Zbierka súdnych rozhodnutí

ROZSUDOK SÚDNEHO DVORA (veľká komora)

zo 6. októbra 2020 *

[Znenie opravené uznesením zo 16. novembra 2020]

Obsah

* Jazyk konania: francúzština.

„Návrh na začatie prejudiciálneho konania – Spracovávanie osobných údajov v sektore elektronických komunikácií – Poskytovatelia elektronických komunikačných služieb – Poskytovatelia hostingových služieb a poskytovatelia prístupu na internet – Všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe – Automatizovaná analýza údajov – Prístup k údajom v reálnom čase – Ochrana národnej bezpečnosti a boj proti terorizmu – Boj proti trestnej činnosti – Smernica 2002/58/ES – Pôsobnosť – Článok 1 ods. 3 a článok 3 – Dôvernosť elektronickej komunikácie – Ochrana – Článok 5 a článok 15 ods. 1 – Smernica 2000/31/ES – Pôsobnosť – Charta základných práv Európskej únie – Články 4, 6 až 8 a 11, ako aj článok 52 ods. 1 – Článok 4 ods. 2 ZEÚ“

V spojených veciach C-511/18, C-512/18 a C-520/18,

ktorých predmetom sú návrhy na začatie prejudiciálneho konania podľa článku 267 ZFEÚ, podané rozhodnutiami Conseil d'État (Štátna rada, Francúzsko) z 26. júla 2018 doručenými Súdnemu dvoru 3. augusta 2018 (C-511/18 a C-512/18) a rozhodnutím Cour constitutionnelle (Ústavný súd, Belgicko) z 19. júla 2018 doručeným Súdnemu dvoru 2. augusta 2018 (C-520/18), ktoré súvisia s konaniami:

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

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

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

Igwan.net (C-511/18),

proti

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

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

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18), za účasti:

Privacy International (C-512/18),

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

a

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,

za účasti:

Child Focus (C-520/18),

SÚDNY DVOR (veľká komora),

v zložení: predseda K. Lenaerts, podpredsedníčka R. Silva de Lapuerta, predsedovia komôr J.-C. Bonichot, A. Arabadžiev, A. Prechal, M. Safjan, P. G. Xuereb a L. S. Rossi, sudcovia J. Malenovský, L. Bay Larsen, T. von Danwitz (spravodajca), C. Toader, K. Jürimäe, C. Lycourgos a N. Piçarra,

generálny advokát: M. Campos Sánchez-Bordona,

tajomník: C. Strömholm, referentka,

so zreteľom na písomnú časť konania a po pojednávaní z 9. a 10. septembra 2019,

so zreteľom na pripomienky, ktoré predložili:

– La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net a Center for Democracy and Technology, v zastúpení: A. Fitzjean Ò Cobhthaigh, avocat,

– French Data Network, v zastúpení: Y. Padova, avocat,

– Privacy International, v zastúpení: H. Roy, avocat,

– Ordre des barreaux francophones et germanophone, v zastúpení: E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart a J.-F. Henrotte, avocats,

– Académie Fiscale ASBL a UA, v zastúpení: J.-P. Riquet,

– Liga voor Mensenrechten ASBL, v zastúpení: J. Vander Velpen, avocat,

– Ligue des Droits de l'Homme ASBL, v zastúpení: R. Jespers a J. Fermon, avocats,

– VZ, WY a XX, v zastúpení: D. Pattyn, avocat,

– Child Focus, v zastúpení: N. Buisseret, K. De Meester a J. Van Cauter, avocats,

– francúzska vláda, v zastúpení: pôvodne D. Dubois, F. Alabrune, D. Colas, E. de Moustier a A.-L. Desjonquères, neskôr D. Dubois, F. Alabrune, E. de Moustier a A.-L. Desjonquères, splnomocnení zástupcovia,

– belgická vláda, v zastúpení: J.-C. Halleux, P. Cottin a C. Pochet, splnomocnení zástupcovia, za právnej pomoci J. Vanpraet, Y. Peeters, S. Depré a E. de Lophem, avocats,

– česká vláda, v zastúpení: M. Smolek, J. Vláčil a O. Serdula, splnomocnení zástupcovia,

– dánska vláda, v zastúpení: pôvodne J. Nymann-Lindegren, M. Wolff a P. Ngo, neskôr J. Nymann-Lindegren a M. Wolff, splnomocnení zástupcovia,

– nemecká vláda, v zastúpení: pôvodne J. Möller, M. Hellmann, E. Lankenau, R. Kanitz a T. Henze, neskôr J. Möller, M. Hellmann, E. Lankenau a R. Kanitz, splnomocnení zástupcovia,

– estónska vláda, v zastúpení: N. Grünberg a A. Kalbus, splnomocnené zástupkyne,

– írska vláda, v zastúpení: A. Joyce, M. Browne a G. Hodge, splnomocnení zástupcovia, za právnej pomoci D. Fennelly, BL,

– španielska vláda, v zastúpení: pôvodne L. Aguilera Ruiz a A. Rubio González, neskôr L. Aguilera Ruiz, splnomocnený zástupca,

– cyperská vláda, v zastúpení: E. Neofytou, splnomocnená zástupkyňa,

– lotyšská vláda, v zastúpení: V. Soņeca, splnomocnená zástupkyňa,

– maďarská vláda, v zastúpení: pôvodne M. Z. Fehér a Z. Wagner, neskôr M. Z. Fehér, splnomocnený zástupca,

– holandská vláda, v zastúpení: M. K. Bulterman a M. A. M. de Ree, splnomocnené zástupkyne,

– poľská vláda, v zastúpení: B. Majczyna, J. Sawicka a M. Pawlicka, splnomocnení zástupcovia,

– švédska vláda, v zastúpení: pôvodne H. Shev, H. Eklinder, C. Meyer-Seitz a A. Falk, neskôr H. Shev, H. Eklinder, C. Meyer-Seitz a J. Lundberg, splnomocnené zástupkyne,

– vláda Spojeného kráľovstva, v zastúpení: S. Brandon, splnomocnený zástupca, za právnej pomoci G. Facenna, QC, a C. Knight, barrister,

– [opravené uznesením zo 16. novembra 2020],

– Európska komisia, v zastúpení: pôvodne H. Kranenborg, M. Wasmeier a P. Costa de Oliveira, neskôr H. Kranenborg a M. Wasmeier, splnomocnení zástupcovia,

– Európsky dozorný úradník pre ochranu údajov, v zastúpení: T. Zerdick a A. Buchta, splnomocnení zástupcovia,

po vypočutí návrhov generálneho advokáta na pojednávaní 15. januára 2020,

vyhlásil tento

Rozsudok

1 Návrhy na začatie prejudiciálneho konania sa týkajú jednak výkladu článku 15 ods. 1 smernice Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 2002, s. 37; Mim. vyd. 13/029, s. 514), zmenenej smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009 (Ú. v. EÚ L 337, 2009, s. 11) (ďalej len „smernica 2002/58“), a jednak článkov 12 až 15 smernice 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode) (Ú. v. ES L 178, 2000, s. 1; Mim. vyd. 13/025, s. 399) v spojení s článkami 4, 6 až 8 a 11, ako aj s článkom 52 ods. 1 Charty základných práv Európskej únie (ďalej len „Charta“) a článkom 4 ods. 2 ZEÚ.

2 Návrh vo veci C-511/18 bol podaný v rámci sporov medzi La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs a Igwan.net na jednej strane a Premier ministre (predseda vlády, Francúzsko), Garde des Sceaux, ministre de la Justice (strážca pečatí, minister spravodlivosti, Francúzsko), ministre de l'Intérieur (minister vnútra, Francúzsko) a ministre des Armées (minister ozbrojených síl, Francúzsko) na druhej strane v súvislosti so zákonnosťou décret nº 2015-1185, du 28 septembre 2015, portant désignation des services spécialisés de renseignement (dekrét č. 2015-1185 z 28. septembra 2015 o určovaní špecializovaných spravodajských služieb) (JORF z 29. septembra 2015, text 1 z 97, ďalej len „dekrét č. 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 (dekrét č. 2015-1211 z 1. októbra 2015 o súdnych konaniach týkajúcich sa uplatňovania spravodajských metód, ktoré podliehajú povoleniu, a záznamov týkajúcich sa bezpečnosti štátu) (JORF z 2. októbra 2015, text 7 zo 108, ďalej len „dekrét č. 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 (dekrét č. 2015-1639 z 11. decembra 2015 o určovaní služieb, ktoré nie sú špecializovanými spravodajskými službami, oprávnených využívať metódy uvedené v hlave V knihy VIII zákonníka vnútornej bezpečnosti) (JORF z 12. decembra 2015, text 28 zo 127, ďalej len „dekrét č. 2015-1639"), a décret nº 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement (dekrét č. 2016-67 z 29. januára 2016 o metódach získavania informácií) (JORF z 31. januára 2016, text 2 zo 113, ďalej len „dekrét č. 2016-67").

3 Návrh vo veci C-512/18 bol podaný v rámci sporov medzi French Data Network, La Quadrature du Net a Fédération des fournisseurs d'accès à Internet associatifs na jednej strane a predsedom vlády (Francúzsko) a strážcom pečate, ministrom spravodlivosti (Francúzsko) na druhej strane v súvislosti so zákonnosťou článku R. 10-13 Code des postes et des communications électroniques (Zákonník pôšt a elektronických komunikácií) (ďalej len „CPCE") a 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 (dekrét č. 2011-219 z 25. februára 2011 o uchovávaní a poskytovaní údajov, ktoré umožňujú identifikovať každú osobu, ktorá prispela k vytvoreniu obsahu poskytovaného online) (JORF z 1. marca 2011, text 32 zo 170, ďalej len „dekrét č. 2011-219").

4 Návrh vo veci C-520/18 bol podaný v rámci sporov medzi Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY a XX na jednej strane a Conseil des ministres (Rada ministrov, Belgicko) na druhej strane v súvislosti so zákonnosťou loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (zákon z 29. mája 2016 o zbere a uchovávaní údajov v odvetví elektronických komunikácií) (*Moniteur belge* z 18. júla 2016, s. 44717, ďalej len „zákon z 29. mája 2016").

Právny rámec

Právo Únie

Smernica 95/46

5 Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Ú. v. ES L 281, 1995, s. 31; Mim. vyd. 13/015, s. 355) bola s účinnosťou od 25. mája 2018 zrušená nariadením Európskeho parlamentu

a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46 (Ú. v. EÚ L 119, 2016, s. 1). Článok 3 ods. 2 smernice 95/46 stanovoval:

„Táto smernica sa neuplatňuje na spracovanie osobných údajov:

– v priebehu činností, ktoré sú mimo rozsahu zákona [práva – *neoficiálny preklad*] spoločenstva, ako sú tie, ktoré sú uvedené v hlave V a VI Zmluvy o Európskej únii, a v žiadnom prípade sa neuplatňuj[e] na operácie spracovania týkajúce sa verejnej bezpečnosti, obrany, bezpečnosti štátu (vrátane hospodárskej prosperity štátu, keď sa operácia spracovania týka záležitostí bezpečnosti štátu) a činností štátu v oblastiach trestného zákona [práva – *neoficiálny preklad*],

– fyzickou osobou v priebehu osobnej činnosti, alebo činnosti týkajúcej sa domácnosti [fyzickou osobou na výkon výlučne osobných alebo domácich činností – *neoficiálny preklad*].“

6 Článok 22 smernice 95/46, ktorý sa nachádza v jej kapitole III s názvom „Súdne opravné prostriedky, zodpovednosť a sankcie“, znel:

„Bez toho, aby bol[i] dotknuté akékoľvek administratívne prostriedky nápravy, pre ktoré sa môže urobiť predpis [ktoré možno podať, – *neoficiálny preklad*] okrem iného pred dozorným orgánom uvedeným v článku 28 pred žiadosťou o súhlas súdneho orgánu [pred predložením veci súdnemu orgánu – *neoficiálny preklad*], zabezpečia členské štáty právo každej osoby na súdny opravný prostriedok za akékoľvek porušenie práv, ktoré [jej] zaručuje vnútroštátne právo, použiteľné na uvedené spracovanie.“

Smernica 97/66

7 Článok 5 smernice Európskeho parlamentu a Rady 97/66/ES z 15. decembra 1997 o spracovaní osobných údajov a ochrane súkromia v telekomunikačnom sektore [*neoficiálny preklad*] (Ú. v. ES L 24, 1998, s. 1.), nazvaný „Dôvernosť správy“, uvádzal:

„1. Členské štáty vnútroštátnymi právnymi predpismi zabezpečia dôvernosť správ prenášaných pomocou verejnej telekomunikačnej siete alebo verejne dostupných telekomunikačných služieb. Zakážu najmä počúvanie, odpočúvanie, ukladanie správ a iné druhy narušovania alebo dohľadu nad správami zo strany iných osôb[,] než sú užívatelia[,] bez súhlasu príslušných užívateľov, pokiaľ tieto činnosti nie sú zákonne oprávnené v súlade s článkom 14 ods. 1.

