalne komisije za nadzor nad obveščevalnimi metodami, navedenih v točkah 2 in 3 člena L. 831-1, ki predsedniku vlade v 48 urah poda mnenje. Če je zahtevo preučila komisija v ožji ali plenarni sestavi, je predsednik vlade o tem nemudoma obveščen, mnenje pa je izdano v 72 urah.“

37 Člen L. 821-4 CSI določa:

„Dovoljenje za izvedbo metod, navedenih v poglavjih od I do IV naslova V te knjige, izda predsednik vlade za največ štiri mesece. […] Dovoljenje vsebuje obrazložitve in navedbe, določene v točkah od 1 do 6 člena L. 821-2. Vsako dovoljenje je mogoče podaljšati pod enakimi pogoji, kot so določeni v tem poglavju.

Če je dovoljenje izdano po odklonilnem mnenju nacionalne komisije za nadzor nad obveščevalnimi metodami, so v njem navedenih razlogi, iz katerih to mnenje ni bilo upoštevano.

[…]“

38 Člen L. 833-4 CSI iz poglavja III tega naslova določa:

„Komisija na svojo pobudo ali na podlagi pritožbe kogar koli, ki želi preveriti, da se v zvezi z njim nobena obveščevalna metoda ne izvaja nezakonito, opravi nadzor nad navedeno metodo ali metodami, da tako preveri, ali se izvajajo ob upoštevanju te knjige. Pritožnika obvesti o tem, da je opravila potrebna preverjanja, pri čemer niti ne potrdi niti ne ovrže njihovega izvajanja.“

39 Člen L. 841-1, prvi in drugi odstavek, CSI določa:

„Conseil d'État (državni svet) je ob upoštevanju posebnih določb člena L. 854-9 tega zakonika pristojen za to, da pod pogoji, določenimi v poglavju IIIa naslova VII knjige VII code de justice administrative (zakonik o upravnem sodstvu), obravnava tožbe v zvezi z izvajanjem obveščevalnih metod iz naslova V te knjige.

Tožbo pri njem lahko vloži:

1. vsak, ki želi preveriti, da se v zvezi z njim nobena obveščevalna metoda ne izvaja nezakonito, in ki predloži dokaz o predhodni izvedbi postopka iz člena L. 833-4;

2. nacionalna komisija za nadzor nad obveščevalnimi metodami pod pogoji, določenimi v členu L. 833-8.“

40 Naslov V knjige VIII zakonodajnega dela CSI, ki se nanaša na „metode zbiranja informacij, za katere je potrebno dovoljenje“, med drugim vsebuje poglavje I, naslovljeno „Dostopi upravnih organov do podatkov o povezavi“, ki vsebuje člene od L. 851-1 do L. 851-7 CSI.

41 Člen L. 851-1 CSI določa:

„Pod pogoji, določenimi v poglavju I naslova II te knjige, je mogoče odobriti, da se od operaterjev elektronskih komunikacij, oseb, navedenih v členu L. 34-1 [CPCE], in oseb, navedenih v členu 6(I), točki 1 in 2, loi no 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (zakon št. 2004-575 z dne 21. junija 2004 o zaupanju v digitalno gospodarstvo) [(JORF z dne 22. junija 2004, str. 11168)], zbirajo informacije ali dokumenti, ki so bili obdelani ali hranjeni v okviru njihovih omrežij ali elektronskih komunikacijskih storitev, vključno s tehničnimi podatki, ki se nanašajo na identifikacijo naročniških številk ali številk za povezavo z elektronskimi komunikacijskimi storitvami,

popis naročniških številk ali številk za povezavo zadevne osebe, lokalizacijo uporabljene terminalske opreme ter komunikacije naročnika v zvezi s seznamom številk odhodnih in dohodnih klicev, trajanjem in datumom komunikacij.

Z odstopanjem od člena L. 821-2 posamično imenovani in pooblaščeni uslužbenci obveščevalnih služb iz členov L. 811-2 in L. 811-4 pisne in obrazložene zahteve v zvezi s tehničnimi podatki, ki se nanašajo na identifikacijo naročniških številk ali številk za povezavo z elektronskimi komunikacijskimi storitvami oziroma na popis vseh naročniških številk ali številk za povezavo zadevne osebe, posredujejo neposredno nacionalni komisiji za nadzor nad obveščevalnimi metodami. Komisija izda svoje mnenje pod pogoji, določenimi v členu L. 821-3.

Služba predsednika vlade je pristojna za zbiranje informacij ali dokumentov pri operaterjih in osebah iz prvega odstavka tega člena. Nacionalna komisija za nadzor nad obveščevalnimi metodami ima stalen, popoln, neposreden in takojšen dostop do zbranih informacij ali dokumentov.

Pogoji za uporabo tega člena se določijo z odlokom Conseil d'État (državni svet), sprejetim po mnenju Commission nationale de l'informatique et des libertés (nacionalna komisija za informatiko in svoboščine) in nacionalne komisije za nadzor nad obveščevalnimi metodami."

42 Člen L. 851-2 CSI določa:

„I. – Pod pogoji, določenimi v poglavju I naslova II te knjige, in zgolj za potrebe preprečevanja terorizma je mogoče posamično dovoliti zbiranje v realnem času – na omrežjih operaterjev in oseb, navedenih v členu L. 851-1 – informacij ali dokumentov, prav tako navedenih v členu L. 851-1, v zvezi s predhodno identificirano osebo, ki bi bila lahko povezana z grožnjo. Če obstajajo resni razlogi za sklepanje, da bi lahko ena ali več oseb, ki pripadajo okolju osebe, na katero se nanaša dovoljenje, zagotovile informacije za uresničitev cilja, s katerim je dovoljenje utemeljeno, je mogoče tako dovoljenje posamično izdati za vsako od teh oseb.

Ia. Največje število hkrati veljavnih dovoljenj, izdanih v skladu s tem členom, določi predsednik vlade po mnenju nacionalne komisije za nadzor nad obveščevalnimi metodami. Ta komisija je obveščena o odločitvi, s katero se določi ta kvota, in porazdelitvi te kvote med ministri, navedenimi v prvem odstavku člena L. 821-2, ter številu izdanih dovoljenj za prestrezanje.

[…]"

43 Člen L. 851-3 CSI določa:

„I. – Pod pogoji, določenimi v poglavju I naslova II te knjige, in zgolj za potrebe preprečevanja terorizma se lahko operaterjem in osebam, navedenim v členu L. 851-1, naloži obveznost, da na svojih omrežjih izvajajo avtomatizirane obdelave podatkov na podlagi parametrov, navedenih v dovoljenju, pri čemer je cilj teh obdelav odkrivanje povezav, ki lahko pomenijo teroristično grožnjo.

Za te avtomatizirane obdelave se uporabljajo izključno informacije ali dokumenti, navedeni v členu L. 851-1, ne da bi se zbirali še drugi podatki poleg tistih, ki se ujemajo z načrtovanimi parametri teh obdelav, pri čemer se ne omogoči identifikacija oseb, na katere se informacije ali dokumenti nanašajo.

Ob upoštevanju načela sorazmernosti je v dovoljenju predsednika vlade natančno navedeno tehnično področje izvajanja teh obdelav.

II. – Nacionalna komisija za nadzor nad obveščevalnimi metodami izda mnenje o zahtevi za dovoljenje v zvezi z avtomatiziranimi obdelavami in o izbranih parametrih odkrivanja. Razpolaga s stalnim, popolnim in neposrednim dostopom do teh obdelav ter zbranih informacij in podatkov. Obveščena je o kakršni koli spremembi obdelav in parametrov, pri čemer lahko poda priporočila.

Prvo dovoljenje za izvedbo avtomatiziranih obdelav, določeno v odstavku I tega člena, se izda za dva meseca. Dovoljenje je mogoče podaljšati pod pogoji glede trajanja, določenimi v poglavju I naslova II te knjige. Zahteva za podaljšanje vsebuje navedbo števila identifikatorjev, odkritih z avtomatizirano obdelavo, in analizo ustreznosti teh opozoril.

III. – Za materialna dejanja, ki jih operaterji in osebe, navedene v členu L. 851-1, opravijo za to izvedbo, veljajo pogoji, določeni v členu L. 871-6.

IV. – Če se pri obdelavah iz odstavka I tega člena odkrijejo podatki, ki bi lahko kazali na obstoj teroristične grožnje, lahko predsednik vlade ali ena od oseb, ki jih je ta pooblastil, po tem, ko nacionalna komisija za nadzor nad obveščevalnimi metodami poda mnenje pod pogoji, določenimi v odstavku I naslova II te knjige, dovoli identifikacijo zadevne osebe ali oseb in zbiranje s tem povezanih podatkov. Ti podatki se uporabijo v 60 dneh po tem zbiranju in so po izteku tega roka uničeni, razen v primeru resnih elementov, ki potrjujejo obstoj teroristične grožnje v zvezi z eno ali več zadevnimi osebami.

[…]“

44 Člen L. 851-4 CSI določa:

„Pod pogoji, določenimi v poglavju I naslova II te knjige, je mogoče tehnične podatke, ki se nanašajo na lokacijo uporabljene terminalske opreme, navedene v členu L. 851-1, zbirati iz omrežja na zahtevo, pri čemer jih operaterji v realnem času posredujejo službi predsednika vlade.“

45 Člen R. 851-5 CSI, ki je v delu tega zakonika, ki vsebuje izvedbene predpise, določa:

„I. – Informacije ali dokumenti, navedeni v členu L. 851-1 – z izjemo vsebine izmenjane korespondence ali pregledanih informacij – so:

1. tisti, navedeni v členih R. 10-13 in R. 10-14 [CPCE] ter členu 1 odloka [št. 2011-219];

2. tehnični podatki, ki niso tisti, navedeni v točki 1, in ki:

(a) omogočajo lokalizacijo terminalske opreme;

(b) se nanašajo na dostop terminalske opreme do omrežij ali do javnih spletnih komunikacijskih storitev;

(c) se nanašajo na prenos elektronskih komunikacij po omrežjih;

(d) se nanašajo na identifikacijo in avtentikacijo uporabnika, povezave, omrežja ali javne spletne komunikacijske storitve;

(e) se nanašajo na značilnosti terminalske opreme in konfiguracijske podatke njene programske opreme.

II. – V skladu s členom L. 851-1 se lahko zbirajo samo informacije in dokumenti, navedeni v točki 1 odstavka I. To zbiranje se opravlja z zamikom.

Informacije, navedene v točki 2 odstavka I, je mogoče zbirati zgolj na podlagi členov L. 851-2 in L. 851-3, pod pogoji in z omejitvami, določenimi v teh členih, ter ob pridržku uporabe člena R. 851-9.“

CPCE

46 Člen L. 34-1 CPCE določa:

„I. – Ta člen se uporablja za obdelavo osebnih podatkov pri opravljanju elektronskih komunikacijskih storitev za javnost; uporablja se zlasti za omrežja, ki podpirajo naprave za zbiranje podatkov in identifikacijo.

II. – Operaterji elektronskih komunikacij in zlasti osebe, katerih dejavnost je zagotavljanje dostopa do javnih spletnih komunikacijskih storitev, izbrišejo ali anonimizirajo vse podatke o prometu, s pridržkom določb odstavkov III, IV, V in VI.

Osebe, ki zagotavljajo javne elektronske komunikacijske storitve, ob upoštevanju določb iz prejšnjega pododstavka vzpostavijo interne postopke, ki omogočijo odgovarjanje na zahteve pristojnih organov.

Osebe, ki v okviru glavne ali pomožne poklicne dejavnosti zagotavljajo javno povezavo, ki omogoča spletno komunikacijo prek dostopa do omrežja, četudi to povezavo zagotavljajo brezplačno, morajo spoštovati določbe, ki se na podlagi tega člena uporabljajo za operaterje elektronskih komunikacij.

III. – Za odkrivanje, preiskovanje in pregon kaznivih dejanj ali kršitev iz člena L. 336-3 code de la propriété intellectuelle (zakonik o intelektualni lastnini) ali za potrebe preventive v zvezi z ogrožanjem sistemov za avtomatizirano obdelavo podatkov, ki so določeni in sankcionirani v členih od 323-1 do 323-3-1 code pénal (kazenski zakonik), ter izključno za morebitne potrebe zagotavljanja potrebnih informacij pravosodnemu organu, visoki oblasti iz člena 331-12 zakonika o intelektualni lastnini ali nacionalnemu organu za varnost informacijskih sistemov iz člena L. 2321-1 code de la défense (zakonik o obrambi) se lahko dejanja izbrisa ali anonimiziranja nekaterih kategorij tehničnih podatkov odložijo največ za eno leto. Z odlokom Conseil d'État (državni svet), sprejetim po mnenju nacionalne komisije za informatiko in svoboščine, se v mejah, opredeljenih v odstavku VI, določijo te kategorije podatkov in trajanje njihovega hranjenja glede na dejavnosti operaterjev in naravo komunikacij ter podrobna pravila o nadomestilu za morebitne dodatne stroške, ki jih je mogoče opredeliti in ki posebej zadevajo storitve, ki jih operaterji na zahtevo države opravijo v zvezi s tem.

[…]

VI. Podatki, ki se hranijo in obdelujejo pod pogoji, določenimi v odstavkih III, IV in V, se nanašajo izključno na identifikacijo uporabnikov storitev, ki jih opravljajo operaterji, tehnične značilnosti komunikacij, ki jih ti operaterji zagotavljajo, in lokacijo terminalske opreme.

V nobenem primeru se ne morejo nanašati na vsebino izmenjane korespondence ali informacije, ki so bile v kakršni koli obliki pregledane v okviru teh komunikacij.

Hramba in obdelava teh podatkov se izvajata ob spoštovanju določb zakona št. 78-17 z dne 6. januarja 1978 o informatiki, datotekah in svoboščinah.

Operaterji sprejmejo vse ukrepe za to, da se prepreči uporaba teh podatkov za namene, ki se razlikujejo od teh, določenih v tem členu.“

47 Člen R. 10-13 CPCE določa:

„I. – Na podlagi odstavka III člena L. 34-1 operaterji elektronskih komunikacij zaradi preiskovanja, ugotavljanja in pregona kaznivih dejanj hranijo:

(a) podatke, ki omogočajo identifikacijo uporabnika;

(b) podatke o uporabljeni komunikacijski terminalski opremi;

(c) tehnične značilnosti ter datum, čas in trajanje vsake komunikacije;

(d) podatke o zahtevanih ali uporabljenih dodatnih storitvah in izvajalcih teh storitev;

(e) podatke, na podlagi katerih je mogoče identificirati namembnega(-e) prejemnika(-e) komunikacije.

II. – Operater pri dejavnosti telefonije hrani podatke iz odstavka II in tudi podatke, ki omogočajo določitev izvora in lokacije komunikacije.

III. – Podatki iz tega člena se hranijo eno leto od datuma svoje shranitve.

IV. – Opredeljivi posebni dodatni stroški, ki jih nosijo operaterji, ki jim pravosodni organi naložijo predložitev podatkov, ki spadajo v kategorije, navedene v tem členu, se povrnejo v skladu s pravili, določenimi v členu R. 213-1 code de procédure pénale (zakonik o kazenskem postopku).“

48 Člen R. 10-14 CPCE določa:

„I. – V skladu z odstavkom IV člena L. 34-1 je operaterjem elektronskih komunikacij za potrebe njihovih transakcij zaračunavanja in plačila dovoljeno hraniti tehnične podatke, ki omogočajo identifikacijo uporabnika, in tehnične podatke iz točk (b), (c) in (d) odstavka I člena R. 10-13.

II. – Operaterji lahko za dejavnosti telefonije poleg podatkov, navedenih v odstavku I, hranijo tehnične podatke, ki se nanašajo na lokacijo komunikacije in identifikacijo prejemnika(-ov) komunikacije, ter podatke, ki omogočajo zaračunavanje.

III. – Podatke iz odstavkov I in II tega člena je mogoče hraniti le, če so potrebni za zaračunavanje in plačilo opravljenih storitev. Njihova hramba mora biti omejena na čas, nujno potreben v ta namen, in ne sme trajati več kot eno leto.

IV. Operaterji lahko zaradi zagotavljanja varnosti omrežij in naprav največ tri mesece hranijo:

(a) podatke, na podlagi katerih je mogoče identificirati izvor komunikacije;

(c) tehnične značilnosti ter datum, čas in trajanje vsake komunikacije;

(c) podatke, na podlagi katerih je mogoče identificirati prejemnika(-e) komunikacije;

(d) podatke o zahtevanih ali uporabljenih dodatnih storitvah in izvajalcih teh storitev.“

Zakon št. 2004-575 z dne 21. junija 2004 o zaupanju v digitalno gospodarstvo

49 Člen 6 Loi n° 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique (zakon št. 2004-575 z dne 21. junija 2004 o zaupanju v digitalno gospodarstvo) (JORF z dne 22. junija 2004, str. 11168, v nadaljevanju: LCEN) določa:

„I. – 1. Osebe, katerih dejavnost je ponujanje dostopa do javnih spletnih komunikacijskih storitev, svoje naročnike obvestijo o obstoju tehničnih sredstev, ki omogočajo omejitev dostopa do nekaterih storitev ali njihovo izbiro, in jim ponudijo vsaj eno od teh sredstev.

[…]

2. Zoper fizične ali pravne osebe, ki za dostop javnosti prek javnih spletnih komunikacijskih storitev zagotavljajo, četudi brezplačno, hrambo vsakršnih signalov, pisnega in slikovnega gradiva, zvokov ali sporočil, ki so jih zagotovili prejemniki teh storitev, ni mogoče uveljavljati civilne odgovornosti zaradi dejavnosti ali informacij, shranjenih na zahtevo prejemnika teh storitev, če navedene osebe niso bile dejansko seznanjene z njihovo nezakonitostjo ali z dejstvi in okoliščinami, iz katerih ta nezakonitost izhaja, oziroma če so se, takoj ko so se s tem seznanile, hitro odzvale in te podatke umaknile ali onemogočile dostop do njih.

[…]

II. – Osebe iz točk 1 in 2 odstavka I imajo in hranijo podatke, ki omogočajo identifikacijo kogar koli, ki je pripomogel k ustvarjanju vsebine ali ene od vsebin storitev, ki jih ponujajo.

Osebam, ki urejajo eno od javnih spletnih komunikacijskih storitev, zagotovijo tehnična sredstva, ki jim omogočajo izpolnjevanje pogojev glede identifikacije, določene v odstavku III.

Pravosodni organ lahko od ponudnikov iz točk 1 in 2 odstavka I zahteva predložitev podatkov, navedenih v prvem odstavku.

Za obdelavo teh podatkov se uporabljajo določbe členov 226-17, 226-21 in 226-22 code pénal (kazenski zakonik).

Z odlokom Conseil d'État (državni svet), sprejetim po mnenju nacionalne komisije za informatiko in svoboščine, se opredelijo podatki iz prvega pododstavka ter določijo trajanje in podrobna pravila o njihovi hrambi.

[…]"

Odlok št. 2011-219

50 Poglavje I odloka št. 2011–219, ki je bil sprejet na podlagi člena 6(II), zadnji odstavek, LCEN, vsebuje člene od 1 do 4 tega odloka.

51 Člen 1 odloka št. 2011-219 določa:

„Podatki iz člena 6(II) [LCEN], ki jih morajo hraniti osebe v skladu s to določbo, so:

1. za osebe iz točke 1 odstavka I istega člena in za vsako povezavo njihovih naročnikov:

(a) identifikator povezave;

(b) identifikator, ki ga te osebe dodelijo naročniku;

(c) identifikator terminala, uporabljenega za povezavo, če imajo dostop do njega;

(d) datum in čas začetka in konca povezave;

(e) značilnosti naročnikove linije;

2. za osebe iz točke 2 odstavka I istega člena in za vsako dejanje ustvarjanja:

(a) identifikator povezave, s katero je bila komunikacija začeta;

(b) identifikator, ki ga informacijski sistem dodeli vsebini, ki je predmet dejanja;

(c) vrste protokolov, uporabljenih za povezavo s storitvijo in za prenos vsebin;

(d) narava dejanja;

(e) datum in ura dejanja;

(f) identifikator, ki ga je uporabil izvajalec dejanja, če ga je ta zagotovil;

3. za osebe iz točk 1 in 2 odstavka I istega člena informacije, ki jih uporabnik predloži ob sklenitvi pogodbe ali odprtju računa:

(a) identifikator povezave ob ustvaritvi računa;

(b) ime in priimek ali firma;

(c) povezani poštni naslovi;

(d) uporabljeni psevdonimi;

(e) naslovi povezane elektronske pošte ali povezanega računa;

(f) telefonske številke;

(g) posodobljeno geslo in podatki, ki omogočajo njegovo preverjanje ali spremembo;

4. za osebe iz točk 1 in 2 odstavka I istega člena, ko je sklenitev pogodbe ali odprtje računa odplačno, spodaj navedene informacije o plačilu za vsako plačilno transakcijo:

(a) vrsta uporabljenega plačila;

(b) referenca plačila;

(c) znesek;

(d) datum in ura transakcije.