2. Odsek 1 nemá vplyv na akékoľvek zákonne oprávnené zaznamenávanie správ v rámci zákonnej obchodnej praxe na účely poskytnutia dôkazu o obchodnej transakcii alebo akejkoľvek inej obchodnej správy.“ [*neoficiálny preklad*]

Smernica 2000/31

8 Odôvodnenia 14 a 15 smernice 2000/31 stanovujú:

„(14) Ochranu jednotlivcov v súvislosti so spracovaním osobných údajov upravuje výlučne smernica [95/46] a smernica [97/66], ktoré sú v plnom rozsahu uplatniteľné aj na služby informačnej spoločnosti; tieto smernice už ustanovili právny rámec spoločenstva v oblasti osobných údajov a preto nie je potrebné sa v tejto smernici touto problematikou zaoberať s cieľom zabezpečiť hladké fungovanie vnútorného trhu, najmä voľného pohybu osobných údajov medzi členskými štátmi; vykonávanie a uplatňovanie tejto smernice by mali byť plne v súlade so zásadami

súvisiacimi s ochranou osobných údajov, najmä čo sa týka nevyžiadanej komerčnej komunikácie a zodpovednosti sprostredkovateľov; táto smernica nemôže brániť anonymnému používaniu otvorených sietí, ako napríklad internetu.

(15) Zachovanie dôvernosti komunikácie (poskytnutých informácií) zaručuje článok 5 smernice [97/66]; v súlade s touto smernicou musia členské štáty zakázať všetky druhy odpočúvania alebo dohľadu nad takouto komunikáciou inými, ako sú odosielatelia alebo príjemcovia, s výnimkou prípadov, keď je to povolené podľa zákona.“

9 Článok 1 smernice 2000/31 znie:

„1. Táto smernica sa snaží prispieť k riadnemu fungovaniu vnútorného trhu zabezpečením voľného pohybu služieb informačnej spoločnosti medzi členskými štátmi.

2. Táto smernica harmonizuje, v rozsahu potrebnom na dosiahnutie cieľa uvedeného v odseku 1, určité vnútroštátne ustanovenia o službách informačnej spoločnosti týkajúce sa vnútorného trhu, sídla poskytovateľov služieb, komerčných oznámení, elektronických zmlúv, zodpovednosti sprostredkovateľov, spravovacích poriadkov, mimosúdneho riešenia sporov a spolupráce medzi členskými štátmi.

3. Táto smernica dopĺňa právo spoločenstva uplatniteľné na služby informačnej spoločnosti bez toho, aby bola dotknutá najmä úroveň ochrany zdravia obyvateľstva a záujmov spotrebiteľa, ktoré sú ustanovené v aktoch spoločenstva a vo vnútroštátnych právnych predpisoch, ktorá ich vykonáva [ktoré ich vykonávajú – *neoficiálny preklad*], pokiaľ to neobmedzuje slobodu poskytovania služieb informačnej spoločnosti.

…

5. Dohovor [Táto smernica – *neoficiálny preklad*] sa nevzťahuje na:

…

b) otázky týkajúce sa služieb informačnej spoločnosti, na ktoré sa vzťahujú smernice [95/46] a [97/66];

…“

10 Článok 2 smernice 2000/31 znie:

„Na účely tejto smernice majú nasledujúce výrazy uvedený význam:

a) ‚služby informačnej spoločnosti‘: služby v zmysle článku 1 ods. 2 smernice [Európskeho parlamentu a Rady] 98/34/ES [z 22. júna 1998, ktorou sa stanovuje postup pri poskytovaní informácií v oblasti technických noriem a predpisov, ako aj pravidiel vzťahujúcich sa na služby informačnej spoločnosti (Ú. v. ES L 204, 1998, s. 37; Mim. vyd. 13/020, s. 337)], naposledy zmenenej a doplnenej smernicou [Európskeho parlamentu a Rady] 98/48/ES [z 20. júla 1998 (Ú. v. ES L 217, 1998, s. 18; Mim. vyd. 13/021, s. 8)];

…“

11 Článok 15 smernice 2000/31 stanovuje:

„1. Členské štáty neuložia poskytovateľom všeobecnú povinnosť pri poskytovaní služieb, na ktoré sa vzťahujú články 12, 13 a 14, aby monitorovali informácie, ktoré prenášajú alebo ktoré uložili, ani všeobecnú povinnosť aktívne zisťovať skutočnosti alebo okolnosti, ktoré by naznačovali, že ide o nezákonnú činnosť.

2. Členské štáty môžu ustanoviť povinnosť, aby poskytovatelia služieb informačnej spoločnosti informovali príslušné verejné orgány o údajných vykonávaných nezákonných činnostiach alebo o údajných nezákonných poskytovaných informáciách, alebo povinnosť oznamovať príslušným orgánom na ich žiadosť informácie, ktoré by im umožnili identifikáciu príjemcov ich služieb, s ktorými uzatvorili dohody o uložení informácií.“

Smernica 2002/21

12 Podľa odôvodnenia 10 smernice Európskeho parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica) (Ú. v. ES L 108, 2002, s. 33; Mim. vyd. 13/029, s. 349):

„Definícia ‚služby informačnej spoločnosti‘ uvedená v článku 1 smernice [98/34, zmenenej smernicou 98/48], zahŕňa široký rozsah ekonomických činností vykonávaných v režime on-line. Pre väčšinu z týchto činností neplatia ustanovenia tejto smernice, pretože nie sú založené úplne alebo zväčša na prenose signálov elektronických komunikačných sietí. Pre služby hlasovej telefónie a prenosu elektronickej pošty platí táto smernica. Jeden podnik, napríklad poskytovateľ služieb Internetu, môže ponúkať elektronické komunikačné služby, ako prístup na Internet a služby, na ktoré sa nevzťahuje táto smernica, ako napríklad poskytovanie webového obsahu.“

13 Článok 2 smernice 2002/21 stanovuje:

„Na účely tejto smernice:

…

c) ‚elektronická komunikačná služba‘ znamená službu bežne poskytovanú za úhradu, ktorá pozostáva úplne alebo prevažne z prenosu signálov v elektronických komunikačných sieťach, vrátane telekomunikačných služieb a prenosových služieb v sieťach používaných na vysielanie, s výnimkou služieb poskytujúcich obsah alebo vykonávajúcich edičnú kontrolu obsahu prenášaného pomocou elektronických komunikačných sietí a služieb; nezahŕňa služby informačnej spoločnosti definované v článku 1 smernice [98/34], ktoré úplne alebo prevažne nepredstavujú prenos signálov v elektronických komunikačných sieťach;

…“

Smernica 2002/58

14 Odôvodnenia 2, 6, 7, 11, 22, 26 a 30 smernice 2002/58 uvádzajú:

„(2) Táto smernica sa snaží rešpektovať základné práva a dodržiavať princípy uznané najmä [Chartou]. Táto smernica sa snaží najmä o plné zabezpečenie práv stanovených v článkoch 7 a 8 uvedenej charty.

…

(6) Internet revolucionalizoval tradičné trhové štruktúry tým, že poskytuje spoločnú, globálnu infraštruktúru pre ponuku širokého rozsahu elektronických komunikačných služieb. Verejne dostupné elektronické komunikačné služby na internete otvárajú nové možnosti pre užívateľov, no prinášajú aj nové riziká pre ich osobné údaje a súkromie.

(7) V prípade verejných komunikačných sietí by sa mali stanoviť špecifické právne, regulačné a technické opatrenia, aby boli chránené základné práva a slobody fyzických osôb a legitímne záujmy právnických osôb, najmä z hľadiska zvyšovania kapacity automatického uchovávania a spracovávania údajov týkajúcich sa účastníkov a užívateľov.

…

(11) Podobne ako smernica [95/46] sa táto smernica netýka otázok ochrany základných práv a slobôd vzťahujúcich sa k činnostiam, ktoré nie sú upravené právom [Únie]. Preto nemení existujúcu rovnováhu medzi právami jednotlivca na súkromie a možnosťami členských štátov prijať opatrenia uvedené v článku 15 ods. 1 tejto smernice, ktoré sú potrebné na ochranu verejnej bezpečnosti, obrany, bezpečnosti štátu (vrátane ekonomického blahobytu štátu, keď sa činnosti týkajú záležitostí bezpečnosti štátu) a presadzovanie trestného práva. Následne táto smernica nemá vplyv na možnosť členských štátov zachytávať elektronické správy alebo prijímať iné opatrenia, ak je to nevyhnutné z akýchkoľvek iných dôvodov a v súlade s Európskym dohovorom o ochrane ľudských práv a základných slobôd [podpísaným v Ríme 4. novembra 1950], interpretovaným rozsudkami súdneho dvora týkajúcimi sa ľudských práv [Európskeho súdu pre ľudské práva – *neoficiálny preklad*]; také opatrenia musia byť primerané, prísne proporcionálne vo vzťahu k zamýšľanému účelu a potrebné v rámci demokratickej spoločnosti a mali by byť predmetom primeranej ochrany v súlade s Európskym dohovorom na ochranu ľudských práv a základných slobôd.

…

(22) Zákaz ukladania správ a príslušných prevádzkových dát [príslušných údajov o prenose dát – *neoficiálny preklad*] osobami inými, než sú užívatelia alebo účastníci bez ich súhlasu, nie je určený na zákaz akéhokoľvek automatického, dočasného a prechodného uloženia týchto informácií, pokiaľ sa to uskutočňuje výhradne na účely výkonu prenosu v elektronickej komunikačnej sieti a za predpokladu, že informácie sa neukladajú na dobu dlhšiu, než je nevyhnutné na prenos a riadenie chodu prenosu a že počas doby uloženia je zaručená dôvernosť informácií. …

…

(26) Údaje vzťahujúce sa k účastníkom, ktoré sú spracovávané v elektronickej komunikačnej sieti a slúžia na zabezpečenie spojenia a prenos informácií, obsahujú údaje o súkromnom živote fyzických osôb a týkajú sa práva na rešpektovanie ich korešpondencie alebo sa týkajú legitímnych záujmov právnických osôb; také údaje sa môžu ukladať len v rozsahu, aký je potrebný na zabezpečenie služby na účely fakturácie a poplatkov za spojenie a len na limitovanú dobu; akékoľvek ďalšie spracovávanie takých údajov…, sa môže povoliť len vtedy, keď účastník s týmto súhlasí na základe úplných a presných informácií poskytovateľa verejne dostupných elektronických komunikačných služieb o druhu ďalšieho spracovania, ktoré zamýšľa vykonať a o právach účastníka nedať alebo odvolať svoj súhlas na také spracovanie; prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*] používané na marketingové komunikačné služby… by sa mali tiež vymazať alebo by mali byť anonymné…

…

(30) Systémy poskytovania elektronických komunikačných sietí a služieb by mali byť konštruované tak, aby bol obmedzený počet nevyhnutných osobných údajov na minimum. …“

15 Článok 1 smernice 2002/58, nazvaný „Rozsah platnosti a cieľ“, stanovuje:

„1. Touto smernicou sa ustanovuje harmonizácia vnútroštátnych ustanovení požadovaných na zabezpečenie primeranej úrovne ochrany základných práv a slobôd, a najmä práva na súkromie a dôvernosť, z hľadiska spracúvania osobných údajov v elektronickom komunikačnom sektore a zabezpečenia voľného pohybu takých údajov a elektronických komunikačných zariadení a služieb v [Európskej únii].

2. Ustanovenia tejto smernice spodrobňujú a dopĺňajú smernicu [95/46] na účely uvedené v odseku 1. Okrem toho poskytujú ochranu legitímnych záujmov účastníkov, ktorí sú právnickými osobami.

3. Táto smernica sa nevzťahuje na činnosti, ktoré sú mimo pôsobnosti [ZFEÚ], ako sú činnosti podľa hlavy V a VI Zmluvy o Európskej únii[,] a v žiadnom prípade na činnosti týkajúce sa verejnej bezpečnosti, obrany, bezpečnosti štátu (vrátane ekonomického blahobytu štátu, keď sa činnosti týkajú záležitostí bezpečnosti štátu) a činnosti [činnosti štátu – *neoficiálny preklad*] v oblasti trestného práva.“

16 Článok 2 smernice 2002/58, nazvaný „Definície“, stanovuje:

„Pokiaľ nie je stanovené inak, platia definície v smernici [95/46] a v smernici [2002/21].