Podatki iz točk 3 in 4 se lahko hranijo le v obsegu, v kakršnem jih osebe običajno zbirajo.“

52 Člen 2 tega odloka določa:

„Prispevek k ustvarjanju vsebine vključuje dejanja, ki se nanašajo na:

(a) začetna ustvarjanja vsebin;

(b) spremembe vsebin in podatkov, povezanih z vsebinami;

(c) odstranitve vsebin.“

53 Člen 3 tega odloka določa:

„Podatki iz člena 1 se hranijo eno leto:

(a) kar zadeva podatke iz točk 1 in 2, od datuma, ko so bile vsebine ustvarjene, za vsako dejanje, ki prispeva k ustvarjanju vsebine, kot je opredeljeno v členu 2;

(b) kar zadeva podatke iz točke 3, od datuma prenehanja pogodbe ali zaprtja računa;

(c) kar zadeva podatke iz točke 4, od datuma izdaje računa ali plačilne transakcije za vsak račun ali plačilno transakcijo.“

Belgijsko pravo

54 Z zakonom z dne 29. maja 2016 so bili med drugim spremenjeni loi du 13 juin 2005 relative aux communications électroniques (zakon z dne 13. junija 2005 o elektronskih komunikacijah) (Moniteur belge z dne 20. junija 2005, str. 28070, v nadaljevanju: zakon z dne 13. junija 2005), code d'instruction criminelle (zakonik o kazenskem postopku) in loi du 30 novembre 1998 organique des services de renseignement et de sécurité (sistemski zakon z dne 30. novembra 1998 o obveščevalnih in varnostnih službah) (Moniteur belge z dne 18. decembra 1998, str. 40312, v nadaljevanju: zakon z dne 30. novembra 1998).

55 Člen 126 zakona z dne 13. junija 2005, v različici, ki izhaja iz zakona z dne 29. maja 2016, določa:

„1. Brez poseganja v loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (zakon z dne 8. decembra 1992 o varstvu zasebnega življenja pri obdelavi osebnih podatkov) ponudniki, ki javnosti ponujajo storitve telefonije, tudi prek interneta, dostop do interneta in elektronsko pošto prek interneta, operaterji, ki ponujajo javna omrežja elektronskih komunikacij, ter operaterji, ki ponujajo le kakšno od teh storitev, hranijo podatke iz odstavka 3, ki jih ustvarijo ali obdelajo v okviru zagotavljanja teh komunikacijskih storitev.

Ta člen se ne nanaša na vsebino komunikacij.

Obveznost hrambe podatkov iz odstavka 3 velja tudi za neuspešne klice, če te podatke v okviru zagotavljanja zadevnih komunikacijskih storitev:

(1) kar zadeva podatke s področja telefonije, ustvarijo ali obdelajo operaterji javno dostopnih elektronskih komunikacijskih storitev ali javnega omrežja elektronskih komunikacij, ali

(2) kar zadeva internetne podatke, beležijo ti ponudniki.

2. Za namene in pod pogoji, naštetimi spodaj, lahko le naslednji organi zahtevajo pridobitev podatkov, ki se hranijo na podlagi tega člena, od ponudnikov in operaterjev iz odstavka 1, prvi pododstavek:

(1) pravosodni organi za namene odkrivanja, preiskovanja in pregona kršitev, za izvrševanje ukrepov iz členov 46a in 88a zakonika o kazenskem postopku in pod pogoji, navedenimi v teh členih;

(2) obveščevalne in varnostne službe, ki zaradi opravljanja obveščevalne dejavnosti uporabljajo metode zbiranja podatkov, določene v členih 16/2, 18/7 in 18/8 sistemskega zakona z dne 30. novembra 1998 o obveščevalnih in varnostnih službah, pod pogoji, določenimi s tem zakonom;

(3) kriminalisti [Institut belge des services postaux et des télécommunications (belgijski inštitut za poštne in telekomunikacijske storitve)] za namene odkrivanja, preiskovanja in pregona kršitev členov 114 in 124 ter tega člena;

(4) urgentne službe, ki zagotavljajo pomoč na kraju samem, kadar po nujnem klicu od zadevnega ponudnika ali operaterja ne dobijo podatkov za identifikacijo klicatelja na podlagi podatkovne zbirke iz člena 107(2), tretji pododstavek, ali dobijo nepopolne ali nepravilne podatke. Zahtevajo se lahko le podatki za identifikacijo klicatelja, in to najkasneje 24 ur po klicu;

(5) kriminalisti Cellule des personnes disparues de la Police Fédérale (oddelek zvezne policije za pogrešane osebe), kadar pomagajo osebi, ki je v nevarnosti, kadar iščejo osebe, katerih izginotje vzbuja skrb, ali kadar obstajajo sumi ali resni indici, da je telesna celovitost pogrešane osebe v neposredni nevarnosti. Od zadevnega operaterja ali ponudnika se prek službe policije, ki jo določi kralj, lahko zahtevajo le podatki iz odstavka 3, prvi in drugi pododstavek, ki se nanašajo na pogrešano osebo, za zadnjih 48 ur pred vložitvijo zahteve za posredovanje podatkov;

(6) Service de médiation pour les télécommunications (služba za mediacijo za telekomunikacije) z namenom identifikacije osebe, ki je zlorabila omrežje ali storitev elektronskih komunikacij, v skladu s pogoji iz člena 43a(3), točka 7, loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (zakon z dne 21. marca 1991 o reformi nekaterih javnih gospodarskih družb). Zahtevajo se lahko le podatki za identifikacijo.

Ponudniki in operaterji iz odstavka 1, prvi pododstavek, zagotovijo, da so podatki iz odstavka 3 neomejeno dostopni iz Belgije ter da se lahko ti podatki in vse druge potrebne informacije v zvezi s temi podatki posredujejo nemudoma in le organom iz tega odstavka.

Ponudniki in operaterji iz odstavka 1, prvi pododstavek, podatkov, ki se hranijo na podlagi odstavka 3, ne morejo uporabiti za druge namene, razen če z zakonom ni določeno drugače.

3. Podatki za identifikacijo uporabnika ali naročnika in komunikacijskih sredstev, razen podatkov, ki so izrecno navedeni v drugem in tretjem pododstavku, se hranijo 12 mesecev od dne, ko je komunikacija prek uporabljene storitve zadnjič mogoča.

Podatki v zvezi z dostopom in povezavo terminalske opreme z omrežjem in s storitvijo ter o lokaciji te opreme, vključno z omrežno priključno točko, se hranijo 12 mesecev od datuma komunikacije.

Podatki o komunikaciji, razen vsebine, vključno z virom in ciljem teh podatkov, se hranijo 12 mesecev od datuma komunikacije.

Kralj z odlokom, ki ga obravnava svet ministrov na predlog ministra za pravosodje in ministra[, pristojnega za elektronske komunikacije,] na podlagi mnenja Commission de la protection de la vie privée (komisija za varstvo zasebnega življenja, Belgija) in inštituta določi podatke, ki jih je treba hraniti, za vsako od kategorij, naštetih v prvem, drugem in tretjem pododstavku, in zahteve, ki jih morajo ti podatki izpolnjevati.

[…]“

Spori o glavni stvari in vprašanja za predhodno odločanje

Zadeva C-511/18

56 Organizacije Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs in Igwan.net so pri Conseil d'État (državni svet, Francija) 30. novembra 2015 in 16. marca 2016 vložile tožbe, ki so bile združene v postopku v glavni stvari, za razglasitev ničnosti odlokov št. 2015-1185, št. 2015-1211, št. 2015-1639 in št. 2016-67, zlasti ker naj bi ti kršili francosko ustavo, Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin (v nadaljevanju: EKČP) ter direktivi 2000/31 in 2002/58 v povezavi s členi 7, 8 in 47 Listine.

57 Kar zadeva posebej tožbene razloge v zvezi s kršitvijo Direktive 2000/31, predložitveno sodišče navaja, da določbe člena L. 851-3 CSI operaterjem elektronskih komunikacij in ponudnikom tehničnih storitev nalagajo, da „na svojih omrežjih izvajajo avtomatizirane obdelave na podlagi parametrov, navedenih v dovoljenju, pri čemer je cilj teh obdelav odkrivanje povezav, ki lahko pomenijo teroristično grožnjo". Namen te metode naj bi bil izključno ta, da se v omejenem obdobju izmed vseh podatkov o povezavah, ki jih obdelujejo ti operaterji in ponudniki, zberejo tisti podatki, ki bi bili lahko povezani s tovrstnim hudim kaznivim dejanjem. V takih okoliščinah naj te določbe, s katerimi naj ne bi bila naložena splošna obveznost aktivnega nadzora, ne bi kršile člena 15 Direktive 2000/31.

58 Predložitveno sodišče v zvezi s tožbenimi razlogi, ki se nanašajo na kršitev Direktive 2002/58, meni, da zlasti iz določb te direktive in sodbe z dne 21. decembra 2016, Tele2 Sverige ter Watson in drugi (C-203/15 in C-698/15, v nadaljevanju: sodba Tele2, EU:C:2016:970), izhaja, da nacionalne določbe, ki ponudnikom elektronskih komunikacijskih storitev nalagajo obveznosti, kot je splošna in neselektivna hramba podatkov o prometu ter podatkov o lokaciji uporabnikov in naročnikov, za namene, navedene v členu 15(1) navedene direktive, ki vključujejo zaščito nacionalne varnosti, obrambe in javne varnosti, spadajo na področje uporabe te direktive, saj ti predpisi urejajo dejavnost teh ponudnikov. Enako naj bi veljalo za predpise, ki urejajo dostop nacionalnih organov do podatkov in njihovo uporabo.

59 Predložitveno sodišče na podlagi tega meni, da na področje uporabe Direktive 2002/58 spadata tako obveznost hrambe na podlagi člena L. 851-1 CSI kot dostopi upravnih organov do navedenih podatkov, vključno s tistimi v realnem času, določenimi v členih L. 851-1, L. 851-2 in L. 851-4 CSI. Po mnenju tega sodišča enako velja za določbe člena L. 851-3 CSI, ki zadevnim operaterjem sicer ne nalagajo splošne obveznosti hrambe, jim pa kljub temu nalagajo izvajanje avtomatiziranih obdelav na njihovih omrežjih, katerih cilj je odkrivanje povezav, ki lahko pomenijo teroristično grožnjo.

60 Nasprotno pa to sodišče meni, da določbe CSI, na katere se nanašajo tožbe za razglasitev ničnosti in ki zadevajo metode pridobivanja informacij, ki jih neposredno izvaja država, ne da bi urejale dejavnosti ponudnikov elektronskih komunikacijskih storitev in jim nalagale posebne obveznosti, ne spadajo na področje uporabe Direktive 2002/58. Teh določb naj ne bi bilo mogoče obravnavati, kot da se z njimi izvaja pravo Unije, zato naj se ne bi bilo mogoče veljavno sklicevati na tožbene razloge, ki se nanašajo na to, da te določbe pomenijo kršitev Direktive 2002/58.

61 Tako naj bi se za rešitev sporov, ki se nanašajo na zakonitost odlokov št. 2015-1185, št. 2015-1211, št. 2015-1639 in št. 2016-67 z vidika Direktive 2002/58, v delu, v katerem so bili sprejeti za izvajanje členov od L. 851-1 do L. 851-4 CSI, postavljala tri vprašanja glede razlage prava Unije.

62 Kar zadeva razlago člena 15(1) Direktive 2002/58, se predložitveno sodišče na prvem mestu sprašuje o tem, ali ni treba obveznosti splošne in neselektivne hrambe, naložene ponudnikom storitev elektronskih komunikacij na podlagi členov L. 851-1 in R. 851-5 CSI – zlasti z vidika jamstev in nadzorov, ki se uporabljajo za dostope upravnih organov do podatkov o povezavi in njihovo

uporabo – obravnavati kot poseg, ki je upravičen na podlagi pravice do varnosti, zagotovljene s členom 6 Listine, in zahtev nacionalne varnosti, za katero so v skladu s členom 4 PEU odgovorne izključno države članice.

63 Na drugem mestu, kar zadeva druge obveznosti, ki jih je mogoče naložiti ponudnikom elektronskih komunikacijskih storitev, predložitveno sodišče navaja, da je na podlagi določb člena L. 851-2 CSI izključno zaradi preprečevanja terorizma dovoljeno, da se od teh oseb zberejo informacije ali dokumenti iz člena L. 851-1 tega zakonika. To zbiranje, ki se nanaša zgolj na eno ali več oseb, ki so predhodno opredeljene kot osebe, ki bi bile lahko povezane s teroristično grožnjo, naj bi se izvajalo v realnem času. Podobno naj bi lahko v skladu z določbami člena L. 851-4 istega zakonika operaterji v realnem času prenašali zgolj tehnične podatke, ki se nanašajo na lokacijo terminalske opreme. S temi metodami naj bi bili za drugačne namene in po drugačnih pravilih urejeni dostopi upravnih organov do podatkov, hranjenih na podlagi CPCE in LCEN, v realnem času, ne da bi bila pri tem zadevnim ponudnikom naložena dodatna zahteva hrambe poleg tiste, ki je potrebna za zaračunavanje in zagotavljanje njihovih storitev. Prav tako naj niti določbe člena L. 851-3 CSI, ki za ponudnike storitev določajo obveznost, da na svojih omrežjih izvajajo avtomatizirano analizo povezav, ne bi nič bolj vključevale splošne in neselektivne hrambe.

64 Po eni strani predložitveno sodišče meni, da tako splošna in neselektivna hramba kot tudi dostop do podatkov o povezavi v realnem času v okoliščinah resnih in trajnih groženj nacionalni varnosti ter zlasti teroristične grožnje pomenita operativno korist, ki je ni mogoče z ničimer nadomestiti. Splošna in neselektivna hramba naj bi namreč obveščevalnim službam omogočala dostop do podatkov v zvezi s komunikacijami še pred opredelitvijo razlogov za to, da se zadevna oseba obravnava kot grožnja javni varnosti, obrambi ali državni varnosti. Poleg tega naj bi dostop do podatkov o povezavi v realnem času omogočal, da se z veliko odzivnostjo spremljajo ravnanja posameznikov, ki bi lahko pomenila neposredno grožnjo javnemu redu.

65 Po drugi strani naj bi metoda iz člena L. 851-3 CSI omogočala, da se na podlagi v ta namen natančno opredeljenih meril odkrijejo posamezniki, katerih ravnanja bi lahko ob upoštevanju njihovih načinov komunikacije razkrivala teroristično grožnjo.

66 Na tretjem mestu, predložitveno sodišče se v zvezi z dostopom pristojnih organov do hranjenih podatkov sprašuje, ali je treba Direktivo 2002/58 ob upoštevanju Listine Evropske unije o temeljnih pravicah razlagati tako, da zakonitost postopkov zbiranja podatkov o povezavi vedno pogojuje z zahtevo po obvestitvi zadevnih oseb, kadar taka obvestitev ne more več ogroziti preiskav, ki jih izvajajo pristojni organi, ali pa je mogoče šteti, da so taki postopki zakoniti ob upoštevanju vseh drugih procesnih jamstev, ki jih določa nacionalno pravo, če ta procesna jamstva zagotavljajo učinkovitost pravice do pravnega sredstva.

67 Kar zadeva ta druga procesna jamstva, predložitveno sodišče zlasti pojasnjuje, da lahko vsaka oseba, ki želi preveriti, da se v zvezi z njo nobena obveščevalna metoda ne uporablja nezakonito, vloži tožbo pri specializirani sestavi Conseil d'État (državni svet), pristojni za to, da ob upoštevanju elementov, ki so ji bili predloženi zunaj kontradiktornega postopka, preveri, ali se je za tožečo stranko uporabila ena od metod in ali se je ta izvedla v skladu s knjigo VIII CSI. Pristojnosti, ki naj bi jih ta sestava imela za preučitev tožb, naj bi zagotavljale učinkovitost sodnega nadzora, ki ga izvaja. Tako naj bi bila pristojna za preučitev tožb ter za to, da po uradni dolžnosti obravnava vse nezakonitosti, ki jih ugotovi, in da upravi naloži sprejetje vseh koristnih ukrepov za odpravo ugotovljenih nezakonitosti. Poleg tega naj bi bila nacionalna komisija za nadzor nad obveščevalnimi metodami pristojna za preverjanje, ali se metode zbiranja informacij na nacionalnem ozemlju izvajajo v skladu z zahtevami, ki izhajajo iz CSI. Tako naj okoliščina, da zakonske določbe iz postopka v glavni stvari ne nalagajo obvestitve zadevnih oseb o nadzornih ukrepih, katerih predmet so bile, sama zase ne bi pomenila pretiranega posega v pravico do spoštovanja zasebnega življenja.

68 V teh okoliščinah je Conseil d'État (državni svet) prekinil odločanje in Sodišču v predhodno odločanje predložil ta vprašanja:

„1. Ali je treba obveznost splošne in neselektivne hrambe, ki je ponudnikom naložena ob upoštevanju pooblastilnih določb člena 15(1) Direktive [2002/58], v okoliščinah hudega in trajnega ogrožanja nacionalne varnosti ter zlasti teroristične grožnje razlagati kot poseg, ki je upravičen na podlagi pravice do varnosti, določene v členu 6 [Listine], in zahtev nacionalne varnosti, za katere v skladu s členom 4 [PEU] ostajajo odgovorne izključno države članice?

2. Ali je treba Direktivo [2002/58] ob upoštevanju [Listine] razlagati tako, da omogoča zakonske ukrepe, kot so ukrepi zbiranja podatkov o prometu in lokaciji zadevnih posameznikov v realnem času, ki sicer vplivajo na pravice in obveznosti ponudnikov storitev elektronskih komunikacij, vendar jim ne nalagajo posebne obveznosti hrambe njihovih podatkov?

3. Ali je treba Direktivo [2002/58] ob upoštevanju [Listine] razlagati tako, da zakonitost postopkov zbiranja podatkov o povezavi vedno pogojuje z zahtevo informiranja zadevnih oseb, kadar tako informiranje ne more več ogroziti preiskav, ki jih izvajajo pristojni organi, ali pa je mogoče šteti, da so taki postopki zakoniti, ob upoštevanju vseh drugih obstoječih procesnih jamstev, ker ta procesna jamstva zagotavljajo učinkovitost pravice do pravnega sredstva?“

Zadeva C-512/18

69 French Data Network, Quadrature du Net in Fédération des fournisseurs d'accès à Internet associatifs so 1. septembra 2015 pri Conseil d'État (državni svet) vložili tožbo za razglasitev ničnosti implicitne odločbe o zavrnitvi, ki izhaja iz molka predsednika vlade o njihovi zahtevi za razveljavitev člena R. 10-13 CPCE in odloka št. 2011-219, zlasti ker naj bi se s tema predpisoma kršil člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 Listine. Organizacijama Privacy International in Center for Democracy and Technology je bila dovoljena intervencija v postopku v glavni stvari.

70 Kar zadeva člen R. 10-13 CPCE ter v njem določeno obveznost splošne in neselektivne hrambe podatkov v zvezi s komunikacijami, predložitveno sodišče, ki navaja podobne preudarke, kot so bili navedeni v zadevi C-511/18, meni, da taka hramba pravosodnemu organu omogoča dostop do podatkov v zvezi s komunikacijami, ki jih je posameznik opravil, preden je bil osumljen storitve kaznivega dejanja, zato ta hramba pomeni korist za preiskovanje, ugotavljanje in pregon kaznivih dejanj, ki je ni mogoče z ničimer nadomestiti.

71 Kar zadeva odlok št. 2011-219, predložitveno sodišče meni, da člen 6(II) LCEN, ki nalaga obveznost posedovanja in hrambe zgolj podatkov, ki se nanašajo na ustvarjanje vsebine, ne spada na področje uporabe Direktive 2002/58, saj je to v skladu z njenim členom 3(1) omejeno zgolj na zagotavljanje javno dostopnih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v Uniji, temveč na področje uporabe Direktive 2000/31.

72 Vendar to sodišče meni, da je iz člena 15(1) in (2) Direktive 2000/31 razvidno, da s to direktivo ni vzpostavljena načelna prepoved hrambe podatkov, ki se nanašajo na ustvarjanje vsebine, od katere bi bilo mogoče odstopiti zgolj izjemoma. Tako naj bi se postavljalo vprašanje, ali je treba člene 12, 14 in 15 navedene direktive v povezavi s členi od 6 do 8 in 11 ter členom 52(1) Listine razlagati tako, da državi članici omogočajo, da uvede nacionalno ureditev, kot je člen 6(II) LCEN, ki zadevnim osebam nalaga hrambo podatkov, ki omogočajo identifikacijo vsakogar, ki je prispeval k ustvarjanju vsebine ali ene od vsebin storitev, ki jih navedene osebe ponujajo, da bi lahko pravosodni organ po potrebi zahteval predložitev teh podatkov za dosego spoštovanja pravil v zvezi s civilno ali kazensko odgovornostjo.