Platia aj tieto definície:

a) ‚užívateľ‘ znamená každú fyzickú osobu, ktorá používa verejne dostupnú elektronickú komunikačnú službu na súkromné alebo obchodné účely bez toho, aby si túto službu predplatil;

b) ‚prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*]‘ znamenajú akékoľvek údaje spracovávané na účely prenosu správy v elektronickej komunikačnej sieti alebo na účely fakturácie prenosu;

c) ‚lokalizačné dáta [údaje o polohe – *neoficiálny preklad*]‘ znamenajú akékoľvek údaje spracúvané v elektronickej komunikačnej sieti alebo prostredníctvom elektronickej komunikačnej služby, udávajúce geografickú polohu koncového zariadenia užívateľa verejne dostupnej elektronickej komunikačnej služby;

d) ‚správa‘ znamená akékoľvek informácie vymieňané alebo prenášané medzi konečným počtom účastníkov pomocou verejne dostupnej elektronickej komunikačnej služby. Toto nezahŕňa akékoľvek informácie prenášané ako časť rozhlasových služieb pre verejnosť v elektronickej komunikačnej sieti, pokiaľ sa informácie nemôžu spájať s identifikovateľným účastníkom alebo užívateľom prijímajúcim informácie;

…“

17 Článok 3 smernice 2002/58, nazvaný „Dotknuté služby“, stanovuje:

„Táto smernica sa vzťahuje na spracúvanie osobných údajov v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach v Spoločenstve vrátane verejných komunikačných sietí, ktoré podporujú zariadenia na zber údajov a identifikáciu.“

18 Podľa článku 5 smernice 2002/58, nazvaného „Dôvernosť správy“:

„1. Členské štáty vnútroštátnymi právnymi predpismi zabezpečia dôvernosť správ a príslušných prevádzkových dát [príslušných údajov o prenose dát – *neoficiálny preklad*] prenášaných pomocou verejnej komunikačnej siete a verejne dostupných elektronických komunikačných sietí. Zakážu najmä počúvanie, odpočúvanie a iné druhy narušovania alebo dohľadu nad správami a príslušnými prevádzkovými dátami [príslušnými údajmi o prenose dát – *neoficiálny preklad*] zo strany iných osôb[,] než sú užívatelia[,] bez súhlasu príslušných užívateľov, pokiaľ to nie je zákonne oprávnené v súlade s článkom 15 ods. 1 Tento odsek nebráni technickému uloženiu, ak je to potrebné s cieľom prenosu správy, bez vplyvu na princíp dôvernosti.

…

3. Členské štáty zabezpečia, aby sa ukladanie informácií alebo získavanie prístupu k informáciám, ktoré už boli uložené, v koncovom zariadení účastníka alebo užívateľa povolilo len pod podmienkou, že dotknutý účastník alebo užívateľ dal na to vopred súhlas na základe jasných a komplexných informácií v súlade so smernicou [95/46], okrem iného aj o účeloch spracovania. To nebráni nijakému technickému uloženiu ani prístupu výhradne na účely výkonu prenosu správy prostredníctvom elektronickej komunikačnej siete alebo ak je to nevyhnutne potrebné na to, aby poskytovateľ služieb informačnej spoločnosti, ktoré si účastník alebo užívateľ výslovne vyžiadal, mohol tieto služby poskytnúť.“

19 Článok 6 smernice 2002/58, nazvaný „Prevádzkové údaje [Údaje o prenose dát – *neoficiálny preklad*]“, stanovuje:

„1. Prevádzkové dáta [Údaje o prenose dát – *neoficiálny preklad*] týkajúce sa účastníkov a užívateľov, spracovávané a uložené poskytovateľom verejnej komunikačnej siete alebo verejne dostupnej elektronickej komunikačnej služby, sa musia vymazať alebo zanonymniť [anonymizovať – *neoficiálny preklad*], ak už naďalej nie sú potrebné na účely prenosu správy, bez vplyvu na odseky 2, 3 a 5 tohto článku a článku 15 ods. 1.

2. Prevádzkové dáta [Údaje o prenose dát – *neoficiálny preklad*] potrebné na účely fakturácie účastníka a platby za spojenie sa môžu spracovávať. Také spracovanie je povolené len do konca obdobia, počas ktorého môže byť faktúra právne napadnutá alebo sa môže uplatniť nárok na platbu.

3. Na účely marketingu elektronických komunikačných služieb alebo na poskytovanie služieb s pridanou hodnotou poskytovateľ verejne dostupnej elektronickej komunikačnej služby môže spracúvať údaje uvedené v odseku 1 v rozsahu a počas trvania potrebného na také služby alebo marketing, ak účastník alebo užívateľ, ktorého sa údaje týkajú, dá na to predtým svoj súhlas. Užívatelia alebo účastníci musia mať možnosť kedykoľvek odvolať svoj súhlas na spracovanie údajov.

…

5. Spracovávanie prevádzkových dát [údajov o prenose dát – *neoficiálny preklad*], v súlade s odsekmi 1, 2, 3 a 4, sa musí obmedziť na osoby konajúce na pokyn poskytovateľa verejných komunikačných sietí a verejne dostupných elektronických komunikačných služieb, ktoré sú zodpovedné za fakturovanie alebo riadenie prevádzky, vybavovanie dotazov zákazníkov, odhaľovanie podvodov, marketing elektronických komunikačných služieb alebo poskytovanie služby s pridanou hodnotou, a musí sa obmedziť na to, čo je nevyhnutné na účely takých činností.“

20 Článok 9 tejto smernice, nazvaný „Miestne dáta [údaje o polohe – *neoficiálny preklad*] iné než prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*]“, vo svojom odseku 1 stanovuje:

„Ak sa môžu spracovávať miestne dáta [údaje o polohe – *neoficiálny preklad*] iné než prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*], ktoré sa týkajú užívateľov alebo účastníkov verejnej komunikačnej siete alebo verejne dostupných elektronických komunikačných služieb, také údaje sa môžu spracovávať, len keď sú anonymné alebo len so súhlasom používateľov alebo účastníkov v rozsahu a trvaní nevyhnutnom na poskytovanie služby s pridanou hodnotou. Poskytovateľ služby musí informovať užívateľov alebo účastníkov predtým, než získa ich súhlas o druhu miestnych dát [údajov o polohe – *neoficiálny preklad*] iných, než sú prevádzkové dáta [údaje o prenose dát – *neoficiálny preklad*], ktoré bude spracovávať, o účele a dobe trvania spracovávania a o tom, či budú dáta prenášané tretej strane na účely poskytovania služby s pridanou hodnotou. …“

21 Článok 15 uvedenej smernice, nazvaný „Uplatňovanie niektorých ustanovení smernice [95/46]“, uvádza:

„1. Členské štáty môžu prijať legislatívne opatrenia na obmedzenie rozsahu práv a povinností uvedených v článku 5, článku 6, článku 8 ods. 1, 2, 3 a 4 a článku 9 tejto smernice, ak také obmedzenie predstavuje nevyhnutné, vhodné a primerané opatrenie v demokratickej spoločnosti na zabezpečenie národnej bezpečnosti (t. j. bezpečnosti štátu), obrany, verejnej bezpečnosti a na zabránenie, vyšetrovanie, odhaľovanie a stíhanie trestných činov alebo neoprávnené používanie [neoprávneného používania – *neoficiálny preklad*] elektronického komunikačného systému podľa článku 13 ods. 1 smernice [95/46]. Na tento účel členské štáty môžu, medzi iným, prijať legislatívne opatrenia umožňujúce zadržanie [uchovávanie – *neoficiálny preklad*] údajov na limitované obdobie, oprávnené z dôvodov stanovených v tomto odseku. Všetky opatrenia uvedené v tomto odseku musia byť v súlade so všeobecnými princípmi práva [Únie] vrátane tých, ktoré sú uvedené v článku 6 ods. 1 a 2 Zmluvy o Európskej únii.

…

2. Ustanovenia kapitoly III smernice [95/46] o právnych opravných prostriedko[ch], záväznosti a sankciách platia vo vzťahu k ustanoveniam prijatým podľa tejto smernice a vo vzťahu k právam jednotlivcov vyplývajúcim z tejto smernice.

…“

Nariadenie 2016/679

22 Odôvodnenie 10 nariadenia 2016/679 uvádza:

„S cieľom zabezpečiť konzistentnú a vysokú úroveň ochrany fyzických osôb a odstrániť prekážky tokov osobných údajov v rámci Únie, úroveň ochrany práv a slobôd fyzických osôb pri spracúvaní týchto údajov by mala byť rovnaká vo všetkých členských štátoch. Konzistentné a jednotné uplatňovanie pravidiel ochrany základných práv a slobôd fyzických osôb pri spracúvaní osobných údajov by sa malo zabezpečiť v rámci celej Únie. …“

23 Článok 2 tohto nariadenia stanovuje:

„1. Toto nariadenie sa vzťahuje na spracúvanie osobných údajov vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.

2. Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov:

a) v rámci činnosti, ktorá nepatrí do pôsobnosti práva Únie;

b) členskými štátmi pri vykonávaní činností patriacich do rozsahu pôsobnosti kapitoly 2 hlavy V ZEÚ;

…

d) príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzania.

…

4. Týmto nariadením preto nie je dotknuté uplatňovanie smernice [2000/31], najmä pravidlá týkajúce sa zodpovednosti poskytovateľov služieb informačnej spoločnosti uvedené v článkoch 12 až 15 uvedenej smernice.“

24 Článok 4 uvedeného nariadenia stanovuje:

„Na účely tohoto nariadenia:

1. ‚osobné údaje‘ sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len ‚dotknutá osoba‘); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby;

2. ‚spracúvanie‘ je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami;

…“

25 Článok 5 nariadenia 2016/679 stanovuje:

„1. Osobné údaje musia byť:

a) spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe (‚zákonnosť, spravodlivosť a transparentnosť‘);

b) získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi; ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či štatistické účely sa v súlade s článkom 89 ods. 1 nepovažuje za nezlučiteľné s pôvodnými účelmi (‚obmedzenie účelu‘);

c) primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú (‚minimalizácia údajov‘);

d) správne a podľa potreby aktualizované; musia sa prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia (‚správnosť‘);

e) uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú; osobné údaje sa môžu uchovávať dlhšie, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely v súlade s článkom 89 ods. 1 za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných týmto nariadením na ochranu práv a slobôd dotknutých osôb (‚minimalizácia uchovávania‘);

f) spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení (‚integrita a dôvernosť‘).

…“

26 Článok 6 tohto nariadenia znie:

„1. Spracúvanie je zákonné iba vtedy a iba v tom rozsahu, keď je splnená aspoň jedna z týchto podmienok:

…

c) spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa;

…

3. Základ pre spracúvanie uvedené v odseku 1 písm. c) a e) musí byť stanovený:

a) v práve Únie alebo

b) v práve členského štátu vzťahujúcom sa na prevádzkovateľa.

Účel spracúvania sa stanoví v tomto právnom základe… Uvedený právny základ môže obsahovať osobitné ustanovenia na prispôsobenie uplatňovania pravidiel tohto nariadenia, vrátane: všeobecných podmienok vzťahujúcich sa na zákonnosť spracúvania prevádzkovateľom; typov spracúvaných údajov; dotknutých osôb; subjektov, ktorým sa môžu osobné údaje poskytnúť, a účely, na ktoré ich možno poskytnúť; obmedzenia účelu; doby uchovávania; a spracovateľských operácií a postupov vrátane opatrení na zabezpečenie zákonného a spravodlivého spracúvania, ako napríklad tie na iné osobitné situácie spracúvania, ako sú stanovené v kapitole IX. Právo Únie alebo právo členského štátu musí spĺňať cieľ verejného záujmu a byť primerané sledovanému oprávnenému cieľu.

…“

27 Článok 23 uvedeného nariadenia stanovuje:

„1. V práve Únie alebo práve členského štátu, ktorému prevádzkovateľ alebo sprostredkovateľ podliehajú, sa prostredníctvom legislatívneho opatrenia môže obmedziť rozsah povinností a práv ustanovených v článkoch 12 až 22 a v článku 34, ako aj v článku 5, pokiaľ jeho ustanovenia

zodpovedajú právam a povinnostiam ustanoveným v článkoch 12 až 22, ak takéto obmedzenie rešpektuje podstatu základných práv a slobôd a je nevyhnutným a primeraným opatrením v demokratickej spoločnosti s cieľom zaistiť:

a) národnú bezpečnosť;

b) obranu;

c) verejnú bezpečnosť;

d) predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie alebo výkon trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzanie;

e) iné dôležité ciele všeobecného verejného záujmu Únie alebo členského štátu, najmä predmet dôležitého hospodárskeho alebo finančného záujmu Únie alebo členského štátu vrátane peňažných, rozpočtových a daňových záležitostí, verejného zdravia a sociálneho zabezpečenia;

f) ochranu nezávislosti súdnictva a súdnych konaní;

g) predchádzanie porušeniam etiky pre regulované profesie, ich vyšetrovanie, odhaľovanie a stíhanie;

h) monitorovaciu, kontrolnú alebo regulačnú funkciu spojenú, hoci aj príležitostne, s výkonom verejnej moci v prípadoch uvedených v písmenách a) až e) a g);

i) ochranu dotknutej osoby alebo práv a slobôd iných;

j) vymáhanie občianskoprávnych nárokov.