73 V teh okoliščinah je Conseil d'État (državni svet) prekinil odločanje in Sodišču v predhodno odločanje predložil ti vprašanji:

„1. Ali je treba obveznost splošne in neselektivne hrambe, ki je ponudnikom naložena ob upoštevanju pooblastilnih določb člena 15(1) Direktive [2002/58], razlagati med drugim ob upoštevanju jamstev in nadzorov, ki se zagotovijo po tem, ko se ti podatki o povezavi zberejo in uporabijo, kot poseg, ki je upravičen na podlagi pravice do varnosti, določene v členu 6 [Listine], in zahtev nacionalne varnosti, za katero v skladu s členom 4 [PEU] ostajajo odgovorne izključno države članice?

2. Ali je treba določbe Direktive [2000/31] ob upoštevanju členov 6, 7, 8 in 11 ter 52(1) [Listine] razlagati tako, da državi članici omogočajo, da sprejme nacionalno ureditev, ki osebam, katerih dejavnost je zagotavljanje dostopa do javnih spletnih komunikacijskih storitev, in fizičnim ali pravnim osebam, ki za dostop javnosti prek javnih spletnih komunikacijskih storitev zagotavljajo, četudi brezplačno, hrambo vsakršnih signalov, pisnega in slikovnega gradiva, zvokov ali sporočil, ki se pridobijo od prejemnikov teh storitev, nalaga hrambo podatkov, ki omogočajo identifikacijo vsakogar, ki je prispeval k ustvarjanju vsebine ali ene od vsebin storitev, ki jih navedene osebe ponujajo, da bi lahko pravosodni organ po potrebi zahteval predložitev teh podatkov za dosego spoštovanja pravil v zvezi s civilno ali kazensko odgovornostjo?“

Zadeva C-520/18

74 Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL in UA, Liga voor Mensenrechten ASBL in Ligue des Droits de l'Homme ASBL ter VZ, WY in XX so 10. januarja, 16. januarja, 17. januarja in 18. januarja 2017 pri Cour constitutionnelle (ustavno sodišče, Belgija) vložili tožbe, ki so bile v okviru postopka v glavni stvari združene, za razglasitev ničnosti zakona z dne 29. maja 2016 z obrazložitvijo, da krši člena 10 in 11 Constitution belge (belgijska ustava) v povezavi s členi 5, od 6 do 11, 14, 15, 17 in 18 EKČP, člene 7, 8, 11 in 47 ter člen 52(1) Listine, člen 17 Mednarodnega pakta o državljanskih in političnih pravicah, ki ga je sprejela Generalna skupščina Združenih narodov 16. decembra 1966 in je začel veljati 23. marca 1976, splošna načela pravne varnosti, sorazmernosti in informacijskega samoodločanja ter člen 5(4) PEU.

75 Tožeče stranke iz postopka v glavni stvari v podporo tožbam v bistvu trdijo, da je zakon z dne 29. maja 2016 nezakonit zlasti zato, ker presega meje tega, kar je nujno potrebno, in ne določa zadostnih jamstev. Natančneje, niti njegove določbe o hrambi podatkov niti določbe, ki urejajo dostop organov do hranjenih podatkov, naj ne bi izpolnjevale zahtev, ki izhajajo iz sodbe z dne 8. aprila 2014, Digital Rights Ireland in drugi (C-293/12 in C-594/12, v nadaljevanju: sodba Digital Rights, EU:C:2014:238), in sodbe z dne 21. decembra 2016, Tele2 (C-203/15 in C-698/15, EU:C:2016:970). Te določbe naj bi namreč vključevale tveganje za to, da pristojni organi izoblikujejo osebnostne profile, iz česar izhaja možnost zlorab, ter naj poleg tega ne bi določale ustrezne ravni za varstvo in zaščito hranjenih podatkov. Nazadnje, ta zakon naj bi zajemal osebe, za katere velja poklicna skrivnost, in osebe, ki jim je naložena obveznost zaupnosti, ter naj bi se nanašal na občutljive osebne podatke o komunikacijah, ne da bi vključeval posebna jamstva za zaščito zadnjenavedenih podatkov.

76 Predložitveno sodišče navaja, da so podatki, ki jih morajo v skladu z zakonom z dne 29. maja 2016 hraniti ponudniki storitev telefonije, vključno s telefonijo prek interneta, dostopa do interneta in elektronske pošte prek interneta, ter operaterji, ki ponujajo javna omrežja elektronskih komunikacij, enaki tistim, naštetim v Direktivi 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL 2006, L 105, str. 54), ne da bi bilo določeno kakršno koli razlikovanje med zadevnimi osebami ali glede na zastavljeni cilj. V zvezi z zadnjenavedenim to sodišče pojasnjuje, da cilj, ki ga želi doseči zakonodajalec s tem zakonom, ni le boj proti terorizmu in otroški pornografiji, ampak tudi možnost uporabe hranjenih podatkov v zelo različnih položajih v okviru kazenske preiskave. Predložitveno

sodišče poleg tega ugotavlja, da je iz obrazložitvenega memoranduma navedenega zakona razvidno, da je nacionalni zakonodajalec menil, da je glede na želeni cilj nemogoče uvesti obveznost ciljne in selektivne hrambe, ter da se je odločil, da bo obveznosti splošne in neselektivne hrambe dodal stroga jamstva tako glede hranjenih podatkov kot glede dostopa do njih, da bi poseganje v pravico do spoštovanja zasebnega življenja omejil na najmanjšo možno mero.

77 Predložitveno sodišče k temu še dodaja, da člen 126(2)(1) in (2) zakona z dne 13. junija 2005 v različici, ki izhaja iz zakona z dne 29. maja 2016, določa pogoje, pod katerimi lahko pravosodni organi oziroma obveščevalne in varnostne službe pridobijo dostop do hranjenih podatkov, zato bi bilo treba preizkus zakonitosti tega zakona z vidika zahtev prava Unije prekiniti, dokler Sodišče ne izda odločb v dveh zadevah za predhodno odločanje, ki jih obravnava in se nanašata na tak dostop.

78 Nazadnje, predložitveno sodišče navaja, da je namen zakona z dne 29. maja 2016 omogočiti učinkovito preiskovanje kaznivih dejanj in učinkovito kaznovanje spolnih zlorab mladoletnikov ter omogočiti identifikacijo storilca takega kaznivega dejanja, tudi kadar se uporabijo sredstva za elektronsko komuniciranje. V postopku pred njim naj bi bila v zvezi s tem pozornost posvečena pozitivnim obveznostim, ki izhajajo iz členov 3 in 8 EKČP. Te obveznosti naj bi lahko izhajale tudi iz ustreznih določb Listine, ki bi lahko vplivale na razlago člena 15(1) Direktive 2002/58.

79 V teh okoliščinah je Cour constitutionnelle (ustavno sodišče) prekinilo odločanje in Sodišču v predhodno odločanje predložilo ta vprašanja:

„1. Ali je treba člen 15(1) Direktive [2002/58] v povezavi s pravico do varnosti, ki jo zagotavlja člen 6 [Listine], in pravico do spoštovanja osebnih podatkov, kot jo zagotavljajo členi 7, 8 in 52(1) [Listine], razlagati tako, da nasprotuje nacionalni zakonodaji, kakršna je ta v postopku v glavni stvari, ki določa splošno obveznost, da operaterji in ponudniki storitev elektronskih komunikacij hranijo podatke o prometu in lokaciji v smislu Direktive [2002/58], ki jih ustvarijo ali obdelajo pri opravljanju teh storitev, pri čemer cilj te nacionalne zakonodaje ni le preiskovanje, odkrivanje in pregon hudega kriminala, temveč tudi zagotavljanje državne varnosti, obrambe in javne varnosti, preiskovanje, odkrivanje in pregon drugih dejanj, ki niso hudi kriminal, preprečevanje prepovedane uporabe elektronskih komunikacijskih sistemov ali doseganje drugih ciljev, ki so našteti v členu 23(1) Uredbe [2016/679], ob tem da so v zvezi s to obveznostjo v tej zakonodaji natančno določena jamstva glede hrambe in dostopa do podatkov?

2. Ali je treba člen 15(1) Direktive [2002/58] v povezavi s členi 4, 7, 8, 11 in 52(1) [Listine] razlagati tako, da nasprotuje nacionalni zakonodaji, kakršna je ta v postopku v glavni stvari, ki določa splošno obveznost, da operaterji in ponudniki elektronskih komunikacijskih storitev hranijo podatke o prometu in lokaciji v smislu Direktive [2002/58], ki jih ustvarijo ali obdelajo pri opravljanju teh storitev, če je cilj te zakonodaje med drugim izpolnitev pozitivnih obveznosti, ki jih ima organ na podlagi členov 4 in [7] Listine, da sprejme zakonski okvir, ki omogoča učinkovito kazensko preiskavo in učinkovito kaznovanje spolnih zlorab mladoletnikov ter ki omogoča uspešno identifikacijo storilcev teh kaznivih dejanj, tudi kadar se uporabijo sredstva za elektronsko komuniciranje?

3. Če bi Cour constitutionnelle (ustavno sodišče) na podlagi odgovorov na prvo ali drugo vprašanje za predhodno odločanje ugotovilo, da izpodbijani zakon krši eno ali več obveznosti, ki izhajajo iz določb, omenjenih v teh vprašanjih, ali lahko odloči, da se učinki zakona [z dne 29. maja 2016] začasno ohranijo, da se prepreči pravna negotovost in da se omogoči, da se prej zbrani in ohranjeni podatki še naprej lahko uporabljajo za cilje, navedene v zakonu?“

Postopek pred Sodiščem

80 S sklepom predsednika Sodišča z dne 25. septembra 2018 sta bili zadevi C-511/18 in C-512/18 združeni za pisni in ustni postopek ter izdajo sodbe. S sklepom z dne 9. julija 2020 je bila zadeva C-520/18 združena s tema zadevama za izdajo sodbe.

Vprašanja za predhodno odločanje

Prvi vprašanji v zadevah C-511/18 in C-512/18 ter prvo in drugo vprašanje v zadevi C-520/18

81 Predložitveni sodišči s prvima vprašanjema v zadevah C-511/18 in C-512/18 ter prvim in drugim vprašanjem v zadevi C-520/18, ki jih je treba obravnavati skupaj, v bistvu sprašujeta, ali je treba člen 15(1) Direktive 2002/58 razlagati tako, da nasprotuje nacionalni ureditvi, ki ponudnikom elektronskih komunikacijskih storitev nalaga splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji za namene, določene v navedenem členu 15(1).

Uvodne ugotovitve

82 Iz spisov, ki so na voljo Sodišču, je razvidno, da ureditve iz postopkov v glavni stvari zajemajo vsa sredstva za elektronsko komuniciranje in veljajo za vse uporabnike teh sredstev brez razlikovanja ali izjeme. Poleg tega so podatki, katerih hrambo te ureditve nalagajo ponudnikom elektronskih komunikacijskih storitev, zlasti tisti, ki so potrebni za izsledtev vira in cilja komunikacije, določitev datuma, ure, trajanja in vrste komunikacije, prepoznavo uporabljene komunikacijske opreme ter ugotovitev lokacije terminalske opreme in komunikacije, med katere spadajo med drugim ime in naslov uporabnika, telefonska številka klicatelja in klicana telefonska številka ter IP naslov za internetne storitve. Navedeni podatki pa ne zajemajo vsebine zadevnih komunikacij.

83 Tako podatki, ki jih je treba v skladu z nacionalnimi ureditvami iz postopkov v glavni stvari hraniti eno leto, omogočajo zlasti ugotovitev, kdo je oseba, s katero je uporabnik elektronskega komunikacijskega sredstva komuniciral, in prek katerega sredstva je ta komunikacija potekala, določitev datuma, ure in trajanja komunikacij, internetnih povezav in kraja, iz katerega so potekale, ter lokalizacijo terminalske opreme, ne da bi bila komunikacija nujno prenesena. Poleg tega omogočajo določitev pogostosti komunikacij uporabnika z določenimi osebami v danem obdobju. Nazadnje, kar zadeva nacionalno ureditev iz zadev C-511/18 in C-512/18, se zdi, da ta – ker zajema tudi podatke v zvezi s prenosom elektronskih komunikacij prek omrežij – omogoča tudi identifikacijo vrste informacij, pregledanih na spletu.

84 Kar zadeva zastavljene cilje, je treba ugotoviti, da se ureditvi iz zadev C-511/18 in C-512/18 med drugimi cilji nanašata na preiskovanje, ugotavljanje in pregon kaznivih dejanj na splošno, državno neodvisnost, ozemeljsko celovitost in nacionalno obrambo, pomembne interese zunanje politike, uresničevanje evropskih in mednarodnih zavez Francije, pomembne gospodarske, industrijske in znanstvene interese Francije ter preprečevanje terorizma, posegov v republikansko obliko institucij in kolektivnega nasilja, ki lahko resno ogrozi javni mir. Kar zadeva ureditev iz zadeve C-520/18, so njeni cilji med drugim preiskovanje, odkrivanje in pregon kaznivih dejanj ter zaščita nacionalne varnosti, obrambe ozemlja in javne varnosti.

85 Predložitveni sodišči se zlasti sprašujeta o morebitnih vplivih pravice do varnosti, določene s členom 6 Listine, na razlago člena 15(1) Direktive 2002/58. Prav tako se sprašujeta, ali je mogoče poseg v temeljne pravice, določene s členoma 7 in 8 Listine, ki ga pomeni hramba podatkov, določena z ureditvama iz postopkov v glavni stvari, ob upoštevanju obstoja pravil, ki omejujejo dostop nacionalnih organov do shranjenih podatkov, obravnavati kot upravičen. Dalje, Conseil d'État (državni svet) meni, da je treba to vprašanje, ker se postavlja v okoliščinah, zaznamovanih z resnimi in trajnimi

grožnjami nacionalni varnosti, presoditi tudi z vidika člena 4(2) PEU. Kar zadeva Cour constitutionnelle (ustavno sodišče), to poudarja, da se z nacionalno ureditvijo iz zadeve C-520/18 uresničujejo tudi pozitivne obveznosti, ki izhajajo iz členov 4 in 7 Listine, katerih namen je določiti zakonski okvir za učinkovito kaznovanje spolnih zlorab mladoletnikov.

86 Čeprav tako Conseil d'État (državni svet) kot tudi Cour constitutionnelle (ustavno sodišče) izhajata iz premise, da nacionalni ureditvi iz postopkov v glavni stvari, ki urejata hrambo podatkov o prometu in podatkov o lokaciji ter dostop nacionalnih organov do teh podatkov za namene, določene s členom 15(1) Direktive 2002/58, kot je zaščita nacionalne varnosti, spadata na področje uporabe te direktive, so nekatere stranke iz postopkov v glavni stvari in nekatere države članice, ki so Sodišču predložile pisna stališča, v zvezi s tem izrazile drugačno mnenje, še zlasti v zvezi z razlago člena 1(3) navedene direktive. Zato je treba najprej preučiti, ali navedeni ureditvi spadata na področje uporabe te direktive.

Področje uporabe Direktive 2002/58

87 Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International in Center for Democracy and Technology v bistvu trdijo – pri čemer se v zvezi s tem sklicujejo na sodno prakso Sodišča, ki se nanaša na področje uporabe Direktive 2002/58 – da na to področje uporabe spadata tako hramba podatkov kot tudi dostop do hranjenih podatkov, pa naj se ta dostop izvede naknadno ali v realnem času. Ker je namreč cilj zaščite nacionalne varnosti izrecno naveden v členu 15(1) te direktive, naj prizadevanje za uresničitev tega cilja ne bi povzročilo neuporabe navedene direktive. Člen 4(2) PEU, na katerega napotujeta predložitveni sodišči, naj ne bi vplival na to presojo.

88 Kar zadeva obveščevalne ukrepe, ki jih neposredno izvajajo pristojni francoski organi, ne da bi ti ukrepi urejali dejavnosti ponudnikov elektronskih komunikacijskih storitev in jim nalagali posebne obveznosti, Center for Democracy and Technology navaja, da ti ukrepi nujno spadajo na področje uporabe Direktive 2002/58 in Listine, saj pomenijo odstopanja od načela zaupnosti, zagotovljenega s členom 5 te direktive. Torej bi morali navedeni ukrepi izpolnjevati zahteve, ki izhajajo iz člena 15(1) te direktive.

89 Francoska, češka in estonska vlada, Irska, ciprska, madžarska, poljska in švedska vlada ter vlada Združenega kraljestva po drugi strani v bistvu trdijo, da se Direktiva 2002/58 ne uporablja za nacionalni ureditvi, kot sta ti iz postopkov v glavni stvari, ker je njun namen zaščita nacionalne varnosti. Dejavnosti obveščevalnih agencij naj bi v delu, v katerem je njihov namen vzdrževanje javnega reda ter zagotavljanje notranje varnosti in ozemeljske celovitosti, spadale med bistvene funkcije držav članic in naj bi bile zato v njihovi izključni pristojnosti, kot naj bi bilo razvidno med drugim iz člena 4(2), tretji stavek, PEU.

90 Te vlade in Irska se poleg tega sklicujejo na člen 1(3) Direktive 2002/58, ki naj bi s področja uporabe te direktive, kot je bilo to določeno že v členu 3(2), prva alinea, Direktive 95/46, izključeval dejavnosti, povezane z javno varnostjo, obrambo in državno varnostjo. V zvezi s tem se opirajo na razlago zadnjenavedene določbe iz sodbe z dne 30. maja 2006, Parlament/Svet in Komisija (C-317/04 in C-318/04, EU:C:2006:346).

91 V zvezi s tem je treba navesti, da Direktiva 2002/58 v skladu s svojim členom 1(1) med drugim določa harmonizacijo nacionalnih določb, ki so potrebne za zagotovitev enakovredne ravni varstva temeljnih pravic in svoboščin ter zlasti pravice do zasebnosti in zaupnosti v zvezi z obdelavo osebnih podatkov na področju elektronskih komunikacij.

92 Člen 1(3) te direktive s področja uporabe te direktive izključuje „dejavnosti države" na področjih, ki so v njem navedena, med katerimi so dejavnosti države na področju kazenskega prava ter dejavnosti v zvezi z javno varnostjo, obrambo in državno varnostjo, vključno z gospodarsko blaginjo države,

kadar se dejavnosti nanašajo na zadeve v zvezi z državno varnostjo. Dejavnosti, ki so tako navedene primeroma, so vedno dejavnosti držav ali državnih organov, ki niso povezane s področji dejavnosti posameznikov (sodba z dne 2. oktobra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, točka 32 in navedena sodna praksa).

93 Poleg tega člen 3 Direktive 2002/58 določa, da se ta direktiva uporablja za obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v Uniji, vključno z javnimi komunikacijskimi omrežji, ki podpirajo zbiranje podatkov in identifikacijske naprave (v nadaljevanju: elektronske komunikacijske storitve). Zato je treba šteti, da navedena direktiva ureja dejavnosti ponudnikov teh storitev (sodba z dne 2. oktobra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, točka 33 in navedena sodna praksa).

94 V tem okviru člen 15(1) Direktive 2002/58 določa, da lahko države članice, ob upoštevanju pogojev, ki jih ta člen določa, sprejmejo „zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, določenih v členu 5, členu 6, členu 8(1), (2), (3) in (4) ter členu 9 te direktive“ (sodba z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 71).

95 Člen 15(1) Direktive 2002/58 pa nujno zahteva, da nacionalni zakonski ukrepi, ki so v njem navedeni, spadajo na področje uporabe te direktive, ker ta državam članicam izrecno dopušča, da jih sprejmejo, le ob upoštevanju pogojev, ki jih določa. Poleg tega taki ukrepi za namene, navedene v tej določbi, urejajo dejavnost ponudnikov elektronskih komunikacijskih storitev (sodba z dne 2. oktobra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, točka 34 in navedena sodna praksa).

96 Sodišče je zlasti glede na te ugotovitve razsodilo, da je treba člen 15(1) Direktive 2002/58 v povezavi s členom 3 te direktive razlagati tako, da na področje uporabe te direktive spada ne le zakonski ukrep, ki ponudnikom elektronskih komunikacijskih storitev nalaga, da hranijo podatke o prometu in podatke o lokaciji, temveč tudi zakonski ukrep, s katerim jim je naloženo, da pristojnim nacionalnim organom odobrijo dostop do teh podatkov. Taki zakonski ukrepi namreč nujno vključujejo obdelavo teh podatkov s strani navedenih ponudnikov in jih v delu, v katerem urejajo dejavnosti navedenih ponudnikov, ni mogoče šteti za dejavnosti držav iz člena 1(3) navedene direktive (glej v tem smislu sodbo z dne 2. oktobra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, točki 35 in 37 ter navedena sodna praksa).

97 Poleg tega bi glede na ugotovitve iz točke 95 te sodbe in glede na splošno sistematiko Direktive 2002/58 razlaga te direktive, v skladu s katero bi bili zakonski ukrepi iz njenega člena 15(1) izključeni s področja uporabe navedene direktive, ker se cilji, ki jim morajo ti ukrepi slediti, v bistvenem prekrivajo z nameni, ki jih uresničujejo dejavnosti iz člena 1(3) te direktive, temu členu 15(1) odvzela polni učinek (glej v tem smislu sodbo z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točki 72 in 73).

98 Pojma „dejavnosti“ iz člena 1(3) Direktive 2002/58 torej ni mogoče – kot je v bistvu navedel generalni pravobranilec v točki 75 sklepnih predlogov v združenih zadevah La Quadrature du Net in drugi (C-511/18 in C-512/18, EU:C:2020:6) – razlagati tako, da zajema zakonske ukrepe iz člena 15(1) te direktive.

99 Določbe člena 4(2) PEU, na katere se sklicujejo vlade, navedene v točki 89 te sodbe, ne morejo ovreči te ugotovitve. V skladu z ustaljeno sodno prakso Sodišča namreč, čeprav so države članice pristojne, da opredelijo svoje bistvene varnostne interese in sprejmejo primerne ukrepe za zagotovitev svoje notranje in zunanje varnosti, zgolj dejstvo, da je bil nacionalni ukrep sprejet zaradi zaščite nacionalne varnosti, ne more povzročiti izključitve uporabe prava Unije in držav članic oprostiti obveznosti spoštovanja tega prava (glej v tem smislu sodbe z dne 4. junija 2013, ZZ, C-300/11, EU:C:2013:363, točka 38 in navedena sodna praksa; z dne 20. marca 2018, Komisija/Avstrija (Državna tiskarna), C-187/16,

EU:C:2018:194, točki 75 in 76, in z dne 2. aprila 2020, Komisija/Poljska, Madžarska in Češka republika (Začasni mehanizem za premestitev prosilcev za mednarodno zaščito), C-715/17, C-718/17 in C-719/17, EU:C:2020:257, točki 143 in 170).

100 Res je, da je Sodišče v sodbi z dne 30. maja 2006, Parlament/Svet in Komisija (C-317/04 in C-318/04, EU:C:2006:346, točke od 56 do 59), razsodilo, da prenos osebnih podatkov s strani letalskih družb javnim organom tretje države zaradi preprečevanja terorizma in drugih hudih kaznivih dejanj ter boja proti njim v skladu s členom 3(2), prva alinea, Direktive 95/46 ne spada na področje uporabe te direktive, ker tak prenos spada v okvir, ki ga določijo javni organi, in se nanaša na javno varnost.

101 Vendar ob upoštevanju ugotovitev iz točk 93, 95 in 96 te sodbe te sodne prakse ni mogoče uporabiti za razlago člena 1(3) Direktive 2002/58. Kot je namreč generalni pravobranilec v bistvu navedel v točkah od 70 do 72 sklepnih predlogov v združenih zadevah La Quadrature du Net in drugi (C-511/18 in C-512/18, EU:C:2020:6), so s členom 3(2), prva alinea, Direktive 95/46, na katerega se nanaša navedena sodna praksa, s področja uporabe zadnjenavedene direktive na splošno izključeni „postopk[i] obdelave v zvezi z javno varnostjo, obrambo, državno varnostjo“, brez razlikovanja glede na to, kdo izvaja zadevno obdelavo podatkov. Nasprotno pa je v okviru razlage člena 1(3) Direktive 2002/58 tako razlikovanje potrebno. Kot izhaja iz točk od 94 do 97 te sodbe, namreč vsi postopki obdelave osebnih podatkov, ki jih izvajajo ponudniki elektronskih komunikacijskih storitev, spadajo na področje uporabe navedene direktive, vključno s tistimi, ki izhajajo iz obveznosti, ki jih tem ponudnikom naložijo javni organi, medtem ko bi zadnjenavedeni postopki obdelave, kadar je to primerno, lahko spadali na področje uporabe izjeme iz člena 3(2), prva alinea, Direktive 95/46 glede na širšo formulacijo te določbe, ki zajema vse postopke obdelave v zvezi z javno varnostjo, obrambo ali državno varnostjo, ne glede na to, kdo jih izvaja.

102 Poleg tega je treba poudariti, da je bila Direktiva 95/46, ki je bila predmet zadeve, v kateri je bila izdana sodba z dne 30. maja 2006, Parlament/Svet in Komisija (C-317/04 in C-318/04, EU:C:2006:346), na podlagi člena 94(1) Uredbe 2016/679 razveljavljena in s to uredbo nadomeščena z učinkom od 25. maja 2018. Čeprav navedena uredba v členu 2(2)(d) določa, da se ne uporablja za obdelavo „s strani pristojnih organov“ za namene, med drugim, preprečevanja in odkrivanja kaznivih dejanj, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, pa iz člena 23(1)(d) in (h) te uredbe izhaja, da obdelava osebnih podatkov, ki jih v iste namene izvajajo posamezniki, spada na njeno področje uporabe. Iz tega sledi, da je zgoraj navedena razlaga členov 1(3), 3 in 15(1) Direktive 2002/58 skladna z opredelitvijo področja uporabe Uredbe 2016/679, ki ga ta direktiva dopolnjuje in podrobneje določa.

103 Kadar pa države članice neposredno izvajajo ukrepe, ki odstopajo od načela zaupnosti elektronskih komunikacij, ne da bi ponudnikom takih komunikacijskih storitev naložile obveznosti obdelave, varstvo podatkov zadevnih oseb ne spada na področje uporabe Direktive 2002/58, temveč zgolj na področje uporabe nacionalnega prava, s pridržkom uporabe Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL 2016, L 119, str. 89), tako da morajo biti zadevni ukrepi skladni med drugim z nacionalnim ustavnim pravom in zahtevami EKČP.

104 Iz navedenih preudarkov izhaja, da nacionalna ureditev, kot sta ti iz postopkov v glavni stvari, s katero je ponudnikom elektronskih komunikacijskih storitev naloženo, da hranijo podatke o prometu in podatke o lokaciji zaradi zaščite nacionalne varnosti in boja proti kriminalu, spada na področje uporabe Direktive 2002/58.

Razlaga člena 15(1) Direktive 2002/58

105 Najprej je treba spomniti, da je treba v skladu z ustaljeno sodno prakso za razlago določbe prava Unije upoštevati ne le njeno besedilo, ampak tudi njeno sobesedilo in cilje, ki jih uresničuje ureditev, katere del je, ter zlasti zgodovino nastanka te ureditve (glej v tem smislu sodbo z dne 17. aprila 2018, Egenberger, C-414/16, EU:C:2018:257, točka 44).

106 Namen Direktive 2002/58 je, kot izhaja med drugim iz njenih uvodnih izjav 6 in 7, zavarovati uporabnike elektronskih komunikacijskih storitev pred tveganji za njihove osebne podatke in zasebnost, ki izhajajo iz novih tehnologij in zlasti čedalje večje zmogljivosti samodejnega shranjevanja in obdelave. Zlasti pa je namen navedene direktive, kot je navedeno v njeni uvodni izjavi 2, zagotoviti polno spoštovanje pravic, določenih v členih 7 in 8 Listine. V zvezi s tem iz obrazložitve predloga direktive Evropskega parlamenta in Sveta o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (COM(2000) 385 final), na podlagi katerega je bila sprejeta Direktiva 2002/58, izhaja, da je zakonodajalec Unije želel „še naprej zagotavljati visoko raven varstva osebnih podatkov in zasebnosti za vse elektronske komunikacijske storitve ne glede na tehnologijo, ki se uporablja“.

107 V ta namen člen 5(1) Direktive 2002/58 določa načelo zaupnosti elektronskih komunikacij in z njimi povezanih podatkov o prometu ter med drugim zahteva, da se načeloma vsem, razen uporabnikom, prepove shranjevanje teh sporočil in podatkov brez privolitve uporabnikov.

108 Zlasti kar zadeva obdelavo in shranjevanje podatkov o prometu s strani ponudnikov elektronskih komunikacijskih storitev, iz člena 6 ter uvodnih izjav 22 in 26 Direktive 2002/58 izhaja, da je taka obdelava dovoljena le v obsegu in trajanju, ki sta potrebna za trženje storitev, njihovo zaračunavanje in opravljanje storitev z dodano vrednostjo. Ko se to obdobje konča, je treba podatke, ki so bili obdelani in shranjeni, izbrisati ali predelati v anonimne. Glede podatkov o lokaciji, ki niso podatki o prometu, člen 9(1) navedene direktive določa, da se smejo takšni podatki obdelati le pod določenimi pogoji in šele po tem, ko postanejo anonimni, ali s privolitvijo uporabnikov ali naročnikov (sodba z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 86 in navedena sodna praksa).

109 Zakonodajalec Unije je tako s sprejetjem te direktive konkretiziral pravice, določene v členih 7 in 8 Listine, tako da so uporabniki elektronskih komunikacijskih sredstev načeloma upravičeni pričakovati, da bodo njihova sporočila in z njimi povezani podatki, če ne privolijo v nasprotno, ostali anonimni in jih ne bo mogoče shraniti.

110 Vendar lahko države članice na podlagi člena 15(1) Direktive 2002/58 določijo izjeme od načelne obveznosti, določene v členu 5(1) te direktive, da zagotavljajo zaupnost osebnih podatkov, in od ustreznih obveznosti, določenih predvsem v členih 6 in 9 navedene direktive, kadar je taka omejitev potreben, primeren in sorazmeren ukrep znotraj demokratične družbe za zaščito nacionalne varnosti, obrambe in javne varnosti ali za preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema. V ta namen lahko države članice med drugim sprejmejo zakonske ukrepe, ki določajo hrambo podatkov za omejeno obdobje, če je to upravičeno iz katerega od teh razlogov.

111 Vendar možnost odstopanja od pravic in obveznosti iz členov 5, 6 in 9 Direktive 2002/58 ne more upravičiti tega, da odstopanje od načelne obveznosti zagotavljanja zaupnosti elektronskih komunikacij in z njimi povezanih podatkov ter zlasti od prepovedi shranjevanja teh podatkov, ki je izrecno določena v členu 5 te direktive, postane pravilo (glej v tem smislu sodbo z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točki 89 in 104).

112 V zvezi s cilji, s katerimi je mogoče upravičiti omejitev pravic in obveznosti, določenih zlasti v členih 5, 6 in 9 Direktive 2002/58, je Sodišče že razsodilo, da je naštevanje ciljev iz člena 15(1), prvi stavek, te direktive izčrpno, tako da mora zakonski ukrep, sprejet na podlagi te določbe, dejansko in strogo ustrezati enemu od teh ciljev (glej v tem smislu sodbo z dne 2. oktobra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, točka 52 in navedena sodna praksa).

113 Poleg tega je iz člena 15(1), tretji stavek, Direktive 2002/58 razvidno, da lahko države članice zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, določenih v členih 5, 6 in 9 te direktive, sprejmejo le ob upoštevanju splošnih načel prava Unije, med katerimi je načelo sorazmernosti, in temeljnih pravic, zagotovljenih z Listino. V zvezi s tem je Sodišče že razsodilo, da se z obveznostjo, ki jo država članica z nacionalno ureditvijo naloži ponudnikom elektronskih komunikacijskih storitev, da hranijo podatke o prometu, da se, če je to potrebno, pristojnim nacionalnim organom omogoči dostop do teh podatkov, postavljajo vprašanja v zvezi s spoštovanjem ne le členov 7 in 8 Listine, ki se nanašata na varstvo zasebnega življenja in varstvo osebnih podatkov, ampak tudi člena 11 Listine, ki se nanaša na svobodo izražanja (glej v tem smislu sodbi z dne 8. aprila 2014, Digital Rights, C-293/12 in C-594/12, EU:C:2014:238, točki 25 in 70, in z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točki 91 in 92 ter navedena sodna praksa).

114 Pri razlagi člena 15(1) Direktive 2002/58 je treba torej upoštevati tako pomembnost pravice do spoštovanja zasebnega življenja, ki jo zagotavlja člen 7 Listine, in pravice do varstva osebnih podatkov, ki jo zagotavlja člen 8 te listine, kot izhaja iz sodne prakse Sodišča, kot tudi pravice do svobode izražanja, glede na to, da je ta temeljna pravica, zagotovljena v členu 11 Listine, eden od glavnih temeljev demokratične in pluralistične družbe ter je del vrednot, na katerih v skladu s členom 2 PEU temelji Unija (glej v tem smislu sodbi z dne 6. marca 2001, Connolly/Komisija, C-274/99 P, EU:C:2001:127, točka 39, in z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 93 in navedena sodna praksa).

115 V zvezi s tem je treba pojasniti, da hramba podatkov o prometu in podatkov o lokaciji sama po sebi pomeni po eni strani odstopanje od prepovedi iz člena 5(1) Direktive 2002/58, ki vsakomur razen uporabnikom prepoveduje shranjevanje teh podatkov, ter po drugi strani poseganje v temeljni pravici do spoštovanja zasebnega življenja in varstva osebnih podatkov, ki sta določeni v členih 7 in 8 Listine, pri čemer ni pomembno, ali so zadevne informacije o zasebnem življenju občutljive oziroma ali so bile zadevne osebe zaradi tega poseganja morda oškodovane (glej v tem smislu mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točki 124 in 126 ter navedena sodna praksa; glej po analogiji v zvezi s členom 8 EKČP sodbo ESČP z dne 30. januarja 2020, Breyer proti Nemčiji, CE:ECHR:2020:0130JUD005000112, točka 81).

116 Prav tako ni pomembno, ali se shranjeni podatki pozneje uporabijo ali ne (glej po analogiji, kar zadeva člen 8 EKČP, ESČP, 16. februar 2000, Amann proti Švici, CE:ECHR:2000:0216JUD002779895, točka 69, in 13. februar 2020, Trjakovski in Chipovski proti Severni Makedoniji, CE:ECHR:2020:0213JUD005320513, točka 51), saj dostop do takih podatkov ne glede na njihovo poznejšo uporabo pomeni ločeno poseganje v temeljni pravici iz prejšnje točke (glej v tem smislu mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točki 124 in 126).

117 Ta ugotovitev je še toliko bolj utemeljena, ker lahko podatki o prometu in podatki o lokaciji razkrijejo informacije o veliko vidikih zasebnega življenja zadevnih oseb, vključno z občutljivimi informacijami, kot so spolna usmerjenost, politična mnenja, verska, filozofska, družbena ali druga prepričanja in zdravstveno stanje, poleg tega pa taki podatki uživajo posebno varstvo v pravu Unije. Na podlagi navedenih podatkov, obravnavanih kot celota, je mogoče izpeljati zelo natančne ugotovitve o zasebnem življenju oseb, katerih podatki so bili shranjeni, kot so vsakodnevne navade, kraji stalnega ali začasnega prebivališča, dnevne ali druge poti, dejavnosti, socialni odnosi teh oseb in socialna okolja, ki jih obiskujejo. Natančneje, ti podatki so sredstva za ugotavljanje profila zadevnih oseb, saj so prav tako občutljive informacije z vidika pravice do spoštovanja zasebnega življenja kot sama vsebina

komunikacij (glej v tem smislu sodbi z dne 8. aprila 2014, Digital Rights, C-293/12 in C-594/12, EU:C:2014:238, točka 27, in z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 99).

118 Zato lahko na eni strani hramba podatkov o prometu in podatkov o lokaciji za policijske namene sama po sebi posega v pravico do spoštovanja komunikacij, določeno v členu 7 Listine, in odvrača uporabnike elektronskih komunikacijskih sredstev od uresničevanja svobode izražanja, ki je zagotovljena s členom 11 Listine (glej v tem smislu sodbi z dne 8. aprila 2014, Digital Rights, C-293/12 in C-594/12, EU:C:2014:238, točka 28, in z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 101). Taki odvračalni učinki pa lahko vplivajo zlasti na osebe, katerih komunikacije so v skladu z nacionalnimi predpisi poklicna skrivnost, ter na žvižgače, katerih dejavnosti so zaščitene z Direktivo (EU) 2019/1937 Evropskega parlamenta in Sveta z dne 23. oktobra 2019 o zaščiti oseb, ki prijavijo kršitve prava Unije (UL 2019, L 305, str. 17). Poleg tega so ti učinki toliko resnejši, kolikor večja sta število in raznovrstnost hranjenih podatkov.

119 Na drugi strani, glede na to, da se s splošnim in neselektivnim ukrepom shranjevanja lahko neprekinjeno shranjuje velika količina podatkov in da so informacije, ki se lahko zagotovijo s temi podatki, občutljive, že samo shranjevanje navedenih podatkov s strani ponudnikov elektronskih komunikacijskih storitev pomeni tveganje zlorabe in nezakonitega dostopa.

120 V členu 15(1) Direktive 2002/58, ki državam članicam omogoča uvedbo odstopanj iz točke 110 te sodbe, pa se odraža dejstvo, da pravice iz členov 7, 8 in 11 Listine niso absolutne, temveč jih je treba upoštevati glede na njihovo funkcijo v družbi (glej v tem smislu sodbo z dne 16. julija 2020, Facebook Ireland in Schrems, C-311/18, EU:C:2020:559, točka 172 in navedena sodna praksa).

121 Kot namreč izhaja iz člena 52(1) Listine, ta dopušča omejitve pri uresničevanju teh pravic, če so te omejitve predpisane z zakonom, če spoštujejo bistveno vsebino teh pravic, če so ob upoštevanju načela sorazmernosti potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali so potrebne zaradi zaščite pravic in svoboščin drugih.

122 Tako razlaga člena 15(1) Direktive 2002/58 v povezavi z Listino zahteva tudi upoštevanje pomena pravic, določenih s členi 3, 4, 6 in 7 Listine, ter pomena ciljev zaščite nacionalne varnosti in boja proti hudemu kriminalu, s čimer se pripomore k varstvu pravic in svoboščin drugih.

123 V zvezi s tem člen 6 Listine, na katerega napotujeta Conseil d'État (državni svet) in Cour constitutionnelle (ustavno sodišče), določa pravico vsakogar ne le do svobode, ampak tudi do varnosti, in zagotavlja pravice, ki ustrezajo pravicam, zagotovljenim s členom 5 EKČP (glej v tem smislu sodbe z dne 15. februarja 2016, N., C-601/15 PPU, EU:C:2016:84, točka 47; z dne 28. julija 2016, JZ, C-294/16 PPU, EU:C:2016:610, točka 48, in z dne 19. septembra 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, točka 42 in navedena sodna praksa).

124 Poleg tega je treba opozoriti, da je namen člena 52(3) Listine zagotoviti potrebno usklajenost med pravicami iz Listine in ustreznimi pravicami, zagotovljenimi z EKČP, ne da bi to škodilo avtonomiji prava Unije in Sodišča Evropske unije. Pri razlagi Listine je torej treba upoštevati ustrezne pravice iz EKČP kot minimalno raven varstva (glej v tem smislu sodbi z dne 12. februarja 2019, TC, C-492/18 PPU, EU:C:2019:108, točka 57, in z dne 21. maja 2019, Komisija/Madžarska (Užitek na kmetijskih zemljiščih), C-235/17, EU:C:2019:432, točka 72 in navedena sodna praksa).

125 Kar zadeva člen 5 EKČP, ki določa „pravico do svobode“ in „pravico do varnosti“, je v skladu s sodno prakso Evropskega sodišča za človekove pravice njegov namen varstvo posameznika pred kakršnim koli samovoljnim ali neutemeljenim odvzemom svobode (glej v tem smislu ESČP, 18. marec 2008, Ladent proti Poljski, CE:ECHR:2008:0318JUD001103603, točki 45 in 46; 29. marec 2010, Medvedyev in drugi proti Franciji, CE:ECHR:2010:0329JUD000339403, točki 76 in 77, ter 13. december 2012, El-Masri proti „The former Yugoslav Republic of Macedonia“, CE:ECHR:2012:1213JUD003963009,

točka 239). Ker pa se ta določba nanaša na odvzem prostosti s strani javnega organa, člena 6 Listine ni mogoče razlagati tako, da je z njim javnim organom naložena obveznost sprejetja posebnih ukrepov za sankcioniranje nekaterih kaznivih dejanj.

126 Kar posebej zadeva učinkovit boj proti kaznivim dejanjem, katerih žrtve so zlasti mladoletniki in druge ranljive osebe, na katerega je napotilo Cour constitutionnelle (ustavno sodišče), pa je treba poudariti, da lahko pozitivne obveznosti za javne organe izhajajo iz člena 7 Listine, da se tako sprejmejo pravni ukrepi za zavarovanje zasebnega in družinskega življenja (glej v tem smislu sodbo z dne 18. junija 2020, Komisija/Madžarska (Preglednost društev), C-78/18, EU:C:2020:476, točka 123 in navedena sodna praksa Evropskega sodišča za človekove pravice). Take obveznosti lahko izhajajo tudi iz navedenega člena 7 v zvezi z varstvom stanovanja in komunikacij, iz členov 3 in 4 pa v zvezi z varstvom telesne in duševne celovitosti oseb ter prepovedjo mučenja in nečloveškega in ponižujočega ravnanja.