2. Konkrétne musí každé legislatívne opatrenie uvedené v odseku 1 obsahovať osobitné ustanovenia, ktoré v relevantných prípado[ch] upravujú aspoň:

a) účely spracúvania alebo kategórie spracúvania;

b) kategórie osobných údajov;

c) rozsah zavedených obmedzení;

d) záruky zabraňujúce zneužitiu údajov alebo nezákonnému prístupu či prenosu;

e) určenie prevádzkovateľa alebo kategórií prevádzkovateľov;

f) doby uchovávania a uplatniteľné záruky, pričom sa zohľadní povaha, rozsah a účely spracúvania alebo kategórie spracúvania;

g) riziká pre práva a slobody dotknutých osôb a

h) práva dotknutých osôb na informovanie o obmedzení, pokiaľ tým nie je ohrozený účel obmedzenia.“

28 Podľa článku 79 ods. 1 uvedeného nariadenia:

„Bez toho, aby bol dotknutý akýkoľvek dostupný správny alebo mimosúdny prostriedok nápravy vrátane práva na podanie sťažnosti dozornému orgánu podľa článku 77, každá dotknutá osoba má právo na účinný súdny prostriedok nápravy, ak sa domnieva, že v dôsledku spracúvania jej osobných údajov v rozpore s týmto nariadením došlo k porušeniu jej práv ustanovených v tomto nariadení.“

29 Podľa článku 94 nariadenia 2016/679:

„1. Smernica [95/46] sa zrušuje s účinnosťou od 25. mája 2018.

2. Odkazy na zrušenú smernicu sa považujú za odkazy na toto nariadenie. Odkazy na Pracovnú skupinu pre ochranu jednotlivcov so zreteľom na spracovanie osobných údajov, zriadenú článkom 29 smernice [95/46], sa považujú za odkazy na Európsky výbor pre ochranu údajov zriadený týmto nariadením.“

30 Článok 95 tohto nariadenia stanovuje:

„Týmto nariadením sa fyzickým či právnickým osobám neukladajú dodatočné povinnosti, pokiaľ ide o spracúvanie v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach v Únii, v prípadoch, keď podliehajú konkrétnym povinnostiam s rovnakým cieľom stanoveným v smernici [2002/58].“

Francúzske právo

Zákonník vnútornej bezpečnosti

31 Kniha VIII legislatívnej časti Code de la sécurité intérieure (Zákonník vnútornej bezpečnosti) (ďalej len „CSI“) vo svojich článkoch L. 801-1 až L. 898-1 stanovuje pravidlá týkajúce sa spravodajských informácií.

32 Článok L. 811-3 CSI stanovuje:

„Špecializované spravodajské služby môžu použiť metódy uvedené v hlave V tejto knihy iba pri výkone svojich príslušných úloh na účely zberu informácií týkajúcich sa ochrany a podpory týchto základných národných záujmov:

1. národná nezávislosť, obrana a územná celistvosť;

2. hlavné záujmy zahraničnej politiky, plnenie európskych a medzinárodných záväzkov Francúzska a predchádzanie akejkoľvek forme zahraničného zasahovania;

3. hlavné hospodárske, priemyselné a vedecké záujmy Francúzska;

4. predchádzanie terorizmu;

5. predchádzanie:
   a) útokom na republikánsku formu inštitúcií;
   b) konaniu zameranému na zachovanie alebo obnovenie zoskupení rozpustených podľa článku L. 212-1;
   c) kolektívnemu násiliu, ktoré môže vážne ohroziť verejný poriadok;

6. predchádzanie trestnej činnosti a organizovanému zločinu;

7. predchádzanie šíreniu zbraní hromadného ničenia.“

33 Článok L. 811-4 CSI uvádza:

„Dekrét prijatý Conseil d'État [(Štátna rada)] po konzultácii s Commission nationale de contrôle des techniques de renseignement [(Národná komisia pre kontrolu spravodajských metód, Francúzsko)] určuje služby, ktoré nie sú špecializovanými spravodajskými službami, podliehajú ministrom obrany, vnútra a spravodlivosti, ako aj ministrom zodpovedným za hospodárstvo, rozpočet alebo clá, a môžu byť oprávnené využívať metódy uvedené v hlave V tejto knihy za podmienok stanovených v tej istej knihe. Pre každú službu spresňuje účely uvedené v článku L. 811-3 a metódy, ktoré môžu byť povolené.“

34 Článok L. 821-1 prvý odsek CSI spresňuje:

„Využívanie metód zberu spravodajských informácií uvedených v kapitolách I až IV hlavy V tejto knihy na vnútroštátnom území podlieha predchádzajúcemu povoleniu predsedu vlády, ktoré vydá po konzultácii s Národnou komisiou pre kontrolu spravodajských metód.“

35 Článok L. 821-2 CSI stanovuje:

„Povolenie uvedené v článku L. 821-1 sa vydáva na základe písomnej a odôvodnenej žiadosti ministra obrany, ministra vnútra, ministra spravodlivosti alebo ministrov zodpovedných za hospodárstvo, rozpočet alebo clá. Každý minister môže túto právomoc individuálne delegovať len na priamych spolupracovníkov, ktorí sú oprávnení nakladať s dôvernými informáciami o národnej obrane.

V žiadosti sa uvedie:

1. metóda alebo metódy, ktoré sa majú použiť;

2. služba, pre ktorú sa žiadosť predkladá;

3. sledovaný účel;

4. dôvody opatrení;

5. doba platnosti povolenia;

6. dotknuté osoby, miesta alebo vozidlá.

Na účely bodu 6 osoby, ktorých totožnosť nie je známa, môžu byť označené ich identifikátormi alebo postavením a miesta alebo vozidlá môžu byť označené odkazom na osoby, ktoré sú predmetom žiadosti.

…“

36 Podľa článku L. 821-3 prvého odseku CSI:

„Žiadosť je zaslaná predsedovi alebo, ak to nie je možné, jednému z členov Národnej komisie pre kontrolu spravodajských metód uvedených v bodoch 2 a 3 článku L. 831-1, ktorý v lehote dvadsaťštyri hodín poskytne stanovisko predsedovi vlády. Ak žiadosť posudzuje komisia zasadajúca v pléne alebo v obmedzenom zložení, predseda vlády je o tom bezodkladne informovaný a stanovisko sa vydá v lehote 72 hodín.“

37 Článok L. 821-4 CSI stanovuje:

„Povolenie na využívanie metód uvedených v kapitolách I až IV hlavy V tejto knihy vydáva predseda vlády na obdobie najviac štyroch mesiacov. … Povolenie obsahuje dôvody a údaje uvedené v bodoch 1 až 6 článku L. 821-2. Každé povolenie možno obnoviť za rovnakých podmienok, aké sú stanovené v tejto kapitole.

Ak sa povolenie vydá napriek zamietavému stanovisku Národnej komisie pre kontrolu spravodajských metód, uvedú sa v ňom dôvody, pre ktoré sa tomuto stanovisku nevyhovelo.

…“

38 Článok L. 833-4 CSI, ktorý sa nachádza v kapitole III tejto hlavy, stanovuje:

„Komisia z vlastného podnetu alebo po prijatí sťažnosti akejkoľvek osoby, ktorá chce overiť, že vo vzťahu k nej nebola protiprávne použitá žiadna spravodajská metóda, vykoná kontrolu namietanej metódy alebo metód s cieľom overiť, či boli alebo sú použité v súlade s touto knihou. Sťažovateľovi oznámi, že boli vykonané potrebné šetrenia bez toho, aby potvrdila alebo vyvrátila ich použitie.“

39 Článok L. 841-1 prvý a druhý odsek CSI znie:

„S výhradou osobitných ustanovení uvedených v článku L. 854-9 tohto zákonníka má Conseil d’État [(Štátna rada)] právomoc rozhodovať za podmienok stanovených v kapitole IIIa hlavy VII knihy VII Code de justice administrative [(Správny súdny poriadok)] o žiadostiach týkajúcich sa využívania spravodajských metód uvedených v hlave V tejto knihy.

Na Conseil d’État [(Štátna rada)] sa môže obrátiť:

1. každá osoba, ktorá chce overiť, že vo vzťahu k nej nebola protiprávne použitá žiadna spravodajská metóda a ktorá preukáže predchádzajúce využitie konania stanoveného v článku L. 833-4;

2. Národná komisia pre kontrolu spravodajských metód za podmienok stanovených v článku L. 833-8.“

40 Hlava V knihy VIII legislatívnej časti CSI, ktorá sa týka „metód zberu spravodajských informácií podliehajúcich povoleniu“, obsahuje okrem iného kapitolu I s názvom „Administratívny prístup k údajom o pripojení“, ktorá obsahuje články L. 851-1 až L. 851-7 CSI.

41 Článok L. 851-1 CSI stanovuje:

„Za podmienok stanovených v kapitole 1 hlavy II tejto knihy možno povoliť, aby sa od prevádzkovateľov elektronických komunikácií a osôb uvedených v článku L. 34-1 [CPCE], ako aj od osôb uvedených v článku 6 ods. I bodoch 1 a 2 loi n.º 2004-575 pour la confiance dans l’économie numérique [(zákon č. 2004-575 o dôvere v digitálne hospodárstvo)] [(JORF z 22. júna 2004, s. 11168)] zbierali informácie alebo dokumenty spracúvané alebo uchovávané prostredníctvom ich elektronických komunikačných sietí alebo služieb, vrátane technických údajov týkajúcich sa identifikácie čísiel predplatného alebo pripojenia k elektronickým komunikačným službám, identifikovania čísel predplatného alebo pripojenia určenej osoby, polohy používaných koncových zariadení, ako aj komunikácií účastníka, konkrétne zoznamu volaných a volajúcich čísel, trvania a dátumu komunikácie.

Odchylne od článku L. 821-2, písomné a odôvodnené žiadosti o technické údaje týkajúce sa identifikácie čísiel predplatného alebo pripojenia k elektronickým komunikačným službám, alebo evidencie všetkých čísel predplatného alebo pripojenia určenej osoby predkladajú priamo Národnej

komisii pre kontrolu spravodajských metód individuálne určení a oprávnení agenti spravodajských služieb uvedených v článkoch L. 811-2 a L. 811-4. Komisia vydá svoje stanovisko za podmienok stanovených v článku L. 821-3.

Za zbieranie informácií a dokumentov od prevádzkovateľov a osôb uvedených v prvom odseku tohto článku zodpovedá oddelenie predsedu vlády. Národná komisia pre kontrolu spravodajských metód má trvalý, úplný, priamy a okamžitý prístup k vyzbieraným informáciám alebo dokumentom.

Podrobné pravidlá uplatňovania tohto článku sú stanovené dekrétom Conseil d'État [(Štátna rada)] prijatým po konzultácii s Commission nationale de l'informatique et des libertés [(Národná komisia pre informačné technológie a občianske slobody, Francúzsko)] a Národnou komisiou pre kontrolu spravodajských metód."

42 Článok L. 851-2 CSI uvádza:

„I. – Za podmienok stanovených v kapitole I hlavy II tejto knihy a výlučne na účely predchádzania terorizmu možno individuálne povoliť, aby sa v sieťach prevádzkovateľov a osôb uvedených v článku L. 851-1 zbierali v reálnom čase informácie alebo dokumenty uvedené v tom istom článku L. 851-1, ktoré sa týkajú osoby vopred označenej ako osoba, v prípade ktorej existuje podozrenie, že má väzbu s určitou hrozbou. Ak existujú závažné dôvody domnievať sa, že jedna alebo viacero osôb patriacich do okolia osoby, ktorej sa týka povolenie, môžu poskytnúť informácie vzhľadom na účel, ktorý odôvodňuje povolenie, možno toto povolenie udeliť individuálne aj pre každú z týchto osôb.

Ia. O maximálnom počte súčasne platných povolení vydaných podľa tohto článku rozhoduje predseda vlády po konzultácii s Národnou komisiou pre kontrolu spravodajských metód. Rozhodnutie, ktorým sa stanovuje táto kvóta a jej rozdelenie medzi ministrov uvedených v prvom odseku článku L. 821-2, sa spolu s počtom povolení na odpočúvanie oznámi komisii.

…"

43 Článok L. 851-3 CSI stanovuje:

„I. – Za podmienok stanovených v kapitole I hlavy II tejto knihy a výlučne na účely predchádzania terorizmu možno uložiť prevádzkovateľom a osobám uvedeným v článku L. 851-1 povinnosť zaviesť automatizované procesy spracovávania v ich sieťach na zisťovanie pripojení, ktoré by mohli predstavovať teroristickú hrozbu, v závislosti od parametrov určených v povolení.

Toto automatizované spracovávanie využíva výlučne informácie alebo dokumenty uvedené v článku L. 851-1 a nezhromažďuje iné údaje ako tie, ktoré zodpovedajú ich predpísaným parametrom, ani neumožňuje identifikáciu osôb, ktorých sa informácie alebo dokumenty týkajú.