127 Ob upoštevanju teh pozitivnih obveznosti je treba uskladiti različne zadevne interese in pravice.

128 Evropsko sodišče za človekove pravice je namreč odločilo, da pozitivne obveznosti, ki izhajajo iz členov 3 in 8 EKČP, katerih ustreznice najdemo v jamstvih iz členov 4 in 7 Listine, vključujejo zlasti sprejetje materialnih in postopkovnih določb ter praktičnih ukrepov, ki omogočajo učinkovit boj proti kršitvam zoper osebe prek učinkovite preiskave in pregona, pri čemer je ta obveznost še toliko pomembnejša, če je ogroženo fizično in psihično dobro počutje otroka. Vendar morajo biti z ukrepi, ki jih morajo sprejeti pristojni organi, v celoti spoštovana pravna sredstva in druga jamstva, s katerimi se omejuje obseg kazenskopravnih preiskovalnih pristojnosti, ter druge svoboščine in pravice. Natančneje, po mnenju tega sodišča je treba vzpostaviti pravni okvir, ki bo omogočal uskladitev različnih interesov in pravic, ki jih je treba varovati (ESČP, 28. oktober 1998, Osman proti Združenemu kraljestvu, CE:ECHR:1998:1028JUD002345294, točki 115 in 116; 4. marec 2004, M. C. proti Bolgariji, CE:ECHR:2003:1204JUD003927298, točka 151; 24. junij 2004, Von Hannover proti Nemčiji, CE:ECHR:2004:0624JUD005932000, točki 57 in 58, in 2. december 2008, K. U. proti Finski, CE:ECHR:2008:1202JUD000287202, točke 46, 48 in 49).

129 Kar zadeva spoštovanje načela sorazmernosti, člen 15(1), prvi stavek, Direktive 2002/58 določa, da lahko države članice sprejmejo ukrep, ki odstopa od načela zaupnosti sporočil in z njimi povezanih podatkov o prometu, kadar je tak ukrep „potreben, primeren in ustrezen [sorazmeren] […] znotraj demokratične družbe“ glede na cilje te določbe. V uvodni izjavi 11 te direktive je pojasnjeno, da mora biti tak ukrep „dosledno“ sorazmeren z zastavljenim ciljem.

130 V zvezi s tem je treba opozoriti, da varstvo temeljne pravice do spoštovanja zasebnega življenja v skladu z ustaljeno sodno prakso Sodišča zahteva, da se odstopanja od varstva osebnih podatkov in njegove omejitve določijo v mejah tega, kar je nujno potrebno. Poleg tega cilja v splošnem interesu ni mogoče uresničevati brez upoštevanja dejstva, da ga je treba uskladiti s temeljnimi pravicami, na katere se nanaša ukrep, in sicer z uravnoteženjem na eni strani cilja v splošnem interesu ter na drugi strani zadevnih pravic (glej v tem smislu sodbe z dne 16. decembra 2008, Satakunnan Markkinapörssi in Satamedia, C-73/07, EU:C:2008:727, točka 56; z dne 9. novembra 2010, Volker und Markus Schecke in Eifert, C-92/09 in C-93/09, EU:C:2010:662, točke 76, 77 in 86, in z dne 8. aprila 2014, Digital Rights, C-293/12 in C-594/12, EU:C:2014:238, točka 52, ter mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točka 140).

131 Natančneje, iz sodne prakse Sodišča je razvidno, da je treba možnost za države članice, da utemeljijo omejitev pravic in obveznosti, določenih zlasti s členi 5, 6 in 9 Direktive 2002/58, presojati tako, da se oceni teža posega, ki ga vključuje taka omejitev, in preveri, ali je cilj splošnega interesa, ki se uresničuje s to omejitvijo, v sorazmerju s to težo (glej v tem smislu sodbo z dne 2. oktobra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, točka 55 in navedena sodna praksa).

132 Za izpolnitev zahteve po sorazmernosti mora ureditev določati jasna in natančna pravila, ki urejajo obseg in uporabo zadevnega ukrepa ter določajo minimalne zahteve, tako da imajo osebe, za osebne podatke katerih gre, na voljo zadostna jamstva, ki omogočajo učinkovito varovanje teh podatkov pred tveganji zlorabe. Ta ureditev mora biti zakonsko zavezujoča v nacionalnem pravu, v njej pa mora biti zlasti navedeno, v kakšnih okoliščinah in pod katerimi pogoji je mogoče sprejeti ukrep, ki določa obdelavo takih podatkov, s čimer se tako zagotovi, da je poseganje omejeno na to, kar je nujno potrebno. Nujnost obstoja takih jamstev je toliko pomembnejša, kadar se osebni podatki obdelujejo avtomatizirano, zlasti kadar obstaja veliko tveganje nezakonitega dostopa do teh podatkov. Te ugotovitve veljajo še posebej, kadar gre za varstvo te posebne kategorije osebnih podatkov, ki so občutljivi podatki (glej v tem smislu sodbi z dne 8. aprila 2014, Digital Rights, C-293/12 in C-594/12, EU:C:2014:238, točki 54 in 55, in z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 117, ter mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točka 141).

133 Tako mora ureditev, ki določa hrambo osebnih podatkov, vedno ustrezati objektivnim merilom, ki vzpostavljajo povezavo med podatki, ki jih je treba hraniti, in zastavljenim ciljem (glej v tem smislu mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točka 191 in navedena sodna praksa, ter sodbo z dne 3. oktobra 2019, A in drugi, C-70/18, EU:C:2019:823, točka 63).

– Zakonski ukrepi, s katerimi je za zaščito nacionalne varnosti določena preventivna hramba podatkov o prometu in podatkov o lokaciji

134 Treba je ugotoviti, da Sodišče v sodbah, v katerih je razlagalo Direktivo 2002/58, še ni posebej preučilo cilja zaščite nacionalne varnosti, na katerega napotujejo predložitveni sodišči in vlade, ki so predložile stališča.

135 V zvezi s tem je treba najprej poudariti, da člen 4(2) PEU določa, da nacionalna varnost ostaja v izključni pristojnosti vsake države članice. Ta pristojnost ustreza prvobitnemu interesu, ki je zaščititi bistvene funkcije države in temeljne interese družbe, ter vključuje preprečevanje in kaznovanje dejavnosti, ki lahko resno destabilizirajo temeljne ustavne, politične, gospodarske ali družbene strukture države ter zlasti neposredno ogrozijo družbo, prebivalstvo ali državo kot tako, kot so zlasti teroristična dejanja.

136 Vendar pa je cilj zaščite nacionalne varnosti, razlagan ob upoštevanju člena 4(2) PEU, pomembnejši od drugih ciljev, navedenih v členu 15(1) Direktive 2002/58, med drugim od ciljev boja proti kriminalu na splošno, tudi hudemu, in zaščite javne varnosti. Grožnje, kot so navedene v prejšnji točki, se namreč po naravi in posebni resnosti razlikujejo od splošnega tveganja, da se pojavijo napetosti ali nemiri, tudi hudi, ki bi ogrozili javno varnost. Ob upoštevanju drugih zahtev iz člena 52(1) Listine je torej s ciljem zaščite nacionalne varnosti mogoče utemeljiti ukrepe, ki pomenijo večji poseg v temeljne pravice od tistega, ki bi ga bilo mogoče utemeljiti z navedenimi drugimi cilji.

137 Tako v položajih, kakršni so opisani v točkah 135 in 136 te sodbe, člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine načeloma ne nasprotuje zakonskemu ukrepu, s katerim je pristojnim organom dovoljeno, da ponudnikom elektronskih komunikacijskih storitev za omejen čas naložijo hrambo podatkov o prometu in podatkov o lokaciji vseh uporabnikov elektronskih komunikacijskih sredstev, če obstajajo dovolj konkretne okoliščine, zaradi katerih je mogoče šteti, da se zadevna država članica spopada z resno grožnjo nacionalni varnosti – kakršna je tista, na katero se nanašata točki 135 in 136 te sodbe – ki se izkaže za resnično in sedanjo ali predvidljivo. Čeprav se tak ukrep brez razlikovanja nanaša na vse uporabnike elektronskih komunikacijskih sredstev, ne da bi se na prvi pogled zdelo, da so v smislu sodne prakse, navedene v točki 133 te sodbe, povezani z grožnjo nacionalni varnosti te države članice, je treba kljub temu šteti, da se že zaradi obstoja take grožnje same po sebi vzpostavi ta povezava.

138 Vendar mora biti odredba o preventivni hrambi podatkov vseh uporabnikov elektronskih komunikacijskih sredstev časovno omejena na to, kar je nujno potrebno. Čeprav ni mogoče izključiti možnosti, da se lahko odredba, v skladu s katero morajo ponudniki elektronskih komunikacijskih storitev hraniti podatke, zaradi nadaljnjega obstoja take grožnje podaljša, trajanje vsake od odredb ne sme preseči predvidljivega časovnega obdobja. Poleg tega morajo za tako hrambo podatkov veljati omejitve in biti določena stroga jamstva, ki omogočajo učinkovito varstvo osebnih podatkov zadevnih oseb pred tveganji zlorabe. Torej ta hramba ne sme biti sistematična.

139 Glede na težo posega v temeljne pravice, določene s členoma 7 in 8 Listine, ki je posledica takega ukrepa splošne in neselektivne hrambe podatkov, je treba zagotoviti, da je njegova uporaba dejansko omejena na položaje, ko obstaja resna grožnja nacionalni varnosti, kot so tisti iz točk 135 in 136 te sodbe. Zato je bistveno, da je lahko sklep o odredbi ponudnikom elektronskih komunikacijskih storitev, da morajo izvajati tako hrambo podatkov, predmet učinkovitega nadzora s strani sodišča ali neodvisnega upravnega organa, katerega odločitev je zavezujoča, da se preveri obstoj enega od teh položajev ter spoštovanje pogojev in jamstev, ki morajo biti določeni.

– Zakonski ukrepi, s katerimi je za boj proti kriminalu in zaščito javne varnosti določena preventivna hramba podatkov o prometu in podatkov o lokaciji

140 Kar zadeva cilj preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj v skladu z načelom sorazmernosti, je mogoče zgolj z bojem proti hudemu kriminalu in preprečevanjem resnih groženj javni varnosti utemeljiti resne posege v temeljne pravice, določene s členoma 7 in 8 Listine, kakršne pomeni hramba podatkov o prometu in podatkov o lokaciji. Torej je mogoče s ciljem preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj na splošno utemeljiti izključno posege v navedene temeljne pravice, ki po naravi niso resni (glej v tem smislu sodbi z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 102, in z dne 2. oktobra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, točki 56 in 57, ter mnenje 1/15 (Sporazum PNR EU-Kanada) z dne 26. julija 2017, EU:C:2017:592, točka 149).

141 Nacionalna ureditev, ki določa splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji zaradi boja proti hudemu kriminalu, presega meje tistega, kar je nujno potrebno, in je ni mogoče šteti za upravičeno v demokratični družbi, kot to zahteva člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine (glej v tem smislu sodbo z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 107).

142 Glede na občutljivost informacij, ki jih je mogoče razbrati iz podatkov o prometu in podatkov o lokaciji, je namreč njihova zaupnost bistvena za pravico do spoštovanja zasebnega življenja. Torej je ob upoštevanju na eni strani odvračilnih učinkov, ki jih lahko ima hramba teh podatkov na uresničevanje temeljnih pravic, določenih s členoma 7 in 11 Listine, na katere se nanaša točka 118 te sodbe, na drugi strani pa teže posega, ki ga pomeni taka hramba, v demokratični družbi nujno, da je tak poseg – kot to določa sistem, vzpostavljen z Direktivo 2002/58 – izjema, ne pa pravilo, ter da teh podatkov ni mogoče hraniti sistematično in neprekinjeno. Ta ugotovitev velja tudi v zvezi s ciljema boja proti hudemu kriminalu in preprečevanja resnih groženj javni varnosti ter velikim pomenom, ki jima ga je treba priznati.

143 Poleg tega je Sodišče poudarilo, da ureditev, ki določa splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji, vključuje elektronske komunikacije praktično celotnega prebivalstva, brez razlikovanja, omejitve ali izjeme glede na zastavljeni cilj. Taka ureditev se v nasprotju z zahtevo, navedeno v točki 133 te sodbe, na splošno nanaša na vse osebe, ki uporabljajo elektronske komunikacijske storitve, ne da bi bile te osebe, čeprav posredno, v položaju, ki bi lahko privedel do kazenskega pregona. Uporablja se torej tudi za osebe, v zvezi s katerimi ni nobenega indica, na podlagi katerega bi bilo mogoče sklepati, da obstaja povezava, čeprav posredna ali daljna, med njihovim ravnanjem in tem ciljem boja proti hudim kaznivim dejanjem, ter zlasti ne da bi bila predvidena

povezava med podatki, katerih hramba je določena, in grožnjo za javno varnost (glej v tem smislu sodbi z dne 8. aprila 2014, Digital Rights Ireland in drugi, C-293/12 in C-594/12, EU:C:2014:238, točki 57 in 58, in z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 105).

144 Natančneje, kot je Sodišče že razsodilo, taka ureditev ni omejena na hrambo bodisi podatkov v zvezi s časovnim obdobjem in/ali geografskim območjem in/ali krogom oseb, ki so lahko tako ali drugače vpletene v hudo kaznivo dejanje, bodisi podatkov v zvezi z osebami, ki bi lahko iz drugih razlogov s tem, da bi se hranili njihovi podatki, prispevale k boju proti hudemu kriminalu (glej v tem smislu sodbi z dne 8. aprila 2014, Digital Rights, C-293/12 in C-594/12, EU:C:2014:238, točka 59, in z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 106).

145 Niti pozitivne obveznosti držav članic, ki bi lahko glede na primer izhajale iz členov 3, 4 oziroma 7 Listine in se nanašajo – kot je bilo navedeno v točkah 126 in 128 te sodbe – na določitev pravil, ki omogočajo učinkovit boj proti kaznivim dejanjem, ne morejo učinkovati tako, da bi utemeljevale tako resne posege v temeljne pravice, določene s členoma 7 in 8 Listine, kot jih vključuje ureditev, ki določa hrambo podatkov o prometu in podatkov o lokaciji za praktično celotno prebivalstvo, ne da bi lahko bila iz podatkov zadevnih oseb razvidna zveza, vsaj posredna, z zastavljenim ciljem.

146 Kot je bilo navedeno v točkah od 142 do 144 te sodbe in ob upoštevanju potrebne uskladitve med zadevnimi pravicami in interesi, pa lahko cilji boja proti hudemu kriminalu, preprečevanja resnih napadov na javno varnost in *a fortiori* zaščite nacionalne varnosti glede na pomen, ki ga imajo, in ob upoštevanju pozitivnih obveznosti, ki so navedene v prejšnji točki in na katere je napotilo zlasti Cour constitutionnelle (ustavno sodišče), upravičijo posebej resen poseg, ki ga pomeni ciljna hramba podatkov o prometu in podatkov o lokaciji.

147 Kot je Sodišče že razsodilo, člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine tako ne nasprotuje temu, da država članica sprejme ureditev, ki preventivno dopušča ciljno hrambo podatkov o prometu in podatkov o lokaciji zaradi boja proti hudemu kriminalu, preprečevanja resnih groženj za javno varnost in tudi zaščite nacionalne varnosti, pod pogojem, da se taka hramba glede kategorij hranjenih podatkov, zajetih komunikacijskih sredstev, zadevnih oseb in določenega trajanja hrambe omeji na to, kar je nujno potrebno (glej v tem smislu sodbo z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 108).

148 Kar zadeva omejitev, ki mora veljati za tak ukrep hrambe podatkov, jo je mogoče določiti zlasti glede na kategorije zadevnih oseb, saj člen 15(1) Direktive 2002/58 ne nasprotuje ureditvi, ki temelji na objektivnih elementih, na podlagi katerih je mogoče opredeliti osebe, katerih podatki o prometu in podatki o lokaciji lahko izkažejo zvezo, vsaj posredno, s hudimi kaznivimi dejanji, tako ali drugače prispevati k boju proti hudemu kriminalu ali preprečiti resno nevarnost za javno varnost ali nevarnost za nacionalno varnost (glej v tem smislu sodbo z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 111).

149 V zvezi s tem je treba pojasniti, da so lahko osebe, na katere se to nanaša, zlasti tiste, ki so bile v okviru nacionalnih postopkov, ki se uporabljajo, in na podlagi objektivnih elementov predhodno opredeljene kot osebe, ki predstavljajo grožnjo javni varnosti ali nacionalni varnosti zadevne države članice.

150 Omejitev ukrepa, ki določa hrambo podatkov o prometu in podatkov o lokaciji, lahko temelji tudi na geografskem merilu, kadar pristojni nacionalni organi na podlagi objektivnih in nediskriminatornih elementov menijo, da na enem ali več geografskih območjih obstaja položaj, za katerega je značilno visoko tveganje za pripravo ali izvršitev hudih kaznivih dejanj (glej v tem smislu sodbo z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 111). Taka območja so lahko zlasti kraji, za katere je značilno veliko število hudih kaznivih dejanj, kraji, posebej izpostavljeni storitvi hudih kaznivih dejanj, kot so kraji ali infrastrukture, ki jih redno obiskuje zelo veliko število ljudi, ali strateški kraji, kot so letališča, železniške postaje ali cestninska območja.

151 Da se zagotovi, da je poseg, ki ga pomenijo ukrepi ciljne hrambe, opisani v točkah od 147 do 150 te sodbe, skladen z načelom sorazmernosti, njihovo trajanje ne sme biti daljše od trajanja, ki je nujno potrebno z vidika zastavljenega cilja in okoliščin, ki jih upravičujejo, kar pa ne vpliva na morebitno podaljšanje zaradi nadaljnjega obstoja potrebe po taki hrambi.

– Zakonski ukrepi, s katerimi je za boj proti kriminalu in zaščito javne varnosti določena preventivna hramba naslovov IP in podatkov o civilni identiteti

152 Treba je ugotoviti, da se naslovi IP, čeprav spadajo med podatke o prometu, ustvarijo, ne da bi bili vezani na določeno komunikacijo, služijo pa predvsem temu, da se prek ponudnikov elektronskih komunikacijskih storitev identificira fizična oseba, ki je lastnik terminalske opreme, s katere je bila opravljena komunikacija prek interneta. Kar zadeva elektronsko pošto in internetno telefonijo, tako naslovi IP kot taki, če se hranijo samo naslovi IP vira komunikacije, ne pa tudi njenega prejemnika, ne razkrivajo nobene informacije o tretjih osebah, ki so bile v stiku z osebo, ki je vir komunikacije. Stopnja občutljivosti te kategorije podatkov je torej nižja od stopnje občutljivosti drugih podatkov o prometu.

153 Ker pa je naslove IP mogoče uporabiti zlasti za izčrpno sledenje brskanju, ki ga je opravil uporabnik interneta, in torej njegovim spletnim dejavnostim, ti podatki omogočajo izoblikovanje njegovega podrobnega profila. Tako hramba in analiza navedenih naslovov IP, ki sta potrebni za tako sledenje, pomenita resna posega v temeljne pravice uporabnika interneta, določene s členoma 7 in 8 Listine, ter imata lahko odvračilne učinke, kakršni so bili navedeni v točki 118 te sodbe.

154 Vendar je treba zaradi nujne uskladitve med zadevnimi pravicami in interesi, ki se zahteva s sodno prakso, navedeno v točki 130 te sodbe, upoštevati dejstvo, da je lahko v primeru kršitve, storjene na spletu, naslov IP edino preiskovalno sredstvo, ki omogoča identifikacijo osebe, ki ji je bil v času storitve tega kaznivega dejanja ta naslov dodeljen. K temu je treba še dodati, da hramba naslovov IP s strani ponudnikov elektronskih komunikacijskih storitev dalj časa, kot traja dodelitev teh podatkov, za namene zaračunavanja zadevnih storitev načeloma ni potrebna, zato se lahko – kot je v stališčih, predloženih Sodišču, navedlo več vlad – odkrivanje kaznivih dejanj, storjenih na spletu, brez uporabe zakonskega ukrepa v skladu s členom 15(1) Direktive 2002/58 izkaže za nemogoče. Kot so trdile te vlade, se to lahko zgodi zlasti v primeru posebej resnih kaznivih dejanj s področja otroške pornografije, kot so pridobivanje, razpošiljanje, posredovanje ali omogočanje spletnega dostopa do otroške pornografije v smislu člena 2(c) Direktive 2011/93/EU Evropskega parlamenta in Sveta z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ (UL 2011, L 335, str. 1).

155 V takih okoliščinah sicer drži, da bi se zakonski ukrep, ki določa hrambo naslovov IP vseh fizičnih oseb, ki so lastniki terminalske opreme, ki omogoča dostop do interneta, nanašal na osebe, ki na prvi pogled v smislu sodne prakse, navedene v točki 133 te sodbe, nimajo nikakršne zveze z zastavljenimi cilji, ter da imajo uporabniki interneta v skladu z ugotovitvami iz točke 109 te sodbe pravico v skladu s členoma 7 in 8 Listine pričakovati, da njihova identiteta načeloma ne bo razkrita, vendar zakonski ukrep, ki določa splošno in neselektivno hrambo zgolj naslovov IP, dodeljenih viru povezave, načeloma ni v nasprotju s členom 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine, če je za to možnost določeno strogo spoštovanje materialnih in postopkovnih pogojev, ki morajo urejati uporabo teh podatkov.

156 Ob upoštevanju resnosti posega v temeljne pravice, določene s členoma 7 in 8 Listine, ki ga pomeni ta hramba, je mogoče navedeni poseg upravičiti zgolj z bojem proti hudemu kriminalu in preprečevanjem resnih groženj javni varnosti, tako kot z zaščito nacionalne varnosti. Poleg tega trajanje hrambe ne sme biti daljše od tega, kar je nujno potrebno z vidika zastavljenega cilja. Nazadnje, pri tovrstnem ukrepu je treba določiti stroge pogoje in jamstva glede uporabe teh podatkov, zlasti s sledenjem, kar zadeva komunikacije in dejavnosti, ki so jih zadevne osebe opravile prek spleta.

157 Nazadnje, kar zadeva podatke v zvezi s civilno identiteto uporabnikov elektronskih komunikacijskih sredstev, ti sami zase ne omogočajo seznanitve z datumom, uro, trajanjem in prejemniki opravljenih komunikacij niti s kraji, kjer so bile te komunikacije opravljene, ali s pogostostjo komunikacij z določenimi osebami v danem obdobju, zato razen kontaktnih podatkov teh oseb, kot so njihovi naslovi, ne dajejo nobene informacije o danih komunikacijah in torej o zasebnem življenju teh oseb. Torej posega, ki ga pomeni hramba teh podatkov, načeloma ni mogoče opredeliti kot resnega (glej v tem smislu sodbo z dne 2. oktobra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, točki 59 in 60).

158 Iz tega sledi – v skladu z navedbami iz točke 140 te sodbe – da je mogoče zakonske ukrepe, katerih namen je obdelava teh podatkov kot takih, zlasti njihova hramba in dostop do njih zgolj za identifikacijo zadevnega uporabnika, ne da bi bilo mogoče te podatke povezati z informacijami o opravljenih komunikacijah, upravičiti s ciljem preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj na splošno, na katerega je napoteno v členu 15(1), prvi stavek, Direktive 2002/58 (glej v tem smislu sodbo z dne 2. oktobra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, točka 62).

159 V takih okoliščinah – ob upoštevanju potrebne uskladitve med zadevnimi pravicami in interesi ter iz razlogov, navedenih v točkah 131 in 158 te sodbe – je treba ugotoviti, da člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine tudi ob neobstoju zveze med vsemi uporabniki elektronskih komunikacijskih sredstev in zastavljenimi cilji ne nasprotuje zakonskemu ukrepu, ki ponudnikom elektronskih komunikacijskih storitev brez posebne časovne omejitve nalaga hrambo podatkov o civilni identiteti vseh uporabnikov elektronskih komunikacijskih sredstev za namene preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj ter zaščite javne varnosti, pri čemer ni potrebno, da so kazniva dejanja ali grožnje javni varnosti oziroma posegi vanjo resni.

– Zakonski ukrepi, s katerimi je za boj proti hudemu kriminalu določena takojšnja hramba podatkov o prometu in podatkov o lokaciji

160 Kar zadeva podatke o prometu in podatke o lokaciji, ki jih obdelujejo in hranijo ponudniki elektronskih komunikacijskih storitev na podlagi členov 5, 6 in 9 Direktive 2002/58 ali na podlagi zakonskih ukrepov, sprejetih v skladu s členom 15(1) te direktive, kot so opisani v točkah od 134 do 159 te sodbe, je treba ugotoviti, da je treba načeloma te podatke po izteku zakonskih rokov, v katerih morata biti v skladu z nacionalnimi določbami, s katerimi je prenesena ta direktiva, opravljeni njihova obdelava in hramba, glede na primer izbrisati ali anonimizirati.

161 Vendar lahko med to obdelavo in hrambo nastanejo položaji, ko se pojavi potreba po hrambi teh podatkov, daljši od navedenih rokov, da se tako razjasnijo huda kazniva dejanja ali posegi v nacionalno varnost, in sicer tako v položaju, ko je bilo ta kazniva dejanja ali te posege že mogoče ugotoviti, kot tudi v položaju, ko je mogoče po objektivni preučitvi vseh upoštevnih okoliščin na njihov obstoj razumno sumiti.

162 V zvezi s tem je treba ugotoviti, da Konvencija Sveta Evrope z dne 23. novembra 2001 o kibernetski kriminaliteti (serija evropskih pogodb – št. 185), ki jo je podpisalo vseh 27 držav članic, ratificiralo pa 25 med njimi, in katere cilj je poenostaviti boj proti kaznivim dejanjem, storjenim prek računalniških omrežij, v členu 14 določa, da pogodbenice za namene preiskav ali posebnih kazenskih postopkov sprejmejo nekatere ukrepe v zvezi z že shranjenimi podatki o prometu, kot je takojšnje zavarovanje teh podatkov. Natančneje, člen 16(1) te konvencije določa, da pogodbenice sprejmejo potrebne zakonske ukrepe, s katerimi pristojnim organom omogočijo, da odredijo ali drugače dosežejo takojšnje zavarovanje podatkov o prometu, ki so bili shranjeni z računalniškim sistemom, še zlasti kadar obstajajo razlogi za prepričanje, da bi se lahko ti podatki izgubili ali spremenili.

163 V položaju, na kakršnega se nanaša točka 161 te sodbe, lahko države članice ob upoštevanju potrebne uskladitve med zadevnimi pravicami in interesi, na katero se nanaša točka 130 te sodbe, v zakonodaji, sprejeti na podlagi člena 15(1) Direktive 2002/58, določijo možnost, da se s sklepom pristojnega organa, ki je predmet učinkovitega sodnega nadzora, ponudnikom elektronskih komunikacijskih storitev odredi, da za določen čas izvedejo takojšnjo hrambo podatkov o prometu in podatkov o lokaciji, s katerimi razpolagajo.

164 Ker se namen take takojšnje hrambe ne ujema več z nameni, za katere so bili podatki prvotno zbrani in shranjeni, in ker mora biti v skladu s členom 8(2) Listine kakršna koli obdelava podatkov izvedena za določene namene, morajo države članice v svoji zakonodaji navesti namen, za katerega je takojšnjo hrambo podatkov mogoče izvesti. Ob upoštevanju resnosti posega v temeljne pravice, določene s členoma 7 in 8 Listine, ki ga lahko taka hramba pomeni, je mogoče navedeni poseg upravičiti zgolj z bojem proti hudemu kriminalu in *a fortiori* z zaščito nacionalne varnosti. Poleg tega se mora, da se zagotovi, da je poseg, ki ga pomeni tovrstni ukrep, omejen na to, kar je nujno potrebno, po eni strani obveznost hrambe nanašati zgolj na podatke o prometu in podatke o lokaciji, ki bi lahko pripomogli k razjasnitvi hudega kaznivega dejanja ali posega v nacionalno varnost. Po drugi strani mora biti trajanje hrambe podatkov omejeno na to, kar je nujno potrebno, vendar ga je mogoče kljub vsemu podaljšati, če je to upravičeno z okoliščinami in ciljem, ki se mu sledi z navedenim ukrepom.

165 V zvezi s tem je treba pojasniti, da ni treba, da je taka takojšnja hramba omejena na podatke oseb, konkretno osumljenih storitve kaznivega dejanja ali napada na nacionalno varnost. Ob upoštevanju okvira, izoblikovanega s členom 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine, ter preudarkov, navedenih v točki 133 te sodbe, je mogoče tak ukrep glede na izbiro zakonodajalca in ob upoštevanju meja tega, kar je nujno potrebno, razširiti na podatke o prometu in podatke o lokaciji v zvezi s še drugimi osebami, ki niso osumljene načrtovanja ali storitve hudega kaznivega dejanja ali napada na nacionalno varnost, če lahko ti podatki na podlagi objektivnih in nediskriminatornih ciljev pripomorejo k razjasnitvi takega kaznivega dejanja ali takega napada na nacionalno varnost, na primer na podatke o žrtvi tega dejanja, o njenem socialnem ali poklicnem okolju ali o določenih geografskih območjih, kot so kraji storitve in priprave zadevnega kaznivega dejanja ali napada na nacionalno varnost. Poleg tega mora biti dostop pristojnih organov do tako shranjenih podatkov izveden ob upoštevanju pogojev, ki izhajajo iz sodne prakse, s katero je bila razložena Direktiva 2002/58 (glej v tem smislu sodbo z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točke od 118 do 121 in navedena sodna praksa).

166 Treba je še dodati, da je – kot je razvidno zlasti iz točk 115 in 133 te sodbe – dostop do podatkov o prometu in podatkov o lokaciji, ki jih hranijo ponudniki v skladu z ukrepom, sprejetim na podlagi člena 15(1) Direktive 2002/58, načeloma mogoče upravičiti zgolj s ciljem v splošnem interesu, za katerega je bila navedena hramba tem ponudnikom naložena. Iz tega predvsem izhaja, da dostopa do takih podatkov za pregon in kaznovanje običajnega kaznivega dejanja nikakor ni mogoče odobriti, kadar je bila njihova hramba upravičena s ciljem boja proti hudemu kriminalu ali *a fortiori* z zaščito nacionalne varnosti. V skladu z načelom sorazmernosti, kot je bilo pojasnjeno v točki 131 te sodbe, pa je mogoče dostop do podatkov, shranjenih za boj proti hudemu kriminalu, če so izpolnjeni materialni in postopkovni pogoji za tak dostop, navedeni v prejšnji točki, upravičiti s ciljem zaščite nacionalne varnosti.

167 V zvezi s tem lahko države članice v svoji zakonodaji določijo, da je dostop do podatkov o prometu in do podatkov o lokaciji ob upoštevanju istih materialnih in postopkovnih pogojev mogoč za boj proti hudemu kriminalu ali zaščito nacionalne varnosti, če jih je ponudnik shranil na način, skladen s členi 5, 6 in 9 ali členom 15(1) Direktive 2002/58.

168 Ob upoštevanju vseh navedenih preudarkov je treba na prvi vprašanji v zadevah C-511/18 in C-512/18 ter na prvo in drugo vprašanje v zadevi C-520/18 odgovoriti, da je treba člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine razlagati tako, da nasprotuje zakonskim

ukrepom, s katerimi je za namene iz tega člena 15(1) preventivno določena splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji. Navedeni člen 15(1) v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine pa ne nasprotuje zakonskim ukrepom, s katerimi je

– v položajih, ko se zadevna država članica spopada z resno grožnjo nacionalni varnosti, ki se izkaže za resnično in sedanjo ali predvidljivo, za zaščito nacionalne varnosti omogočena uporaba odredbe, s katero se ponudnikom elektronskih komunikacijskih storitev naloži splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji, pri čemer je sklep o tej odredbi lahko predmet učinkovitega nadzora s strani sodišča ali neodvisnega upravnega organa, katerega odločitev je zavezujoča, da se preveri obstoj enega od teh položajev ter spoštovanje pogojev in jamstev, ki morajo biti določeni, in je navedeni sklep mogoče izdati le za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, vendar ga je v primeru nadaljnjega obstoja te grožnje mogoče podaljšati;

– za zaščito nacionalne varnosti, boj proti hudemu kriminalu in preprečevanje resnih groženj javni varnosti za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, vendar ga je mogoče podaljšati, določena ciljna hramba podatkov o prometu in podatkov o lokaciji, ki je na podlagi objektivnih in nediskriminatornih elementov omejena glede na kategorije zadevnih oseb ali z geografskim merilom;

– za zaščito nacionalne varnosti, boj proti hudemu kriminalu in preprečevanje resnih groženj javni varnosti za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, določena splošna in neselektivna hramba naslovov IP, dodeljenih viru povezave;

– za zaščito nacionalne varnosti, boj proti kriminalu in zaščito javne varnosti določena splošna in neselektivna hramba podatkov o civilni identiteti uporabnikov elektronskih komunikacijskih sredstev ter

– za boj proti hudemu kriminalu in *a fortiori* za zaščito nacionalne varnosti omogočena uporaba odredbe, s katero je ponudnikom elektronskih komunikacijskih storitev prek sklepa pristojnega organa, ki je predmet učinkovitega sodnega nadzora, za določeno obdobje naložena takojšnja hramba podatkov o prometu in podatkov o lokaciji, s katerimi ti ponudniki storitev razpolagajo,

če je s temi ukrepi z jasnimi in natančnimi pravili zagotovljeno, da je hramba zadevnih podatkov pogojena s spoštovanjem zadevnih materialnih in postopkovnih pogojev ter da imajo zadevne osebe na voljo učinkovita jamstva proti tveganjem zlorabe.

Drugo in tretje vprašanje v zadevi C-511/18

169 Predložitveno sodišče z drugim in tretjim vprašanjem v zadevi C-511/18 v bistvu sprašuje, ali je treba člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine razlagati tako, da nasprotuje nacionalni ureditvi, ki ponudnikom elektronskih komunikacijskih storitev nalaga, da v svojih omrežjih izvajajo ukrepe, ki omogočajo, prvič, avtomatizirano analizo in zbiranje podatkov o prometu in podatkov o lokaciji v realnem času ter, drugič, zbiranje tehničnih podatkov, ki se nanašajo na lokacijo uporabljene terminalske opreme, v realnem času, vendar ne predvideva, da bi bile osebe, ki jih ta obdelava in to zbiranje zadevata, o tem obveščene.

170 Predložitveno sodišče pojasnjuje, da metode zbiranja informacij, določene s členi od L. 851-2 do L. 851-4 CSI, ne vključujejo posebne zahteve za ponudnike elektronskih komunikacijskih storitev, da morajo hraniti podatke o prometu in podatke o lokaciji. Kar natančneje zadeva avtomatizirano analizo, na katero se nanaša člen L. 851-3 CSI, to sodišče navaja, da je namen te obdelave odkrivanje povezav, ki bi lahko razkrile teroristično grožnjo, na podlagi v ta namen opredeljenih meril. Kar zadeva zbiranje v realnem času iz člena L. 851-2 CSI, navedeno sodišče ugotavlja, da se nanaša le na

eno ali več oseb, za katere je bilo predhodno ugotovljeno, da bi lahko bile povezane s teroristično grožnjo. Po navedbah istega sodišča je mogoče ti metodi uporabiti zgolj za preprečevanje terorizma ter se nanašata na podatke iz členov L. 851-1 in R. 851-5 CSI.

171 Uvodoma je treba pojasniti, da okoliščina, da v skladu s členom L. 851-3 CSI avtomatizirana analiza, določena s tem členom, kot taka ne omogoča identifikacije uporabnikov, katerih podatki se tako analizirajo, še ne preprečuje opredelitve takih podatkov kot „osebnih podatkov“. Ker namreč postopek, določen v odstavku IV iste določbe, v poznejši fazi omogoča identifikacijo osebe ali oseb, na katere se nanašajo podatki, katerih avtomatizirana analiza je razkrila, da bi lahko pomenile teroristično grožnjo, je mogoče vse osebe, katerih podatki so predmet avtomatizirane analize, na podlagi teh podatkov še vedno identificirati. V skladu z opredelitvijo osebnih podatkov iz člena 4(1) Uredbe 2016/679 so namreč informacije med drugim v zvezi z določljivim posameznikom osebni podatki.

Avtomatizirana analiza podatkov o prometu in podatkov o lokaciji

172 Iz člena L. 851-3 CSI je razvidno, da avtomatizirana analiza, določena v tem členu, v bistvu ustreza filtriranju vseh podatkov o prometu in podatkov o lokaciji, shranjenih pri ponudnikih elektronskih komunikacijskih storitev, ki ga ti izvedejo na zahtevo pristojnih nacionalnih organov in v skladu s parametri, ki so jih določili ti organi. Iz tega sledi, da se za vse podatke uporabnikov elektronskih komunikacijskih sredstev preveri, ali ustrezajo tem parametrom. Zato je treba šteti, da avtomatizirana analiza za zadevne ponudnike elektronskih komunikacijskih storitev pomeni, da morajo za račun pristojnega organa izvesti splošno in neselektivno obdelavo v obliki uporabe z avtomatiziranimi sredstvi v smislu člena 4(2) Uredbe 2016/679, v kar so zajeti vsi podatki o prometu in podatki o lokaciji vseh uporabnikov elektronskih komunikacijskih sredstev. Ta obdelava je neodvisna od poznejšega zbiranja podatkov v zvezi z osebami, identificiranimi na podlagi avtomatizirane analize, pri čemer je to zbiranje dovoljeno na podlagi člena L. 851-3(IV) CSI.

173 Nacionalna ureditev, ki dovoljuje tako avtomatizirano analizo podatkov o prometu in podatkov o lokaciji, odstopa od načelne obveznosti iz člena 5 Direktive 2002/58, da se zagotovi zaupnost elektronskih komunikacij in z njimi povezanih podatkov. Taka ureditev pomeni tudi poseg v temeljne pravice iz členov 7 in 8 Listine, ne glede na nadaljnjo uporabo teh podatkov. Nazadnje, navedena ureditev ima lahko v skladu s sodno prakso, navedeno v točki 118 te sodbe, odvračilne učinke na uresničevanje svobode izražanja, določene v členu 11 Listine.

174 Poleg tega je poseg, ki izhaja iz avtomatizirane analize podatkov o prometu in podatkov o lokaciji, kakršen je ta iz postopka v glavni stvari, še posebej resen, saj splošno in neselektivno zajema podatke oseb, ki uporabljajo elektronska komunikacijska sredstva. Ta ugotovitev še toliko bolj drži, kadar – kot to izhaja iz nacionalne ureditve iz postopka v glavni stvari – podatki, ki so predmet avtomatizirane analize, lahko razkrijejo naravo informacij, pregledanih na spletu. Poleg tega se taka avtomatizirana analiza uporablja na splošno za vse osebe, ki uporabljajo elektronska komunikacijska sredstva, in zato tudi za osebe, v zvezi s katerimi ni nobenega indica, na podlagi katerega bi bilo mogoče sklepati, da obstaja povezava, čeprav posredna ali daljna, med njihovimi ravnanji in terorističnimi dejavnostmi.

175 V zvezi z upravičenostjo takega poseganja je treba pojasniti, da zahteva iz člena 52(1) Listine, da mora biti kakršno koli omejevanje uresničevanja temeljnih pravic predpisano z zakonom, pomeni, da mora biti že v pravni podlagi, ki omogoča poseg v te pravice, opredeljen obseg omejitve uresničevanja zadevne pravice (glej v tem smislu sodbo z dne 16. julija 2020, Facebook Ireland in Schrems, C-311/18, EU:C:2020:559, točka 175 in navedena sodna praksa).

176 Poleg tega, da bi bila izpolnjena zahteva po sorazmernosti iz točk 130 in 131 te sodbe, v skladu s katero morajo biti odstopanja in omejitve pri varstvu osebnih podatkov strogo omejeni na tisto, kar je nujno potrebno, mora nacionalna ureditev, ki ureja dostop pristojnih organov do hranjenih podatkov o prometu in podatkov o lokaciji, izpolnjevati zahteve, ki izhajajo iz sodne prakse, navedene

v točki 132 te sodbe. Natančneje, taka ureditev ne more zgolj zahtevati, da dostop organov do podatkov ustreza cilju, ki mu sledi ta ureditev, temveč mora določati tudi materialne in postopkovne pogoje za to uporabo (glej po analogiji mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točka 192 in navedena sodna praksa).

177 V zvezi s tem je treba opozoriti, da lahko posebej resen poseg, ki ga pomeni splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji, na katero se nanašajo preudarki iz točk od 134 do 139 te sodbe, ter posebej resen poseg, ki ga pomeni avtomatizirana analiza teh podatkov, izpolnita zahtevo po sorazmernosti zgolj v položajih, ko se država članica spopada z resno grožnjo nacionalni varnosti, ki se izkaže za resnično in sedanjo ali predvidljivo, ter pod pogojem, da je trajanje te hrambe omejeno na to, kar je nujno potrebno.

178 V položajih, kot so ti iz prejšnje točke, je mogoče šteti, da je izvajanje avtomatizirane analize podatkov o prometu in podatkov o lokaciji vseh uporabnikov elektronskih komunikacijskih sredstev v strogo omejenem obdobju upravičeno glede na zahteve, ki izhajajo iz člena 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine.

179 Da pa se zagotovi, da je uporaba takega ukrepa dejansko omejena na to, kar je nujno potrebno za zaščito nacionalne varnosti in, natančneje, za preprečevanje terorizma, je v skladu z ugotovitvami iz točke 139 te sodbe bistveno, da je lahko sklep, s katerim se dovoli avtomatizirana analiza, predmet učinkovitega nadzora s strani sodišča ali neodvisnega upravnega organa, katerega odločitev je zavezujoča, da se preverita obstoj položaja, ki upravičuje navedeni ukrep, ter spoštovanje pogojev in jamstev, ki morajo biti določeni.

180 V zvezi s tem je treba pojasniti, da morajo biti predhodno določeni modeli in merila, na katerih temelji ta vrsta obdelave podatkov, na eni strani specifični in zanesljivi, da privedejo do rezultatov, na podlagi katerih je mogoče identificirati posameznike, glede katerih bi lahko bil podan utemeljen sum sodelovanja pri terorističnih kaznivih dejanjih, na drugi strani pa nediskriminatorni (glej v tem smislu mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017, EU:C:2017:592, točka 172).