V súlade so zásadou proporcionality sa v povolení predsedu vlády spresňuje technický rozsah vykonávania týchto procesov spracúvania.

II. – Národná komisia pre kontrolu spravodajských metód vydáva stanovisko k žiadosti o povolenie pre automatizované procesy spracovávania a k vybraným parametrom detekcie. Má stály, úplný a priamy prístup k týmto procesom spracovávania, ako aj k zozbieraným informáciám a údajom. Ďalej je informovaná o akýchkoľvek zmenách týkajúcich sa procesov spracovávania a parametrov a môže vydávať odporúčania.

Prvé povolenie na vykonanie automatizovaných procesov spracovávania uvedených v bode I tohto článku sa vydáva na obdobie dvoch mesiacov. Povolenie možno obnoviť za podmienok dĺžky trvania stanovených v kapitole I hlavy II tejto knihy. Žiadosť o obnovenie obsahuje záznam o počte identifikátorov nahlásených automatizovaným spracovávaním a analýzu relevantnosti týchto oznámení.

III. – Podmienky stanovené v článku L. 871-6 sa uplatňujú na fyzické operácie vykonávané prevádzkovateľmi a osobami uvedenými v článku L. 851-1 na účely vykonania tohto spracúvania.

IV. – Ak procesy spracovávania uvedené v bode I tohto článku odhalia údaje, ktoré môžu poukazovať na existenciu teroristickej hrozby, predseda vlády alebo jedna z ním poverených osôb môže, po konzultácii s Národnou komisiou pre kontrolu spravodajských metód za podmienok stanovených v kapitole I hlavy II tejto knihy, povoliť identifikáciu dotknutej osoby alebo osôb a zber súvisiacich údajov. Tieto údaje sa využívajú po dobu 60 dní odo dňa tohto zberu a po uplynutí tejto lehoty sa zničia, pokiaľ neexistujú závažné skutočnosti potvrdzujúce existenciu teroristickej hrozby spojenej s jednou alebo viacerými dotknutými osobami.

…“

44 Článok L. 851-4 CSI znie:

„Za podmienok stanovených v kapitole I hlavy II tejto knihy môžu byť technické údaje o polohe použitých koncových zariadení uvedené v článku L. 851-1 zozbierané na požiadanie zo siete a prenášané prevádzkovateľmi v reálnom čase oddeleniu predsedu vlády.“

45 Článok R. 851-5 CSI, ktorý sa nachádza v regulačnej časti tohto zákonníka, stanovuje:

„I. – Informácie alebo dokumenty uvedené v článku L. 851-1 sú s výnimkou obsahu prijatej alebo odoslanej korešpondencie alebo konzultovaných informácií tieto:

1. Údaje vymenované v článkoch R. 10-13 a R. 10-14 [CPCE] a v článku 1 dekrétu [č. 2011-219];

2. Technické údaje iné ako údaje uvedené v bode 1:

a) umožňujúce lokalizovať koncové zariadenia;

b) týkajúce sa prístupu koncových zariadení k verejným komunikačným sieťam alebo verejne dostupným komunikačným službám online;

c) týkajúce sa prenosu elektronických komunikácií prostredníctvom sietí;

d) týkajúce sa identifikácie a overenia používateľa, pripojenia, verejnej komunikačnej siete alebo verejne dostupnej komunikačnej služby online;

e) týkajúce sa charakteristík koncových zariadení a konfiguračných údajov ich softvéru.

II. – Na základe článku L. 851-1 možno zbierať len informácie a dokumenty uvedené v odseku I. bode 1. Tento zber sa uskutočňuje s časovým odstupom.

Informácie uvedené v odseku I bode 2 možno zbierať iba na základe článkov L. 851-2 a L. 851-3 za podmienok a v medziach stanovených týmito článkami a s výhradou uplatnenia článku R. 851-9.“

Zákonník pôšt a elektronických komunikácií (CPCE)

46 Článok L. 34-1 CPCE stanovuje:

„I. – Tento článok sa vzťahuje na spracovávanie osobných údajov pri poskytovaní elektronických komunikačných služieb verejnosti; vzťahuje sa najmä na siete, ktoré využívajú zariadenia na zber údajov a identifikačné zariadenia.

II. – Bez toho, aby boli dotknuté odseky III, IV, V a VI, prevádzkovatelia elektronických komunikácií a najmä osoby, ktorých činnosť spočíva v poskytovaní prístupu verejnosti ku komunikačným službám online, vymažú alebo anonymizujú všetky údaje o prenose dát.

Osoby, ktoré poskytujú verejnosti elektronické komunikačné služby, zavedú v súlade s predchádzajúcim pododsekom interné postupy na spracovanie žiadostí príslušných orgánov.

Osoby, ktoré v rámci hlavnej alebo vedľajšej podnikateľskej činnosti poskytujú verejnosti pripojenie, ktoré umožňuje komunikáciu online prostredníctvom prístupu k sieti, a to aj bezodplatne, musia dodržiavať ustanovenia vzťahujúce sa na prevádzkovateľov elektronických komunikácií na základe tohto článku.

III. – Na účely vyšetrovania, odhaľovania a stíhania trestných činov alebo porušenia povinnosti vymedzenej v článku L. 336-3 Code de la propriété intellectuelle [(Zákonník duševného vlastníctva)] alebo na účely predchádzania útokom na systémy automatizovaného spracovávania údajov stanoveným a sankcionovaným v článkoch 323-1 až 323-3-1 Code pénal [(Trestný zákon)] a len s cieľom umožniť v prípade potreby poskytnutie súdnemu orgánu alebo vysokému orgánu uvedenému v článku L. 331-12 Zákonníka duševného vlastníctva alebo národnému orgánu pre bezpečnosť informačných systémov uvedenému v článku L. 2321-1 Code de la défense [(Obranný zákonník)] možno úkony zamerané na vymazanie alebo anonymizáciu určitých kategórií technických údajov odložiť najdlhšie o jeden rok. Dekrétom prerokovaným v Conseil d'État [(Štátna rada)], prijatým po stanovisku Národnej komisie pre informačné technológie a občianske slobody, sa v medziach stanovených v odseku VI určia tieto kategórie údajov a doba ich uchovávania podľa činnosti prevádzkovateľov a povahy komunikácie, ako aj podmienky náhrady prípadných dodatočných nákladov, ktoré možno určiť a ktoré konkrétne súvisia so službami, ktoré prevádzkovatelia z tohto dôvodu zabezpečujú na žiadosť štátu.

…

VI. – Údaje uchovávané a spracovávané za podmienok stanovených v odsekoch III, IV a V sa týkajú výlučne identifikácie používateľov služieb poskytovaných prevádzkovateľmi, technických vlastností komunikácie zabezpečovanej prevádzkovateľmi a polohy koncových zariadení.

V nijakom prípade sa nemôžu týkať obsahu prijatej alebo odoslanej korešpondencie alebo informácií konzultovaných v akejkoľvek forme v rámci tejto komunikácie.

Uchovávanie a spracovávanie údajov sa uskutočňuje v súlade s ustanoveniami loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [(zákon č. 78-17 zo 6. januára 1978 o informatike, súboroch a slobodách)].

Prevádzkovatelia prijmú všetky opatrenia s cieľom zabrániť využívaniu týchto údajov na iné účely než tie, ktoré sú uvedené v tomto článku.“

47 Článok R. 10-13 CPCE znie:

„I. – Podľa článku L. 34-1 ods. III prevádzkovatelia na účely vyšetrovania, odhaľovania a stíhania trestných činov uchovávajú nasledujúce údaje:

a) informácie, ktoré umožňujú identifikovať používateľa;

b) údaje o použitých koncových komunikačných zariadeniach;

c) technické vlastnosti, ako aj dátum, čas a dĺžku trvania každej komunikácie;

d) údaje o vyžiadaných alebo použitých doplnkových službách a ich poskytovateľoch;

e) údaje, ktoré umožňujú identifikovať jedného alebo viacerých adresátov komunikácie.

II. – V prípade telefonických činností prevádzkovateľ uchováva údaje uvedené v odseku II a navyše aj tie, ktoré umožnia identifikovať pôvod a miesto komunikácie.

III. – Doba uchovávania údajov uvedených v tomto článku je jeden rok odo dňa ich zaznamenania.

IV. – Identifikovateľné a konkrétne dodatočné náklady, ktoré vzniknú prevádzkovateľom, od ktorých si súdne orgány vyžiadali údaje patriace do kategórií uvedených v tomto článku, sú hradené v súlade s podmienkami stanoveným v článku R. 213-1 Code de procédure pénale [(Trestný poriadok)].“

48 Článok R. 10-14 CPCE stanovuje:

„I. – Podľa článku L. 34-1 ods. IV sú prevádzkovatelia elektronických komunikácií oprávnení uchovávať technické údaje umožňujúce identifikovať používateľa a údaje uvedené v článku R. 10-13 ods. I písm. b), c) a d) pre potreby svojich fakturačných a platobných transakcií.

II. – V prípade telefonických činností môžu prevádzkovatelia uchovávať okrem údajov uvedených v odseku I aj technické údaje týkajúce sa miesta komunikácie, identifikácie jedného alebo viacerých adresátov komunikácie a údaje pre potreby fakturácie.

III. – Údaje uvedené v odsekoch I a II tohto článku sa uchovávajú len vtedy, ak je to potrebné na fakturáciu a platby za poskytnuté služby. Ich uchovávanie sa musí obmedziť na čas nevyhnutne potrebný na tento účel, nie však dlhšie ako jeden rok.

IV. – Prevádzkovatelia môžu na zaistenie bezpečnosti sietí a zariadení uchovávať po dobu najviac tri mesiace tieto údaje:

a) údaje umožňujúce identifikovať pôvod komunikácie;

b) technické vlastnosti, ako aj dátum, čas a dĺžku trvania každej komunikácie;

c) technické údaje, ktoré umožňujú identifikovať jedného alebo viacerých adresátov komunikácie;

d) údaje o vyžiadaných alebo použitých doplnkových službách a ich poskytovateľoch.“

Zákon č. 2004-575 z 21. júna 2004 o dôvere v digitálne hospodárstvo

49 Článok 6 loi nº 2004-575, du 21 juin 2004, pour la confiance dans l’économie numérique (zákon č. 2004-575 z 21. júna 2004 o dôvere v digitálne hospodárstvo) (JORF z 22. júna 2004, s. 11168, ďalej len „LCEN“) stanovuje:

„I. – 1. Osoby, ktorých činnosť spočíva v poskytovaní prístupu verejnosti ku komunikačným službám online, informujú účastníkov o existencii technických nástrojov umožňujúcich obmedziť prístup k určitým službám alebo si ich vybrať a ponúknu im aspoň jeden z týchto nástrojov.

…

2. Fyzické alebo právnické osoby, ktoré pre verejnosť prostredníctvom verejných komunikačných služieb online, a to aj bezodplatne, zabezpečujú uchovávanie signálov, písaného textu, obrázkov a zvukov alebo správ akéhokoľvek druhu dodaných príjemcami týchto služieb, nemôžu niesť

zodpovednosť za škodu spôsobenú činnosťami alebo informáciami uloženými na žiadosť príjemcu týchto služieb, ak nič nevedeli o ich nezákonnej povahe alebo si neboli vedomí skutočností alebo okolností, z ktorých by bola zrejmá táto povaha, alebo ak od okamihu, keď sa dozvedeli o tejto nezákonnej povahe, konali urýchlene s cieľom odstrániť tieto údaje alebo znemožniť k nim prístup.

…

II. – Osoby uvedené v odseku I bodoch 1 a 2 ukladajú a uchovávajú údaje umožňujúce zistiť, kto prispel k tvorbe obsahu alebo jedného z obsahov služieb, ktorých sú poskytovateľmi.

Poskytnú osobám, ktoré publikujú vo verejne dostupnej komunikačnej službe online, technické prostriedky, ktoré im umožnia splniť podmienky identifikácie stanovené v odseku III.

Súdny orgán môže od poskytovateľov uvedených v odseku I bodoch 1 a 2 vyžadovať poskytnutie údajov uvedených v prvom pododseku.

Na spracovanie týchto údajov sa vzťahujú ustanovenia článkov 226-17, 226-21 a 226-22 Trestného zákona.

Dekrétom Conseil d'État [(Štátna rada)], prijatom po konzultácii s Národnou komisiou pre informačné technológie a občianske slobody, sa vymedzia údaje uvedené v prvom pododseku a stanoví sa doba a podmienky ich uchovávania.

…“

Dekrét č. 2011-219

50 Kapitola I dekrétu č. 2011-219 prijatého na základe článku 6 ods. II posledného pododseku LCEN obsahuje články 1 až 4 tohto dekrétu.