181 Poleg tega je treba opozoriti, da bi bila vsakršna avtomatizirana analiza, izvedena po modelu in merilih, ki bi temeljili na postulatu, da bi bili lahko rasna ali etnična pripadnost, politična mnenja, verska ali filozofska prepričanja, sindikalna pripadnost, zdravstveno stanje ali spolno življenje osebe sami po sebi in neodvisno od posamičnega ravnanja te osebe upoštevni z vidika preprečevanja terorizma, v nasprotju s pravicami, zagotovljenimi s členoma 7 in 8 Listine v povezavi z njenim členom 21. Torej predhodno določeni modeli in merila za avtomatizirano analizo, katerih namen je preprečevanje terorističnih dejavnosti, ki pomenijo resno grožnjo nacionalni varnosti, ne morejo temeljiti zgolj na teh občutljivih podatkih (glej v tem smislu mnenje 1/15 (Sporazum PNR EU-Kanada) z dne 26. julija 2017, EU:C:2017:592, točka 165).

182 Ker poleg tega avtomatizirane analize podatkov o prometu in podatkov o lokaciji nujno vključujejo neko stopnjo napake, mora biti vsak pozitiven rezultat, pridobljen na podlagi avtomatizirane obdelave, predmet posamičnega pregleda z neavtomatiziranimi sredstvi, preden se sprejme posamični ukrep z negativnimi učinki na zadevne osebe, na primer poznejše zbiranje podatkov o prometu in podatkov o lokaciji v realnem času, saj tak ukrep namreč ne more odločilno temeljiti zgolj na rezultatu avtomatizirane obdelave. Prav tako bi morali biti – da bi se v praksi zagotovilo, da predhodno določeni modeli in merila, njihova uporaba ter uporabljene podatkovne baze niso diskriminatorni in da so omejeni na to, kar je nujno potrebno z vidika cilja preprečevanja terorističnih dejavnosti, ki pomenijo resno grožnjo nacionalni varnosti – zanesljivost in aktualnost teh predhodno določenih modelov in meril ter uporabljenih podatkovnih baz predmet rednih pregledov (glej v tem smislu mnenje 1/15 (Sporazum PNR EU-Kanada) z dne 26. julija 2017, EU:C:2017:592, točki 173 in 174).

Zbiranje podatkov o prometu in podatkov o lokaciji v realnem času

183 Kar zadeva zbiranje podatkov o prometu in podatkov o lokaciji v realnem času, na katero se nanaša člen L. 851-2 CSI, je treba ugotoviti, da je mogoče to posamično dovoliti v zvezi s „predhodno identificirano osebo, ki bi bila lahko povezana [s teroristično] grožnjo“. Prav tako je mogoče na podlagi te določbe, „[č]e obstajajo resni razlogi za sklepanje, da bi lahko ena ali več oseb, ki pripadajo okolju osebe, na katero se nanaša dovoljenje, zagotovile informacije za uresničitev cilja, s katerim je dovoljenje utemeljeno, […] tako dovoljenje posamično izdati za vsako od teh oseb“.

184 Podatki, ki so predmet tovrstnega ukrepa, pristojnim nacionalnim organom omogočajo, da v času veljavnosti dovoljenja neprekinjeno in v realnem času nadzirajo sogovornike, s katerimi zadevne osebe komunicirajo, sredstva, ki jih uporabljajo, trajanje komunikacij, ki jih imajo, ter njihove kraje prebivališča in gibanja. Prav tako lahko razkrijejo naravo informacij, pregledanih na spletu. Kot je razvidno iz točke 117 te sodbe, ti podatki, obravnavani kot celota, omogočajo izpeljati zelo natančne ugotovitve o zasebnem življenju zadevnih oseb in zagotavljajo sredstva za ugotavljanje njihovega profila, taka informacija pa je prav tako občutljiva z vidika pravice do spoštovanja zasebnega življenja kot sama vsebina komunikacij.

185 Kar zadeva zbiranje podatkov v realnem času, na katero se nanaša člen L. 851-4 CSI, ta določba omogoča zbiranje tehničnih podatkov o lokaciji terminalske opreme in prenos službi predsednika vlade v realnem času. Taki podatki pristojni službi kadar koli v času veljavnosti dovoljenja omogočajo, da neprekinjeno in v realnem času določi lokacijo uporabljene terminalske opreme, na primer mobilnih telefonov.

186 Nacionalna ureditev, ki dovoljuje taka zbiranja v realnem času, podobno kot tista, ki dovoljuje avtomatizirano analizo podatkov, odstopa od načelne obveznosti iz člena 5 Direktive 2002/58, da se zagotovi zaupnost elektronskih komunikacij in z njimi povezanih podatkov. Torej tudi ta ureditev pomeni poseg v temeljne pravice, določene s členoma 7 in 8 Listine, ter lahko ima odvračilne učinke na uresničevanje svobode izražanja, zagotovljene v členu 11 Listine.

187 Treba je poudariti, da je poseg, ki ga pomeni zbiranje podatkov, ki omogočajo lokalizacijo terminalske opreme, v realnem času, še posebej resen, saj pristojni nacionalni organi s temi podatki pridobijo sredstvo za natančno in stalno spremljanje gibanja uporabnikov mobilnih telefonov. Ker je treba te podatke obravnavati kot posebej občutljive, je treba dostop pristojnih organov do takih podatkov v realnem času razlikovati od naknadnega dostopa do njih, saj je prvonavedeni bolj invaziven, ker omogoča praktično popoln nadzor nad temi uporabniki (glej po analogiji, kar zadeva člen 8 EKČP, ESČP, 8. februar 2018, Ben Faiza proti Franciji, CE:ECHR:2018:0208JUD003144612, točka 74). Intenzivnost tega posega je še večja, če zbiranje v realnem času zajema tudi podatke o prometu zadevnih oseb.

188 Čeprav je mogoče glede na velik pomen cilja preprečevanja terorizma, zastavljenega z nacionalno ureditvijo iz postopka v glavni stvari, s tem ciljem utemeljiti poseg, ki ga pomeni zbiranje podatkov o prometu in podatkov o lokaciji v realnem času, je mogoče tak ukrep ob upoštevanju njegove posebno invazivne narave izvesti samo glede oseb, za katere obstaja veljaven razlog za sum, da so tako ali drugače vpletene v teroristične dejavnosti. Kar zadeva podatke oseb, ki ne spadajo v to kategorijo, so lahko predmet le naknadnega dostopa, pri čemer lahko do tega dostopa v skladu s sodno prakso Sodišča pride le v posebnih okoliščinah, kot so tiste, v katerih gre za teroristične dejavnosti, in kadar obstajajo objektivni elementi, na podlagi katerih je mogoče šteti, da bi ti podatki lahko v konkretnem primeru učinkovito prispevali k boju proti terorizmu (glej v tem smislu sodbo z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 119 in navedena sodna praksa).

189 Poleg tega mora sklep o dovoljenju za zbiranje podatkov o prometu in podatkov o lokaciji v realnem času temeljiti na objektivnih merilih, določenih v nacionalni zakonodaji. Natančneje, v tej zakonodaji morajo biti v skladu s sodno prakso, navedeno v točki 176 te sodbe, navedene okoliščine, v katerih je

mogoče tako zbiranje dovoliti, in določeni pogoji za to, hkrati pa mora biti v njej določeno – kot je bilo pojasnjeno v prejšnji točki – da se lahko uporablja samo za osebe, ki so objektivno povezane s ciljem preprečevanja terorizma. Poleg tega mora sklep o dovoljenju za zbiranje podatkov o prometu in podatkov o lokaciji v realnem času temeljiti na objektivnih in nediskriminatornih merilih, določenih v nacionalni zakonodaji. Da bi se v praksi zagotovilo spoštovanje teh pogojev, je bistveno, da je izvajanje ukrepa, s katerim je dovoljeno zbiranje podatkov v realnem času, predmet predhodnega nadzora, ki ga izvaja sodišče ali neodvisen upravni organ, katerega odločitev je zavezujoča, pri čemer se mora to sodišče ali organ zlasti prepričati, da je takšno zbiranje podatkov v realnem času dovoljeno samo v mejah tega, kar je nujno potrebno (glej v tem smislu sodbo z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 120). V nujnem in ustrezno utemeljenem primeru se mora nadzor izvesti v najkrajšem možnem času.

Obvestitev oseb, katerih podatki so bili zbrani ali analizirani

190 Pomembno je, da pristojni nacionalni organi, ki v realnem času zbirajo podatke o prometu in podatke o lokaciji, v okviru veljavnih nacionalnih postopkov o tem obvestijo zadevne osebe, če in takoj ko ta obvestitev ne more ogroziti preiskav, ki jih ti organi vodijo. Ta obvestitev je namreč dejansko nujna, da te osebe lahko uveljavljajo pravice, ki zanje izhajajo iz členov 7 in 8 Listine, da lahko zahtevajo dostop do svojih osebnih podatkov, ki so predmet teh ukrepov, in po potrebi njihov popravek ali izbris, ter da lahko v skladu s členom 47, prvi odstavek, Listine vložijo učinkovito pravno sredstvo pred sodiščem, pri čemer je taka pravica izrecno zagotovljena tudi s členom 15(2) Direktive 2002/58 v povezavi s členom 79(1) Uredbe 2016/679 (glej v tem smislu sodbo z dne 21. decembra 2016, Tele2, C-203/15 in C-698/15, EU:C:2016:970, točka 121 in navedena sodna praksa, ter mnenje 1/15 (Sporazum PNR EU-Kanada) z dne 26. julija 2017, EU:C:2017:592, točki 219 in 220).

191 Kar zadeva obvestitev, ki se zahteva v okviru avtomatizirane analize podatkov o prometu in podatkov o lokaciji, mora pristojni nacionalni organ objaviti splošne informacije o tej analizi, ne da bi moral zadevne osebe individualno obvestiti. V primeru, da podatki ustrezajo parametrom, opredeljenim v ukrepu, s katerim je dovoljena avtomatizirana analiza, in ta organ zadevno osebo identificira za bolj poglobljeno analizo podatkov, ki se nanašajo nanjo, pa je individualna obvestitev te osebe nujna. Vendar lahko do take obvestitve pride le, če in takoj ko ta ne more ogroziti nalog, ki jih opravlja navedeni organ (glej po analogiji mnenje 1/15 (Sporazum PNR EU-Kanada) z dne 26. julija 2017, EU:C:2017:592, točke od 222 do 224).

192 Ob upoštevanju vseh navedenih preudarkov je treba na drugo in tretje vprašanje v zadevi C-511/18 odgovoriti, da je treba člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine razlagati tako, da ne nasprotuje nacionalni ureditvi, s katero je ponudnikom elektronskih komunikacijskih storitev naloženo, prvič, da avtomatizirano analizirajo in v realnem času zbirajo med drugim podatke o prometu in podatke o lokaciji ter, drugič, da v realnem času zbirajo tehnične podatke o lokaciji uporabljene terminalske opreme, če

– je uporaba avtomatizirane analize omejena na položaje, ko se zadevna država članica spopada z resno grožnjo nacionalni varnosti, ki se izkaže za resnično in sedanjo ali predvidljivo, in je uporaba te analize lahko predmet učinkovitega nadzora s strani sodišča ali neodvisnega upravnega organa, katerega odločitev je zavezujoča, da se preveri obstoj položaja, ki upravičuje navedeni ukrep, ter spoštovanje pogojev in jamstev, ki morajo biti določeni, ter če

– je uporaba zbiranja podatkov o prometu in podatkov o lokaciji v realnem času omejena na osebe, v zvezi s katerimi obstaja utemeljen razlog za sum, da so tako ali drugače vpletene v teroristične dejavnosti, in je predmet predhodnega nadzora, ki ga opravi sodišče ali neodvisen upravni organ, katerega odločitev je zavezujoča, da se zagotovi, da je takšno zbiranje v realnem času dovoljeno samo v mejah tega, kar je nujno potrebno. V nujnem in ustrezno utemeljenem primeru se mora nadzor izvesti v najkrajšem možnem času.

Drugo vprašanje v zadevi C-512/18

193 Z drugim vprašanjem v zadevi C-512/18 želi predložitveno sodišče v bistvu izvedeti, ali je treba določbe Direktive 2000/31 v povezavi s členi od 6 do 8 in 11 ter členom 52(1) Listine razlagati tako, da nasprotujejo nacionalni ureditvi, ki ponudnikom dostopa do javnih spletnih komunikacijskih storitev in ponudnikom storitev gostovanja nalaga splošno in neselektivno hrambo med drugim osebnih podatkov v zvezi s temi storitvami.

194 Predložitveno sodišče, ki meni, da take storitve spadajo na področje uporabe Direktive 2000/31, ne pa Direktive 2002/58, je mnenja, da člen 15(1) in (2) Direktive 2000/31 v povezavi s členoma 12 in 14 te direktive sam zase ne določa načelne prepovedi hrambe podatkov v zvezi z ustvarjanjem vsebine, od katere bi bilo mogoče odstopiti le izjemoma. To sodišče se kljub vsemu glede na nujno spoštovanje temeljnih pravic, določenih v členih od 6 do 8 in 11 Listine, sprašuje, ali je treba to presojo uporabiti.

195 Poleg tega predložitveno sodišče še pojasnjuje, da se njegovo vprašanje nanaša na obveznost hrambe, določeno v členu 6 LCEN v povezavi z odlokom št. 2011-219. Podatki, ki jih morajo ponudniki zadevnih storitev hraniti iz tega naslova, vključujejo zlasti podatke o civilni identiteti oseb, ki uporabljajo te storitve, kot so njihov priimek, ime, povezani poštni naslovi, naslovi elektronske pošte ali povezani računi, njihova gesla in – kadar je sklenitev pogodbe ali odprtje računa odplačno – vrsta uporabljenega plačila, referenca plačila, znesek ter datum in ura transakcije.

196 Prav tako podatki, za katere velja obveznost hrambe, vključujejo identifikatorje naročnikov, povezav in uporabljene terminalske opreme, identifikatorje, dodeljene vsebini, datume in ure začetka in konca povezave in dejanj ter vrste protokolov, uporabljenih za povezavo s storitvijo in za prenos vsebin. Dostop do teh podatkov, katerih hramba traja eno leto, je mogoče zahtevati v okviru kazenskih in civilnih postopkov zaradi zagotovitve spoštovanja pravil v zvezi s civilno ali kazensko odgovornostjo ter v okviru ukrepov zbiranja informacij, za katere se uporablja člen L. 851-1 CSI.

197 V zvezi s tem je treba ugotoviti, da Direktiva 2000/31 v skladu z njenim členom 1(2) usklajuje nekatere nacionalne določbe, ki se uporabljajo za storitve informacijske družbe, na katere se nanaša člen 2(a) te direktive.

198 Take storitve sicer res zajemajo storitve, ki se opravljajo na daljavo z uporabo naprav za elektronsko obdelavo in shranjevanje podatkov, na posamezno zahtevo prejemnika storitev in običajno za plačilo, kakršne so storitve dostopa do interneta ali komunikacijskega omrežja ter storitve gostovanja (glej v tem smislu sodbe z dne 24. novembra 2011, Scarlet Extended, C-70/10, EU:C:2011:771, točka 40; z dne 16. februarja 2012, SABAM, C-360/10, EU:C:2012:85, točka 34; z dne 15. septembra 2016, Mc Fadden, C-484/14, EU:C:2016:689, točka 55, ter z dne 7. avgusta 2018, SNB-REACT, C-521/17, EU:C:2018:639, točka 42 in navedena sodna praksa).

199 Vendar člen 1(5) Direktive 2000/31 določa, da se ta direktiva ne uporablja za vprašanja v zvezi s storitvami informacijske družbe, ki jih zajemata direktivi 95/46 in 97/66. V zvezi s tem je iz uvodnih izjav 14 in 15 Direktive 2000/31 razvidno, da varstvo zaupnosti komunikacij in posameznikov pri obdelavi osebnih podatkov v okviru storitev informacijske družbe urejata izključno direktivi 95/46 in 97/66, pri čemer zadnjenavedena v členu 5 za namene varstva zasebnosti komunikacij prepoveduje kakršno koli obliko prestrezanja ali nadzora komunikacij.

200 Tako je treba vprašanja, povezana z varstvom zaupnosti komunikacij in osebnih podatkov presojati ob upoštevanju Direktive 2002/58 in Uredbe 2016/679, ki sta nadomestili Direktivo 97/66 oziroma Direktivo 95/46, pri čemer je treba pojasniti, da varstvo, ki ga želi zagotoviti Direktiva 2000/31, nikakor ne more posegati v zahteve, ki izhajajo iz Direktive 2002/58 in Uredbe 2016/679 (glej v tem smislu sodbo z dne 29. januarja 2008, Promusicae, C-275/06, EU:C:2008:54, točka 57).

201 Obveznost, naloženo z nacionalno ureditvijo, navedeno v točki 195 te sodbe, v skladu s katero morajo ponudniki dostopa do javnih spletnih komunikacijskih storitev in ponudniki storitev gostovanja hraniti osebne podatke v zvezi s temi storitvami, je treba torej – kot je navedel generalni pravobranilec v točki 141 sklepnih predlogov v združenih zadevah La Quadrature du Net in drugi (C-511/18 in C-512/18, EU:C:2020:6) – presojati ob upoštevanju Direktive 2002/58 ali Uredbe 2016/679.

202 Tako bo zagotavljanje storitev, zajetih s to nacionalno ureditvijo, glede na to, ali spada na področje uporabe Direktive 2002/58 ali ne, urejeno bodisi z zadnjenavedeno direktivo, zlasti z njenim členom 15(1) v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine, bodisi z Uredbo 2016/679, zlasti z njenim členom 23(1) v povezavi z istimi določbami Listine.

203 Kot je navedla Evropska komisija v pisnem stališču, v obravnavani zadevi ni mogoče izključiti, da so nekatere storitve, na katere se nanaša nacionalna ureditev, navedena v točki 195 te sodbe, elektronske komunikacijske storitve v smislu Direktive 2002/58, kar mora preveriti predložitveno sodišče.

204 V zvezi s tem je treba poudariti, da Direktiva 2002/58 zajema elektronske komunikacijske storitve, ki izpolnjujejo pogoje iz člena 2(c) Direktive 2002/21, na katerega je napoteno v členu 2 Direktive 2002/58 in ki opredeljuje elektronsko komunikacijsko storitev kot „storitev, ki se navadno opravlja za plačilo in je v celoti ali pretežno sestavljena iz prenosa signalov po elektronskih komunikacijskih omrežjih ter vključuje telekomunikacijske storitve in storitve prenosa po omrežjih, ki se uporabljajo za radiodifuzijo“. Kar zadeva storitve informacijske družbe, kakršne so navedene v točkah 197 in 198 te sodbe in so zajete z Direktivo 2000/31, so to storitve informacijske družbe, saj so v celoti ali pretežno sestavljene iz prenosa signalov po elektronskih komunikacijskih omrežjih (glej v tem smislu sodbo z dne 5. junija 2019, Skype Communications, C-142/18, EU:C:2019:460, točki 47 in 48).

205 Tako so storitve dostopa do interneta, za katere se zdi, da so zajete z nacionalno ureditvijo iz točke 195 te sodbe, kot potrjuje uvodna izjava 10 Direktive 2002/21, elektronske komunikacijske storitve v smislu te direktive (glej v tem smislu sodbo z dne 5. junija 2019, Skype Communications, C-142/18, EU:C:2019:460, točka 37). Enako velja za internetne storitve elektronske pošte, za katere se ne zdi izključeno, da prav tako spadajo na področje uporabe te nacionalne ureditve, saj na tehnični ravni v celoti ali pretežno vključujejo prenos signalov po elektronskih komunikacijskih omrežjih (glej v tem smislu sodbo z dne 13. junija 2019, Google, C-193/18, EU:C:2019:498, točki 35 in 38).

206 Kar zadeva zahteve, ki izhajajo iz člena 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine, je treba napotiti na vse ugotovitve in presoje v okviru odgovora, danega na prvi vprašanji v zadevah C-511/18 in C-512/18 ter na prvo in drugo vprašanje v zadevi C-520/18.

207 Kar zadeva zahteve, ki izhajajo iz Uredbe 2016/679, je treba opozoriti, da je njen namen zlasti – kot je razvidno iz njene uvodne izjave 10 – zagotoviti visoko raven varstva posameznikov v Uniji ter v ta namen zagotoviti dosledno in enotno uporabo pravil za varstvo temeljnih svoboščin in pravic teh posameznikov pri obdelavi osebnih podatkov v celotni Uniji (glej v tem smislu sodbo z dne 16. julija 2020, Facebook Ireland in Schrems, C-311/18, EU:C:2020:559, točka 101).