51 Článok 1 dekrétu č. 2011-219 stanovuje:

„Údajmi uvedenými v článku 6 ods. II [LCEN], ktoré sú osoby povinné uchovávať na základe tohto ustanovenia, sú tieto údaje:

1. V prípade osôb uvedených v odseku I bode 1 toho istého článku a pre každé pripojenie ich účastníkov:

a) identifikátor pripojenia;

b) identifikátor priradený týmito osobami účastníkovi;

c) identifikátor koncového zariadenia použitého pri pripojení, ak k nemu majú prístup;

d) dátum a čas začatia a ukončenia pripojenia;

e) vlastnosti linky účastníka.

2. V prípade osôb uvedených v odseku I bode 2 toho istého článku a pre každú operáciu vytvárania obsahu:

a) identifikátor pripojenia na začiatku komunikácie;

b) identifikátor priradený informačným systémom obsahu, ktorý je predmetom operácie;

c) typy protokolov použitých na pripojenie k službe a na prenos obsahu;

d) povaha operácie;

e) dátum a čas operácie;

f) identifikátor použitý autorom operácie pri jej poskytnutí.

3. V prípade osôb uvedených v odseku I bodoch 1 a 2 toho istého článku informácie, ktoré používateľ poskytol pri uzatvorení zmluvy alebo vytvorení účtu:

a) identifikátor pripojenia v čase vytvorenia účtu;

b) meno, priezvisko alebo obchodné meno;

c) súvisiace poštové adresy;

d) použité aliasy;

e) súvisiace e-mailové adresy a adresy účtu;

f) telefónne čísla;

g) aktuálne heslo a údaje, ktoré ho umožňujú overiť alebo zmeniť.

4. V prípade osôb uvedených v odseku I bodoch 1 a 2 toho istého článku, ak je podpísanie zmluvy alebo vytvorenie účtu spoplatnené, nasledujúce informácie týkajúce sa platby, za každú platobnú transakciu:

a) druh použitej platby;

b) referenčné číslo platby;

c) suma;

d) dátum a čas transakcie.

Údaje uvedené v bodoch 3 a 4 sa majú uchovávať len v rozsahu, v akom ich osoby zvyčajne zbierajú.“

52 Článok 2 tohto dekrétu znie:

„Prispievanie k tvorbe obsahu zahŕňa tieto operácie:

a) počiatočné vytváranie obsahu;

b) zmeny obsahu a údajov súvisiacich s obsahom;

c) vymazanie obsahu.“

53 Článok 3 uvedeného dekrétu stanovuje:

„Doba uchovávania údajov uvedených v článku 1 je jeden rok odo dňa:

a) vytvorenia obsahu, pre každú operáciu prispievajúcu k vytvoreniu obsahu v zmysle článku 2, pokiaľ ide o údaje uvedené v bodoch 1 a 2;

b) ukončenia zmluvy alebo uzavretia účtu, pokiaľ ide o údaje uvedené v bode 3;

c) vystavenia faktúry alebo platobnej transakcie, pre každú faktúru alebo platobnú transakciu, pokiaľ ide o údaje uvedené v bode 4.“

Belgické právo

54 Zákon z 29. mája 2016 zmenil najmä loi du 13 juin 2005 relative aux communications électroniques (zákon z 13. júna 2005 o elektronických komunikáciách) (*Moniteur belge* z 20. júna 2005, s. 28070, ďalej len „zákon z 13. júna 2005“), Code d'instruction criminelle (Trestný poriadok) a loi du 30 novembre 1998 organique des services de renseignement et de sécurité (organický zákon z 30. novembra 1998 o spravodajských a bezpečnostných službách) (*Moniteur belge* z 18. decembra 1998, s. 40312, ďalej len „zákon z 30. novembra 1998“).

55 Článok 126 zákona z 13. júna 2005 v znení zákona z 29. mája 2016 stanovuje:

„(1) Bez toho, aby boli dotknuté ustanovenia loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel [(zákon z 8. decembra 1992 o ochrane súkromného života s ohľadom na spracovanie osobných údajov)], poskytovatelia verejných telefonických služieb, vrátane telefonických služieb cez internet, pripojenia na internet, elektronickej pošty cez internet, operátori, ktorí prevádzkujú verejné elektronické komunikačné siete, ako aj operátori poskytujúci niektorú z týchto služieb uchovávajú údaje uvedené v odseku 3, ktoré vytvárajú alebo spracúvajú v rámci poskytovania predmetných komunikačných služieb.

Tento článok sa nevzťahuje na obsah komunikácie.

Povinnosť uchovávať údaje uvedené v odseku 3 sa vzťahuje aj na neúspešné volania, ak sú tieto údaje v rámci poskytovania príslušných komunikačných služieb:

1. vytvárané alebo spracúvané poskytovateľmi verejne dostupných elektronických komunikačných služieb alebo verejnej elektronickej komunikačnej siete, pokiaľ ide o telefónne údaje, alebo

2. zaznamenané týmito poskytovateľmi, pokiaľ ide o internetové údaje.

(2) Iba nasledujúce orgány sú na základe jednoduchej žiadosti oprávnené získať od poskytovateľov a operátorov uvedených v odseku 1 prvom pododseku údaje uchovávané podľa tohto článku na účely a za podmienok uvedených nižšie:

1. súdne orgány na účely pátrania, vyšetrovania a stíhania trestných činov, na účely vykonania opatrení uvedených v článkoch 46a a 88a Code d'instruction criminelle [(Trestný poriadok)] a za podmienok uvedených v týchto článkoch;

2. spravodajské a bezpečnostné služby na plnenie spravodajských úloh pomocou metód zberu údajov uvedených v článkoch 16/2, 18/7 a 18/8 [zákona z 30. novembra 1998] a za podmienok stanovených týmto zákonom;

3. každý príslušník justičnej polície Institut belge des services postaux et des télécommunications [(Belgický inštitút pre poštové služby a telekomunikácie)] na účely pátrania, vyšetrovania a stíhania porušení článkov 114, 124 a tohto článku;

4. tiesňové služby, ktoré poskytujú pomoc na mieste, ak po uskutočnení tiesňového hovoru nezískajú od príslušného poskytovateľa alebo operátora identifikačné údaje volajúceho pomocou databázy uvedenej v článku 107 ods. 2 pododseku 3 alebo získajú neúplné alebo nesprávne údaje. Možno požadovať výlučne identifikačné údaje volajúceho, a to najneskôr do 24 hodín od uskutočnenia hovoru;

5. príslušník justičnej polície Cellule des personnes disparues de la Police Fédérale [(Jednotka nezvestných osôb Federálnej polície)] v rámci plnenia svojej úlohy spočívajúcej v poskytnutí pomoci ohrozenej osobe, v pátraní po osobách, ktorých zmiznutie je znepokojujúce, pokiaľ existuje predpoklad alebo dôvodné podozrenie, že je bezprostredne ohrozená telesná integrita nezvestnej osoby. Príslušník policajného útvaru povereného kráľom môže operátora alebo poskytovateľa žiadať výlučne o poskytnutie údajov o nezvestnej osobe uvedených v odseku 3 prvom a druhom pododseku, ktoré boli uchovávané počas 48 hodín pred predložením žiadosti o poskytnutie údajov;

6. Service de médiation pour les télécommunications [(Mediačná služba pre oblasť telekomunikácií)] na účely identifikácie osoby, ktorá zneužila sieť alebo službu elektronickej komunikácie, v súlade s podmienkami uvedenými v článku 43a ods. 3 bode 7 loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques [(zákon z 21. marca 1991 o reforme niektorých štátnych hospodárskych podnikov)]. Možno žiadať výlučne o identifikačné údaje.

Poskytovatelia a operátori uvedení v odseku 1 prvom pododseku zabezpečia, aby boli údaje uvedené v odseku 3 dostupné bez obmedzení z územia Belgicka a aby bolo tieto údaje a akékoľvek iné potrebné informácie týkajúce sa týchto údajov možné poskytnúť bezodkladne a výlučne orgánom uvedeným v tomto odseku.

Bez toho, aby tým boli dotknuté iné zákonné ustanovenia, poskytovatelia a operátori uvedení v odseku 1 prvom pododseku nie sú oprávnení použiť údaje uchovávané v zmysle odseku 3 na iné účely.

(3) Údaje umožňujúce identifikáciu používateľa alebo účastníka a komunikačných prostriedkov, okrem údajov osobitne uvedených v druhom a treťom pododseku, sa uchovávajú po dobu dvanástich mesiacov odo dňa, keď sa komunikácia môže s pomocou využívanej služby uskutočniť posledný krát.

Údaje o prístupe a pripojení koncového zariadenia k sieti a k službe, ako aj údaje o polohe tohto zariadenia, vrátane koncového bodu siete, sa uchovávajú po dobu dvanástich mesiacov od dátumu komunikácie.

Údaje o komunikácii okrem obsahu, vrátane ich pôvodu a cieľa, sa uchovávajú po dobu dvanástich mesiacov od dátumu komunikácie.

Kráľ nariadením prijatým Conseil des ministres [(Rada ministrov)] na návrh ministre de la Justice [(minister spravodlivosti)] a ministra [príslušného pre oblasť elektronických komunikácií] po vyjadrení Commission de la protection de la vie privée [(Komisia pre ochranu súkromia)] a Inštitútu určí údaje, ktoré sa majú uchovávať v každej z kategórií uvedených v prvom až treťom pododseku, spolu s požiadavkami, ktoré musia tieto údaje spĺňať.

…“

Spory vo veciach samých a prejudiciálne otázky

Vec C-511/18

56 Návrhmi podanými 30. novembra 2015 a 16. marca 2016, ktoré boli spojené do konania vo veci samej, La Quadrature du Net, French Data Network, Igwan.net a Fédération des fournisseurs d'accès à Internet associatifs podali na Conseil d'État (Štátna rada, Francúzsko) žaloby, ktorými sa domáhali zrušenia dekrétov č. 2015-1185, 2015-1211, 2015-1639 a 2016-67 najmä z dôvodu, že porušujú francúzsku ústavu, Európsky dohovor o ochrane ľudských práv a základných slobôd (ďalej len „EDĽP"), ako aj smernice 2000/31 a 2002/58 v spojení s článkami 7, 8 a 47 Charty.

57 Pokiaľ ide konkrétne o žalobné dôvody založené na porušení smernice 2000/31, vnútroštátny súd uvádza, že ustanovenia článku L. 851-3 CSI ukladajú prevádzkovateľom elektronických komunikácií a poskytovateľom technických služieb povinnosť „zaviesť automatizované procesy spracovávania v ich sieťach na zisťovanie pripojení, ktoré by mohli predstavovať teroristickú hrozbu, v závislosti od parametrov určených v povolení". Cieľom tejto metódy je vyzbierať výlučne počas obmedzenej doby spomedzi všetkých údajov o pripojení spracúvaných týmito prevádzkovateľmi a poskytovateľmi len tie údaje, ktoré by mohli súvisieť s takýmto závažným trestným činom. Za týchto podmienok, uvedené ustanovenia, ktoré neukladajú všeobecnú povinnosť aktívneho monitorovania, nie sú podľa názoru vnútroštátneho súdu v rozpore s článkom 15 smernice 2000/31.

58 Pokiaľ ide o žalobné dôvody založené na porušení smernice 2002/58, vnútroštátny súd zastáva názor, že predovšetkým z ustanovení tejto smernice a z rozsudku z 21. decembra 2016, Tele2 Sverige a Watson a i. (C-203/15 a C-698/15, ďalej len „rozsudok Tele2", EU:C:2016:970), vyplýva, že vnútroštátne ustanovenia ukladajúce povinnosti poskytovateľom elektronických komunikačných služieb, ako napríklad všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe ich používateľov a účastníkov na účely uvedené v článku 15 ods. 1 uvedenej smernice, medzi ktoré patria ochrana národnej bezpečnosti, obrana a verejná bezpečnosť, patria do pôsobnosti tej istej smernice, keďže upravujú činnosť uvedených poskytovateľov. To isté platí pre právne predpisy upravujúce prístup vnútroštátnych orgánov k údajom a ich využívanie.

59 Vnútroštátny súd z toho vyvodzuje, že do pôsobnosti smernice 2002/58 patrí jednak povinnosť uchovávať údaje vyplývajúca z článku L. 851-1 CSI, ako aj administratívny prístup k týmto údajom, vrátane prístupu v reálnom čase, stanovený v článkoch L. 851-1, L. 851-2 a L. 851-4 uvedeného zákonníka. To isté platí podľa tohto súdu aj o ustanoveniach článku L. 851-3 toho istého zákonníka, ktoré síce pre dotknutých prevádzkovateľov nestanovujú všeobecnú povinnosť uchovávať údaje, ukladajú im však povinnosť zaviesť automatizované procesy spracovávania v ich sieťach na zisťovanie pripojení, ktoré by mohli predstavovať teroristickú hrozbu.

60 Na druhej strane vnútroštátny súd zastáva názor, že do pôsobnosti smernice 2002/58 nepatria ustanovenia CSI uvedené v žalobách o neplatnosť, ktoré sa týkajú metód zberu spravodajských informácií, ktoré uplatňuje priamo štát bez toho, aby upravoval činnosti poskytovateľov elektronických komunikačných služieb tým, že by im ukladal osobitné povinnosti. Tieto ustanovenia sa teda nemôžu považovať za ustanovenia, ktorými sa vykonáva právo Únie, takže nemožno účinne uplatňovať žalobné dôvody založené na tom, že tieto ustanovenia porušujú smernicu 2002/58.

61 S cieľom vyriešiť spory týkajúce sa zákonnosti dekrétov č. 2015-1185, 2015-1211, 2015-1639 a 2016-67 z hľadiska smernice 2002/58 v rozsahu, v akom boli prijaté na vykonanie článkov L. 851-1 až L. 851-4 CSI, tak vyvstávajú tri otázky výkladu práva Únie.

62 V prvom rade, pokiaľ ide o výklad článku 15 ods. 1 smernice 2002/58, vnútroštátny súd sa pýta, či povinnosť všeobecného a nediferencovaného uchovávania údajov, uloženú poskytovateľom elektronických komunikačných služieb na základe článkov L. 851-1 a R. 851-5 CSI, nemožno

považovať najmä vzhľadom na záruky a kontroly, ktoré sú spojené s administratívnym prístupom k údajom o pripojení a ich využívaním, za zásah odôvodnený právom na bezpečnosť zaručeným v článku 6 Charty a požiadavkami národnej bezpečnosti, za ktorú podľa článku 4 ZEÚ nesú zodpovednosť len členské štáty.

63 V druhom rade, pokiaľ ide o ďalšie povinnosti, ktoré môžu byť uložené poskytovateľom elektronických komunikačných služieb, vnútroštátny súd uvádza, že ustanovenia článku L. 851-2 CSI povoľujú výlučne na účely predchádzania terorizmu zber informácií alebo dokumentov uvedených v článku L. 851-1 tohto zákonníka od tých istých osôb. Tento zber, ktorý sa týka len jedného alebo viacerých jednotlivcov vopred označených ako osoby, v prípade ktorých existuje podozrenie, že majú väzbu s teroristickou hrozbou, sa uskutočňuje v reálnom čase. To isté platí aj pre článok L. 851-4 uvedeného zákonníka, ktorý dovoľuje, aby prevádzkovatelia v reálnom čase prenášali len technické údaje týkajúce sa polohy koncových zariadení. Tieto metódy upravujú administratívny prístup v reálnom čase k údajom uchovávaným na základe CPCE a LCEN na rôzne účely a rôznymi prostriedkami bez toho, aby dotknutým poskytovateľom ukladali ďalšie požiadavky uchovávania nad rámec toho, čo je potrebné na fakturáciu a poskytovanie ich služieb. Rovnako ani ustanovenia článku L. 851-3 CSI, ktoré poskytovateľom služieb ukladajú povinnosť zaviesť automatizovanú analýzu pripojení v ich sieťach, nezahŕňajú povinnosť všeobecného a nediferencovaného uchovávania.

64 Vnútroštátny súd na jednej strane zastáva názor, že všeobecné a nediferencované uchovávanie a prístup k údajom o pripojení v reálnom čase sú v kontexte poznačenom vážnymi a pretrvávajúcimi hrozbami pre národnú bezpečnosť, najmä pokiaľ ide o riziko terorizmu, bezkonkurenčne operatívne užitočné. Všeobecné a nediferencované uchovávanie totiž umožňuje spravodajským službám získať prístup k údajom týkajúcim sa komunikácií ešte pred tým, ako sa identifikujú dôvody domnienky, že predstavuje hrozbu pre verejnú bezpečnosť, obranu alebo bezpečnosť štátu. Okrem toho prístup k údajom o pripojení v reálnom čase umožňuje s vysokou reakčnou schopnosťou sledovať správanie jednotlivcov, ktorí by mohli predstavovať bezprostrednú hrozbu pre verejný poriadok.

65 Na druhej strane metóda stanovená v článku L. 851-3 CSI umožňuje na základe kritérií osobitne vymedzených na tento účel zistiť jednotlivcov, ktorých správanie môže vzhľadom na ich spôsob komunikácie odhaliť teroristickú hrozbu.

66 V treťom rade, pokiaľ ide o prístup príslušných orgánov k uchovávaným údajom, vnútroštátny súd sa pýta, či sa má smernica 2002/58 v spojení s Chartou vykladať v tom zmysle, že v každom prípade podmieňuje zákonnosť postupov zberu údajov o pripojení požiadavkou informovania dotknutých osôb, pokiaľ takáto informácia už nemôže ohroziť vyšetrovanie vedené príslušnými orgánmi, alebo či sa takéto postupy môžu považovať za zákonné vzhľadom na všetky ostatné existujúce procesné záruky stanovené vo vnútroštátnom práve, ak tieto záruky zabezpečujú účinnosť práva na prostriedok nápravy.

67 Pokiaľ ide o tieto ďalšie procesné záruky, vnútroštátny súd predovšetkým uvádza, že každá osoba, ktorá chce overiť, že vo vzťahu k nej nebola protiprávne použitá žiadna spravodajská metóda, sa môže obrátiť na špecializovaný súdny útvar Conseil d'État (Štátna rada), ktorému prináleží overiť, vzhľadom na skutočnosti, ktoré sú mu oznámené v rámci konania, kde sa neuplatňuje zásada kontradiktórnosti, či sa na žiadateľa vzťahovala určitá spravodajská metóda a či bola táto metóda použitá v súlade s knihou VIII CSI. Právomoci zverené tomuto útvaru na prešetrovanie žiadostí zaručujú účinnosť súdneho preskúmania, ktoré vykonáva. Má totiž právomoc prešetrovať žiadosti, preskúmať *ex offo* všetky nezákonnosti, ktoré zistí, a nariadiť správnemu orgánu, aby prijal všetky potrebné opatrenia na účely nápravy zistených nezákonností. Okrem toho Národnej komisii pre kontrolu spravodajských metód prináleží overovať, či sú metódy zberu spravodajských informácií na vnútroštátnom území vykonávané v súlade s požiadavkami vyplývajúcimi z CSI. Okolnosť, že legislatívne ustanovenia, o ktoré ide vo veci samej, nestanovujú oznámenie dotknutým osobám o opatreniach dohľadu, ktorým boli vystavení, teda sama osebe nepredstavuje nadmerný zásah do práva na rešpektovanie súkromného života.

68 Za týchto podmienok Conseil d'État (Štátna rada) rozhodla prerušiť konanie a položiť Súdnemu dvoru tieto prejudiciálne otázky:

„1. Má sa povinnosť všeobecného a nediferencovaného uchovávania, uložená poskytovateľom na základe ustanovení článku 15 ods. 1 smernice [2002/58], považovať v kontexte, ktorý sa vyznačuje vážnymi a pretrvávajúcimi hrozbami pre národnú bezpečnosť, najmä rizikom terorizmu, za zásah odôvodnený právom na bezpečnosť zaručeným v článku 6 [Charty] a požiadavkami národnej bezpečnosti, za ktorú podľa článku 4 [ZEÚ] nesú zodpovednosť len členské štáty?

2. Má sa smernica [2002/58] v spojení s [Chartou] vykladať v tom zmysle, že povoľuje legislatívne opatrenia, akými sú opatrenia týkajúce sa zberu údajov o prenose dát a polohe určitých jednotlivcov v reálnom čase, ktoré síce zasahujú do práv a povinností poskytovateľov elektronických komunikačných služieb, no neukladajú im konkrétnu povinnosť uchovávať ich údaje?

3. Má sa smernica [2002/58] v spojení s [Chartou] vykladať v tom zmysle, že v každom prípade podmieňuje zákonnosť postupov zberu údajov o pripojení požiadavkou informovania dotknutých osôb, pokiaľ takáto informácia už nemôže ohroziť vyšetrovanie vedené príslušnými orgánmi, alebo takéto postupy sa môžu považovať za zákonné vzhľadom na všetky ostatné existujúce procesné záruky za predpokladu, že tieto záruky zabezpečujú účinnosť práva na prostriedok nápravy?“

Vec C-512/18

69 Návrhom podaným 1. septembra 2015 French Data Network, La Quadrature du Net a Fédération des fournisseurs d'accès à Internet associatifs podali na Conseil d'État (Štátna rada) žalobu o neplatnosť implicitného rozhodnutia o zamietnutí vyplývajúceho z nečinnosti predsedu vlády vo vzťahu k ich žiadosti o zrušenie článku R. 10-13 CPCE a dekrétu č. 2011-219 najmä z dôvodu, že tieto legislatívne texty porušujú článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11 Charty. Privacy International a Center for Democracy and Technology bol umožnený vstup do konania vo veci samej ako vedľajším účastníkom.

70 Pokiaľ ide o článok R. 10-13 CPCE a v ňom stanovenú povinnosť všeobecného a nediferencovaného uchovávania údajov týkajúcich sa komunikácií, vnútroštátny súd, ktorý vyjadruje podobné úvahy ako vo veci C-511/18, poznamenáva, že takéto uchovávanie umožňuje súdnym orgánom získať prístup k údajom týkajúcim sa komunikácií, ktoré jednotlivec vykonal skôr, než sa stal podozrivým zo spáchania trestného činu, takže takéto uchovávanie je bezkonkurenčne užitočné pre vyšetrovanie, odhaľovanie a stíhanie trestných činov.

71 Pokiaľ ide o dekrét č. 2011-219, vnútroštátny súd zastáva názor, že článok 6 ods. II LCEN, ktorý stanovuje povinnosť ukladať a uchovávať len údaje týkajúce sa tvorby obsahu, nepatrí do pôsobnosti smernice 2002/58, keďže pôsobnosť tejto smernice je podľa jej článku 3 ods. 1 obmedzená na poskytovanie verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach v Únii, ale naopak patrí do pôsobnosti smernice 2000/31.

72 Tento súd sa však domnieva, že z článku 15 ods. 1 a 2 smernice 2000/31 vyplýva, že táto smernica nestanovuje zásadný zákaz uchovávania údajov týkajúcich sa tvorby obsahu, od ktorého by bolo možné sa odchýliť len výnimočne. Vyvstáva teda otázka, či sa články 12, 14 a 15 uvedenej smernice v spojení s článkami 6 až 8 a 11, ako aj s článkom 52 ods. 1 Charty majú vykladať v tom zmysle, že umožňujú členskému štátu zaviesť takú vnútroštátnu právnu úpravu, akou je článok 6 ods. II LCEN, ktorá ukladá dotknutým osobám povinnosť uchovávať údaje umožňujúce zistiť, kto prispel k tvorbe obsahu alebo jedného z obsahov služieb, ktorých sú poskytovateľmi, aby súdny orgán mohol prípadne požiadať o ich poskytnutie na účely uplatňovania predpisov týkajúcich sa občianskoprávnej alebo trestnej zodpovednosti.

73 Za týchto podmienok Conseil d'État (Štátna rada) rozhodla prerušiť konanie a položiť Súdnemu dvoru tieto prejudiciálne otázky:

„1. Má sa povinnosť všeobecného a nediferencovaného uchovávania, uložená poskytovateľom na základe ustanovení článku 15 ods. 1 smernice [2002/58], považovať najmä vzhľadom na záruky a kontroly, ktoré sú spojené so zberom a použitím týchto údajov o pripojení, za zásah odôvodnený právom na bezpečnosť zaručeným v článku 6 [Charty] a požiadavkami národnej bezpečnosti, za ktorú podľa článku 4 [ZEÚ] nesú zodpovednosť len členské štáty?

2. Majú sa ustanovenia smernice [2000/31] v spojení s článkami 6, 7, 8 a 11, ako aj článkom 52 ods. 1 [Charty] vykladať v tom zmysle, že umožňujú členskému štátu zaviesť vnútroštátnu právnu úpravu, ktorá ukladá osobám, ktorých činnosť spočíva v poskytovaní prístupu verejnosti ku komunikačným službám online, a fyzickým alebo právnickým osobám, ktoré na účely poskytovania verejnosti prostredníctvom verejných komunikačných služieb online, a to aj bezodplatne, zabezpečujú uchovávanie signálov, písaného textu, obrázkov a zvukov alebo správ akéhokoľvek druhu dodaných príjemcami týchto služieb, povinnosť uchovávať údaje umožňujúce zistiť, kto prispel k tvorbe obsahu alebo jedného z obsahov služieb, ktorých sú poskytovateľmi, aby súdny orgán mohol prípadne požiadať o ich poskytnutie na účely uplatňovania predpisov týkajúcich sa občianskoprávnej alebo trestnej zodpovednosti?“

Vec C-520/18

74 Návrhmi podanými 10. januára, 16. januára, 17. januára a 18. januára 2017, ktoré boli spojené do konania vo veci samej, Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL a UA, Liga voor Mensenrechten ASBL a Ligue des Droits de l'Homme ASBL, ako aj VZ, WY a XX podali na Cour constitutionnelle (Ústavný súd, Belgicko) žaloby o neplatnosť zákona z 29. mája 2016 z dôvodu, že tento zákon porušuje články 10 a 11 belgickej ústavy v spojení s článkami 5, 6 až 11, 14, 15, 17 a 18 EDĽP, článkami 7, 8, 11, 47 a článkom 52 ods. 1 Charty, článkom 17 Medzinárodného paktu o občianskych a politických právach prijatého Valným zhromaždením Organizácie Spojených národov 16. decembra 1966, ktorý nadobudol platnosť 23. marca 1976, všeobecnými zásadami právnej istoty, proporcionality a sebaurčenia v oblasti informácií a článkom 5 ods. 4 ZEÚ.