208 V ta namen mora vsaka obdelava osebnih podatkov – s pridržkom odstopanj, dovoljenih v členu 23 Uredbe 2016/679 – spoštovati načela, ki urejajo obdelave osebnih podatkov, in pravice zadevnih oseb, navedene v poglavjih II oziroma III te uredbe. Natančneje, vsaka obdelava osebnih podatkov mora, prvič, biti v skladu z načeli iz člena 5 navedene uredbe in, drugič, ustrezati pogojem za zakonitost, navedenim v členu 6 iste uredbe (glej po analogiji, kar zadeva Direktivo 95/46, sodbo z dne 30. maja 2013, Worten, C-342/12, EU:C:2013:355, točka 33 in navedena sodna praksa).

209 Kar natančneje zadeva člen 23(1) Uredbe 2016/679, je treba ugotoviti, da ta člen po zgledu določb člena 15(1) Direktive 2002/58 državam članicam omogoča, da ob upoštevanju namenov, ki jih določa, in z zakonskimi ukrepi omejijo obseg obveznosti in pravic, na katere se nanaša, „če taka omejitev

spoštuje bistvo temeljnih pravic in svoboščin ter je potreben in sorazmeren ukrep v demokratični družbi za zagotavljanje“ zastavljenega cilja. Vsak zakonski ukrep, sprejet na tej podlagi, mora zlasti izpolnjevati posebne zahteve, določene v členu 23(2) te uredbe.

210 Tako člena 23(1) in (2) Uredbe 2016/679 ni mogoče razlagati tako, da državam članicam daje pooblastilo za poseganje v spoštovanje zasebnega življenja v nasprotju s členom 7 Listine in v druga z Listino določena jamstva (glej po analogiji, kar zadeva Direktivo 95/46, sodbo z dne 20. maja 2003, Österreichischer Rundfunk in drugi, C-465/00, C-138/01 in C-139/01, EU:C:2003:294, točka 91). Zlasti je mogoče po zgledu tistega, kar velja za člen 15(1) Direktive 2002/58, pristojnost, ki je s členom 23(1) Uredbe 2016/679 podeljena državam članicam, izvajati le ob upoštevanju zahteve po sorazmernosti, v skladu s katero je treba odstopanja od varstva osebnih podatkov in njihove omejitve določiti v mejah tega, kar je nujno potrebno (glej po analogiji, kar zadeva Direktivo 95/46, sodbo z dne 7. novembra 2013, IPI, C-473/12, EU:C:2013:715, točka 39 in navedena sodna praksa).

211 Iz tega sledi, da se ugotovitve in presoje iz okvira odgovora, danega na prvi vprašanji v zadevah C-511/18 in C-512/18 ter na prvo in drugo vprašanje v zadevi C-520/18, *mutatis mutandis* uporabljajo tudi za člen 23 Uredbe 2016/679.

212 Glede na zgoraj navedeno je treba na drugo vprašanje v zadevi C-512/18 odgovoriti, da je treba Direktivo 2000/31 razlagati tako, da se na področju varstva zaupnosti sporočil in varstva posameznikov pri obdelavi osebnih podatkov v okviru storitev informacijske družbe ne uporablja, saj je to varstvo glede na primer urejeno z Direktivo 2002/58 ali z Uredbo 2016/679. Člen 23(1) Uredbe 2016/679 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine je treba razlagati tako, da nasprotuje nacionalni ureditvi, s katero je ponudnikom dostopa do javnih spletnih komunikacijskih storitev in ponudnikom storitev gostovanja naložena splošna in neselektivna hramba med drugim osebnih podatkov v zvezi s temi storitvami.

Tretje vprašanje v zadevi C-520/18

213 S tretjim vprašanjem v zadevi C-520/18 želi predložitveno sodišče v bistvu izvedeti, ali lahko nacionalno sodišče uporabi določbo nacionalnega prava, na podlagi katere lahko časovno omeji učinke ugotovitve nezakonitosti, ki jo mora sprejeti na podlagi tega prava v zvezi z nacionalno ureditvijo, s katero je ponudnikom elektronskih komunikacijskih storitev za – med drugim – zaščito nacionalne varnosti in boj proti kriminalu naložena splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji, ki ni združljiva s členom 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine.

214 Načelo primarnosti prava Unije določa prednost prava Unije pred pravom držav članic. To načelo zato vsem organom držav članic nalaga, da različnim predpisom Unije zagotovijo polni učinek, pri čemer pravo držav članic ne more vplivati na učinek, ki je tem različnim predpisom priznan na ozemlju navedenih držav (sodbi z dne 15. julija 1964, Costa, 6/64, EU:C:1964:66, str. 1159 in 1160, ter z dne 19. novembra 2019, A. K. in drugi (Neodvisnost disciplinskega senata vrhovnega sodišča), C-585/18, C-624/18 in C-625/18, EU:C:2019:982, točki 157 in 158 ter navedena sodna praksa).

215 Če nacionalno sodišče, ki v okviru svojih pristojnosti uporablja določbe prava Unije, ne more podati razlage nacionalne ureditve, ki bi bila skladna z zahtevami prava Unije, ima na podlagi načela primarnosti dolžnost zagotoviti polni učinek teh določb, pri čemer lahko po potrebi po uradni dolžnosti odloči, da ne bo uporabilo neskladne določbe nacionalne zakonodaje, tudi poznejše, ne da bi mu bilo treba zahtevati ali čakati na predhodno odpravo te določbe po zakonodajni poti ali kakšnem drugem ustavnem postopku (sodbe z dne 22. junija 2010, Melki in Abdeli, C-188/10 in C-189/10, EU:C:2010:363, točka 43 in navedena sodna praksa; z dne 24. junija 2019, Popławski, C-573/17, EU:C:2019:530, točka 58, in z dne 19. novembra 2019, A. K. in drugi (Neodvisnost disciplinskega senata vrhovnega sodišča), C-585/18, C-624/18 in C-625/18, EU:C:2019:982, točka 160).

216 Le Sodišče lahko izjemoma in iz nujnih razlogov pravne varnosti prizna začasno odložitev učinka izrinjenja, ki ga ima pravilo prava Unije v razmerju do nacionalnega prava, ki je v nasprotju z njim. Tako časovno omejitev učinkov razlage tega prava, ki jo je podalo Sodišče, je mogoče priznati le v sodbi, s katero se odloči o zahtevani razlagi (glej v tem smislu sodbe z dne 23. oktobra 2012, Nelson in drugi, C-581/10 in C-629/10, EU:C:2012:657, točki 89 in 91; z dne 23. aprila 2020, Herst, C-401/18, EU:C:2020:295, točki 56 in 57, in z dne 25. junija 2020, A in drugi (Vetrne elektrarne v občinah Aalter in Nevele), C-24/19, EU:C:2020:503, točka 84 in navedena sodna praksa).

217 Če bi bila nacionalna sodišča pristojna, da nacionalnim določbam priznajo prednost pred pravom Unije, ki ga te določbe kršijo, četudi samo začasno, bi to poseglo v primarnost in enotno uporabo prava Unije (glej v tem smislu sodbo z dne 29. julija 2019, Inter-Environnement Wallonie in Bond Beter Leefrice Vlaanderen, C-411/17, EU:C:2019:622, točka 177 in navedena sodna praksa).

218 Vendar je Sodišče v zadevi, v kateri je bila obravnavana zakonitost ukrepov, sprejetih v nasprotju z obveznostjo, ki jo določa pravo Unije, da se opravi predhodna presoja vplivov projekta na okolje in na zavarovano območje, razsodilo, da lahko nacionalno sodišče, če to dopušča nacionalno pravo, izjemoma ohrani učinke takih ukrepov, če to ohranitev upravičujejo nujni razlogi, povezani s potrebo po odpravi dejanske in resne grožnje prekinitve oskrbe z električno energijo zadevne države članice, ki je ni mogoče odpraviti z drugimi sredstvi in alternativami, zlasti v okviru notranjega trga, pri čemer lahko ta ohranitev zajema le obdobje, ki je nujno potrebno za odpravo te nezakonitosti (glej v tem smislu sodbo z dne 29. julija 2019, Inter-Environnement Wallonie in Bond Beter Leefrice Vlaanderen, C-411/17, EU:C:2019:622, točke 175, 176, 179 in 181).

219 Vendar drugače kot pri opustitvi postopkovne obveznosti, kakršna je predhodna presoja vplivov projekta na posebnem področju varstva okolja, kršitve člena 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine ni mogoče regularizirati prek postopka, primerljivega s tistim, navedenim v prejšnji točki. Ohranitev učinkov nacionalne zakonodaje, kakršna je ta iz postopka v glavni stvari, bi namreč pomenila, da ta zakonodaja ponudnikom elektronskih komunikacijskih storitev še naprej nalaga obveznosti, ki so v nasprotju s pravom Unije in ki vključujejo resne posege v temeljne pravice oseb, katerih podatki so bili shranjeni.

220 Zato predložitveno sodišče ne sme uporabiti določbe svojega nacionalnega prava, na podlagi katere lahko časovno omeji učinke ugotovitve nezakonitosti, ki jo mora sprejeti na podlagi tega prava v zvezi z nacionalno ureditvijo iz postopka v glavni stvari.

221 Ob tem pa VZ, WY in XX v stališčih, ki so jih predložili Sodišču, trdijo, da tretje vprašanje implicitno, vendar nujno sproža vprašanje, ali pravo Unije nasprotuje temu, da se v okviru kazenskega postopka uporabijo informacije in dokazi, pridobljeni s splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji, nezdružljivo s tem pravom.

222 V zvezi s tem je treba, da bi predložitvenemu sodišču dali koristen odgovor, opozoriti, da je v trenutnem stanju prava Unije načeloma v izključni pristojnosti nacionalnega prava, da določi pravila v zvezi z dopustnostjo in presojo informacij in dokazov, pridobljenih s tako hrambo podatkov, ki je v nasprotju s pravom Unije, v kazenskem postopku zoper osebe, osumljene hudih kaznivih dejanj.

223 Iz ustaljene sodne prakse namreč izhaja, da mora, kadar neko področje ni urejeno s predpisi Unije, notranji pravni red posamezne države članice v skladu z načelom procesne avtonomije določiti postopkovna pravila za uveljavljanje pravnih sredstev pred sodišči, katerih namen je varstvo pravic, ki jih posameznikom daje pravo Unije, vendar pod pogojem, da ta pravila niso manj ugodna od tistih, ki urejajo podobne položaje v nacionalnem pravu (načelo enakovrednosti), in da v praksi ne onemogočajo ali pretirano otežujejo uresničevanja pravic, ki jih podeljuje pravo Unije (načelo učinkovitosti) (glej v tem smislu sodbe z dne 6. oktobra 2015, Târşia, C-69/14, EU:C:2015:662, točki 26 in 27; z dne 24. oktobra 2018, XC in drugi, C-234/17, EU:C:2018:853, točki 21 in 22 ter navedena sodna praksa, in z dne 19. decembra 2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, točka 33).

224 Kar zadeva načelo enakovrednosti, mora nacionalno sodišče, ki odloča v kazenskem postopku, ki temelji na informacijah ali dokazih, pridobljenih v nasprotju z zahtevami, ki izhajajo iz Direktive 2002/58, preveriti, ali nacionalno pravo, ki ureja ta postopek, določa manj ugodna pravila, kar zadeva dopustnost in uporabo takih informacij in takih dokazov, kot so pravila, ki urejajo informacije in dokaze, pridobljene v nasprotju z nacionalnim pravom.

225 Kar zadeva načelo učinkovitosti, je treba poudariti, da je namen nacionalnih pravil v zvezi z dopustnostjo in uporabo informacij in dokazov – glede na izbire, opravljene v nacionalnem pravu – preprečiti, da bi nezakonito pridobljene informacije in dokazi neupravičeno škodovali osebi, osumljeni storitve kaznivih dejanj. Vendar je mogoče ta cilj – odvisno od nacionalnega prava – doseči ne le s prepovedjo uporabe takih informacij in dokazov, ampak tudi z nacionalnimi pravili in praksami, ki urejajo presojo in ponderiranje informacij in dokazov, ali celo z upoštevanjem njihove nezakonitosti pri določanju kazni.

226 Iz sodne prakse Sodišča pa je razvidno, da je treba o nujnosti izključitve informacij in dokazov, pridobljenih v nasprotju z določbami prava Unije, presojati zlasti z vidika tveganja, ki ga ima dopustnost takih informacij in dokazov za spoštovanje načela kontradiktornosti in zato za pravico do poštenega sojenja (glej v tem smislu sodbo z dne 10. aprila 2003, Steffensen, C-276/01, EU:C:2003:228, točki 76 in 77). Tako mora sodišče, ki meni, da stranka ne more učinkovito podati stališča o dokaznem sredstvu, ki izvira s področja, na katero se sodišče ne spozna, in ki lahko bistveno vpliva na presojo dejanskega stanja, ugotoviti kršitev pravice do poštenega sojenja in tako dokazno sredstvo izključiti, da se taka kršitev prepreči (glej v tem smislu sodbo z dne 10. aprila 2003, Steffensen, C-276/01, EU:C:2003:228, točki 78 in 79).

227 Zato načelo učinkovitosti nacionalnemu kazenskemu sodišču narekuje, da v okviru kazenskega postopka zoper osebe, osumljene kaznivih dejanj, zavrne informacije in dokaze, pridobljene s splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji, ki ni združljiva s pravom Unije, če te osebe ne morejo učinkovito podati stališča o teh informacijah in dokazih, ki izvirajo s področja, na katero se sodišče ne spozna, in ki lahko bistveno vplivajo na presojo dejanskega stanja.

228 Ob upoštevanju navedenih preudarkov je treba na tretje vprašanje v zadevi C-520/18 odgovoriti, da nacionalno sodišče ne more uporabiti določbe nacionalnega prava, na podlagi katere lahko časovno omeji učinke ugotovitve nezakonitosti, ki jo mora sprejeti na podlagi tega prava v zvezi z nacionalno ureditvijo, s katero je ponudnikom elektronskih komunikacijskih storitev za – med drugim – zaščito nacionalne varnosti in boj proti kriminalu naložena splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji, ki ni združljiva s členom 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine. Ta člen 15(1), razlagan ob upoštevanju načela učinkovitosti, zahteva, da nacionalno kazensko sodišče v okviru kazenskega postopka zoper osebe, osumljene kaznivih dejanj, zavrne informacije in dokaze, pridobljene s splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji, ki ni združljiva s pravom Unije, če te osebe ne morejo učinkovito podati stališča o teh informacijah in dokazih, ki izvirajo s področja, na katero se sodišče ne spozna, in ki lahko bistveno vplivajo na presojo dejanskega stanja.

Stroški

229 Ker je ta postopek za stranke v postopkih v glavni stvari ena od stopenj v postopkih pred predložitvenima sodiščema, ti odločita o stroških. Stroški za predložitev stališč Sodišču, ki niso stroški omenjenih strank, se ne povrnejo.

Iz teh razlogov je Sodišče (veliki senat) razsodilo:

1. **Člen 15(1) Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009, v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine Evropske unije o temeljnih pravicah je treba razlagati tako, da nasprotuje zakonskim ukrepom, s katerimi je za namene iz tega člena 15(1) preventivno določena splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji. Člen 15(1) Direktive 2002/58, kakor je bila spremenjena z Direktivo 2009/136, v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine o temeljnih pravicah pa ne nasprotuje zakonskim ukrepom, s katerimi je**

   – **v položajih, ko se zadevna država članica spopada z resno grožnjo nacionalni varnosti, ki se izkaže za resnično in sedanjo ali predvidljivo, za zaščito nacionalne varnosti omogočena uporaba odredbe, s katero se ponudnikom elektronskih komunikacijskih storitev naloži splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji, pri čemer je sklep o tej odredbi lahko predmet učinkovitega nadzora s strani sodišča ali neodvisnega upravnega organa, katerega odločitev je zavezujoča, da se preveri obstoj enega od teh položajev ter spoštovanje pogojev in jamstev, ki morajo biti določeni, in je navedeni sklep mogoče izdati le za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, vendar ga je v primeru nadaljnjega obstoja te grožnje mogoče podaljšati;**

   – **za zaščito nacionalne varnosti, boj proti hudemu kriminalu in preprečevanje resnih groženj javni varnosti za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, vendar ga je mogoče podaljšati, določena ciljna hramba podatkov o prometu in podatkov o lokaciji, ki je na podlagi objektivnih in nediskriminatornih elementov omejena glede na kategorije zadevnih oseb ali z geografskim merilom;**

   – **za zaščito nacionalne varnosti, boj proti hudemu kriminalu in preprečevanje resnih groženj javni varnosti za obdobje, katerega trajanje je omejeno na to, kar je nujno potrebno, določena splošna in neselektivna hramba naslovov IP, dodeljenih viru povezave;**

   – **za zaščito nacionalne varnosti, boj proti kriminalu in zaščito javne varnosti določena splošna in neselektivna hramba podatkov o civilni identiteti uporabnikov elektronskih komunikacijskih sredstev ter**

   – **za boj proti hudemu kriminalu in *a fortiori* za zaščito nacionalne varnosti omogočena uporaba odredbe, s katero je ponudnikom elektronskih komunikacijskih storitev prek sklepa pristojnega organa, ki je predmet učinkovitega sodnega nadzora, za določeno obdobje naložena takojšnja hramba podatkov o prometu in podatkov o lokaciji, s katerimi ti ponudniki storitev razpolagajo,**

   če je s temi ukrepi z jasnimi in natančnimi pravili zagotovljeno, da je hramba zadevnih podatkov pogojena s spoštovanjem zadevnih materialnih in postopkovnih pogojev ter da imajo zadevne osebe na voljo učinkovita jamstva proti tveganjem zlorabe.

2. **Člen 15(1) Direktive 2002/58, kakor je bila spremenjena z Direktivo 2009/136, v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine o temeljnih pravicah je treba razlagati tako, da ne nasprotuje nacionalni ureditvi, s katero je ponudnikom elektronskih komunikacijskih storitev naloženo, prvič, da avtomatizirano analizirajo in v realnem času zbirajo med drugim podatke o prometu in podatke o lokaciji ter, drugič, da v realnem času zbirajo tehnične podatke o lokaciji uporabljene terminalske opreme, če**

– **je uporaba avtomatizirane analize omejena na položaje, ko se zadevna država članica spopada z resno grožnjo nacionalni varnosti, ki se izkaže za resnično in sedanjo ali predvidljivo, in je uporaba te analize lahko predmet učinkovitega nadzora s strani sodišča ali neodvisnega upravnega organa, katerega odločitev je zavezujoča, da se preveri obstoj položaja, ki upravičuje navedeni ukrep, ter spoštovanje pogojev in jamstev, ki morajo biti določeni, ter če**

– **je uporaba zbiranja podatkov o prometu in podatkov o lokaciji v realnem času omejena na osebe, v zvezi s katerimi obstaja utemeljen razlog za sum, da so tako ali drugače vpletene v teroristične dejavnosti, in je predmet predhodnega nadzora, ki ga opravi sodišče ali neodvisen upravni organ, katerega odločitev je zavezujoča, da se zagotovi, da je takšno zbiranje v realnem času dovoljeno samo v mejah tega, kar je nujno potrebno. V nujnem in ustrezno utemeljenem primeru se mora nadzor izvesti v najkrajšem možnem času.**

3. **Direktivo 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju) je treba razlagati tako, da se na področju varstva zaupnosti sporočil in varstva posameznikov pri obdelavi osebnih podatkov v okviru storitev informacijske družbe ne uporablja, saj je to varstvo glede na primer urejeno z Direktivo 2002/58, kakor je bila spremenjena z Direktivo 2009/136, ali z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46. Člen 23(1) Uredbe 2016/679 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine o temeljnih pravicah je treba razlagati tako, da nasprotuje nacionalni ureditvi, s katero je ponudnikom dostopa do javnih spletnih komunikacijskih storitev in ponudnikom storitev gostovanja naložena splošna in neselektivna hramba med drugim osebnih podatkov v zvezi s temi storitvami.**

4. **Nacionalno sodišče ne more uporabiti določbe nacionalnega prava, na podlagi katere lahko časovno omeji učinke ugotovitve nezakonitosti, ki jo mora sprejeti na podlagi tega prava v zvezi z nacionalno ureditvijo, s katero je ponudnikom elektronskih komunikacijskih storitev za – med drugim – zaščito nacionalne varnosti in boj proti kriminalu naložena splošna in neselektivna hramba podatkov o prometu in podatkov o lokaciji, ki ni združljiva s členom 15(1) Direktive 2002/58, kakor je bila spremenjena z Direktivo 2009/136, v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine o temeljnih pravicah. Ta člen 15(1), razlagan ob upoštevanju načela učinkovitosti, zahteva, da nacionalno kazensko sodišče v okviru kazenskega postopka zoper osebe, osumljene kaznivih dejanj, zavrne informacije in dokaze, pridobljene s splošno in neselektivno hrambo podatkov o prometu in podatkov o lokaciji, ki ni združljiva s pravom Unije, če te osebe ne morejo učinkovito podati stališča o teh informacijah in dokazih, ki izvirajo s področja, na katero se sodišče ne spozna, in ki lahko bistveno vplivajo na presojo dejanskega stanja.**

Podpisi