75 Na podporu svojich žalôb žalobcovia vo veci samej v podstate tvrdia, že protiprávnosť zákona z 29. mája 2016 sa týka najmä skutočnosti, že tento zákon ide nad rámec toho, čo je prísne nevyhnutné, a nestanovuje dostatočné záruky ochrany. Konkrétne jeho ustanovenia týkajúce sa uchovávania údajov, ani tie, ktoré upravujú prístup orgánov k uchovávaným údajom, nespĺňajú požiadavky vyplývajúce z rozsudkov z 8. apríla 2014, Digital Rights Ireland a i. (C-293/12 a C-594/12, ďalej len „rozsudok Digital Rights“, EU:C:2014:238), a z 21. decembra 2016, Tele2 (C-203/15 a C-698/15, EU:C:2016:970). Tvrdia totiž, že tieto ustanovenia so sebou nesú riziko, že budú vytvorené osobnostné profily, ktoré môžu byť zneužité zo strany príslušných orgánov, a že nestanovujú primeranú úroveň zabezpečenia a ochrany uchovávaných údajov. Napokon sa podľa nich tento zákon vzťahuje rovnako na osoby viazané profesijným tajomstvom a osoby, ktoré majú povinnosť zachovávať mlčanlivosť, a týka sa citlivých osobných údajov o komunikácii, pričom neobsahuje osobitné záruky na účely ochrany týchto údajov.

76 Vnútroštátny súd uvádza, že údaje, ktoré majú podľa zákona z 29. mája 2016 uchovávať poskytovatelia telefonických služieb, vrátane telefonických služieb cez internet, pripojenia na internet, elektronickej pošty cez internet, a prevádzkovatelia, ktorí poskytujú verejné elektronické komunikačné siete, sú totožné s údajmi vymenovanými v smernici Európskeho parlamentu a Rady 2006/24/ES z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES (Ú. v. EÚ L 105, 2006, s. 54) bez toho, že by sa stanovilo rozlišovanie medzi dotknutými osobami alebo na základe sledovaného cieľa. V tejto poslednej uvedenej súvislosti

vnútroštátny súd uvádza, že cieľ, ktorý zákonodarca sleduje prijatím tohto zákona nespočíva iba v boji proti terorizmu a detskej pornografii, ale aj v umožnení využívania uchovávaných údajov v rôznych situáciách v rámci trestného vyšetrovania. Okrem toho vnútroštátny súd konštatuje, že z dôvodovej správy k uvedenému zákonu vyplýva, že vnútroštátny zákonodarca zastával názor, že vzhľadom na sledovaný cieľ nebolo možné zaviesť povinnosť cieleného a diferencovaného uchovávania údajov a že sa rozhodol pre spojenie všeobecnej a nediferencovanej povinnosti s prísnymi zárukami, jednak na úrovni ochrany uchovávaných údajov, a jednak na úrovni prístupu k nim, s cieľom obmedziť čo možno najviac zásah do práva na rešpektovanie súkromného života.

77 Vnútroštátny súd dodáva, že článok 126 ods. 2 body 1 a 2 zákona z 13. júna 2005 v znení zákona z 29. mája 2016 stanovuje podmienky, za ktorých môžu súdne orgány a spravodajské a bezpečnostné služby získať prístup k uchovávaným údajom, takže preskúmanie zákonnosti tohto zákona z hľadiska požiadaviek práva Únie by sa malo pozastaviť až dovtedy, kým Súdny dvor nerozhodne v dvoch prebiehajúcich prejudiciálnych konaniach, ktoré sa týkajú tohto prístupu.

78 Napokon vnútroštátny súd uvádza, že cieľom zákona z 29. mája 2016 je umožniť trestné vyšetrovanie a uloženie účinnej sankcie za sexuálne zneužívanie maloletých osôb a umožniť účinnú identifikáciu páchateľa takéhoto skutku, a to aj v prípade, ak sa využívajú prostriedky elektronickej komunikácie. Počas konania na tomto súde sa v tejto súvislosti upriamila pozornosť na pozitívne záväzky vyplývajúce z článkov 3 a 8 EDĽP. Tieto povinnosti môžu rovnako vyplývať aj z príslušných ustanovení Charty, čo môže mať vplyv na výklad článku 15 ods. 1 smernice 2002/58.

79 Za týchto podmienok Cour constitutionnelle (Ústavný súd) rozhodol prerušiť konanie a položiť Súdnemu dvoru tieto prejudiciálne otázky:

„1. Má sa článok 15 ods. 1 smernice [2002/58] v spojení s právom na bezpečnosť zaručeným článkom 6 [Charty] a s právom na rešpektovanie osobných údajov, ktoré zaručujú články 7 a 8 a článok 52 ods. 1 Charty, vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, o akú ide v konaní vo veci samej, ktorá ukladá operátorom a poskytovateľom elektronických komunikačných služieb všeobecnú povinnosť uchovávať údaje o prenose dát a polohe v zmysle smernice [2002/58], ktoré tieto subjekty vytvárajú alebo spracúvajú v rámci poskytovania takýchto služieb, pričom cieľom tejto vnútroštátnej právnej úpravy nie je len vyšetrovanie, odhaľovanie a stíhanie závažných trestných činov, ale aj zaručenie národnej bezpečnosti, obrany územia a verejnej bezpečnosti, vyšetrovanie, odhaľovanie a stíhanie menej závažných trestných činov alebo zabránenie nepovolenému používaniu elektronických komunikačných systémov alebo dosiahnutie iného cieľa uvedeného v článku 23 ods. 1 [2016/679], a ktorá je navyše podmienená zárukami spresnenými v tejto právnej úprave, pokiaľ ide o uchovávanie údajov a prístup k nim?

2. Má sa článok 15 ods. 1 smernice [2002/58] v spojení s článkami 4, 7, 8, 11 a článkom 52 ods. 1 Charty vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, o akú ide v konaní vo veci samej, ktorá ukladá operátorom a poskytovateľom elektronických komunikačných služieb všeobecnú povinnosť uchovávať údaje o prenose dát a polohe v zmysle smernice [2002/58], ktoré tieto subjekty vytvárajú alebo spracúvajú v rámci poskytovania takýchto služieb, ak je cieľom tejto právnej úpravy najmä plniť pozitívne záväzky, ktoré orgánu vyplývajú z článkov 4 a [7] Charty a ktoré spočívajú vo vytvorení právneho rámca, ktorý umožní účinné vyšetrovanie a účinné potláčanie sexuálneho zneužívania maloletých osôb a tiež umožní skutočne identifikovať páchateľa trestného činu, a to aj vtedy, ak sa využívajú prostriedky elektronickej komunikácie?

3. Ak by Cour constitutionnelle [Ústavný súd] na základe odpovedí na prvú alebo druhú prejudiciálnu otázku dospel k záveru, že napadnutý zákon porušuje jednu alebo viaceré povinnosti vyplývajúce z ustanovení uvedených v týchto otázkach, mohol by dočasne zachovať účinky [zákona z 29. mája 2016], aby tak zabránil vzniku právnej neistoty a umožnil použitie v minulosti zhromaždených a uchovávaných údajov na účely stanovené zákonom?“

O konaní na Súdnom dvore

80 Rozhodnutím predsedu Súdneho dvora z 25. septembra 2018 boli veci C-511/18 a C-512/18 spojené na účely písomnej časti konania, ústnej časti konania a rozsudku. Vec C-520/18 bola spojená s týmito vecami rozhodnutím predsedu Súdneho dvora z 9. júla 2020 na účely vyhlásenia rozsudku.

O prejudiciálnych otázkach

O prvých otázkach vo veciach C-511/18 a C-512/18, ako aj o prvej a druhej otázke vo veci C-520/18

81 Prvými otázkami vo veciach C-511/18 a C-512/18, ako aj prvou a druhou otázkou vo veci C-520/18, ktoré treba preskúmať spoločne, sa vnútroštátne súdy v podstate pýtajú, či sa má článok 15 ods. 1 smernice 2002/58 vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá poskytovateľom elektronických komunikačných služieb ukladá na účely stanovené v tomto článku 15 ods. 1 povinnosť všeobecne a nediferencovane uchovávať údaje o prenose dát a polohe.

Úvodné poznámky

82 Zo spisov, ktoré má Súdny dvor k dispozícii, vyplýva, že právne predpisy dotknuté vo veciach samých sa vzťahujú na všetky prostriedky elektronickej komunikácie a zahŕňajú všetkých používateľov týchto prostriedkov bez toho, aby sa v tomto smere robili nejaké rozdiely alebo výnimky. Okrem toho údajmi, ktoré musia podľa týchto právnych predpisov uchovávať poskytovatelia elektronických komunikačných služieb, sú najmä údaje potrebné na zistenie zdroja komunikácie a jej adresáta, určenie dátumu, času, trvania a typu komunikácie, identifikáciu použitého komunikačného zariadenia a polohy koncových zariadení a komunikácie, pričom medzi tieto údaje patria najmä meno a adresa používateľa, telefónne čísla volajúceho a volaného, ako aj IP adresa pre internetové služby. Tieto údaje na druhej strane nezahŕňajú obsah dotknutej komunikácie.

83 Údaje, ktoré sa podľa vnútroštátnych právnych predpisov dotknutých vo veciach samých musia uchovávať po dobu jedného roka, tak umožňujú predovšetkým zistiť, s kým používateľ elektronického komunikačného prostriedku komunikoval a akým spôsobom táto komunikácia prebiehala, určiť dátum, čas a trvanie komunikácie a pripojení na internet, ako aj miesto, z ktorého prebiehali, a lokalizovať koncové zariadenia bez toho, aby bola komunikácia nevyhnutne prenášaná. Okrem toho tieto údaje umožňujú zistiť, ako často používateľ komunikoval s určitými osobami v danom období. Napokon, pokiaľ ide o vnútroštátnu právnu úpravu dotknutú vo veciach C-511/18 a C-512/18, zdá sa, že táto právna úprava v rozsahu, v akom sa vzťahuje aj na údaje týkajúce sa prenosu elektronických komunikácií v sieťach, umožňuje tiež identifikovať povahu informácií konzultovaných online.

84 Pokiaľ ide o sledované ciele, treba uviesť, že právne predpisy dotknuté vo veciach C-511/18 a C-512/18 sa týkajú okrem iných cieľov aj vyšetrovania, odhaľovania a stíhania trestných činov vo všeobecnosti, národnej nezávislosti, obrany a územnej celistvosti, hlavných záujmov zahraničnej politiky, plnenia európskych a medzinárodných záväzkov Francúzska, hlavných hospodárskych, priemyselných a vedeckých záujmov Francúzska, ako aj predchádzania terorizmu, útokom na republikánsku formu inštitúcií a kolektívnemu násiliu, ktoré môže vážne ohroziť verejný poriadok. Pokiaľ ide o právnu úpravu dotknutú vo veci C-520/18, jej cieľom je okrem iného vyšetrovanie, odhaľovanie a stíhanie trestných činov, ako aj ochrana národnej bezpečnosti, obrana územia a verejná bezpečnosť.

85 Vnútroštátne súdy sa pýtajú najmä na možný vplyv práva na bezpečnosť zakotveného v článku 6 Charty na výklad článku 15 ods. 1 smernice 2002/58. Rovnako sa pýtajú, či zásah do základných práv zakotvených v článkoch 7 a 8 Charty, ktorý predstavuje uchovávanie údajov stanovené právnymi predpismi dotknutými vo veciach samých, možno vzhľadom na existenciu pravidiel obmedzujúcich

prístup vnútroštátnych orgánov k uchovávaným údajom považovať za odôvodnený. Navyše podľa Conseil d'État (Štátna rada) musí byť táto otázka posúdená aj vzhľadom na článok 4 ods. 2 ZEÚ, keďže vzniká v kontexte, ktorý sa vyznačuje vážnymi a pretrvávajúcimi hrozbami pre národnú bezpečnosť. Cour constitutionnelle (Ústavný súd) zdôrazňuje, že vnútroštátna právna úprava dotknutá vo veci C-520/18 vykonáva tiež pozitívne záväzky vyplývajúce z článkov 4 a 7 Charty, ktoré spočívajú v stanovení právneho rámca umožňujúceho účinné potláčanie sexuálneho zneužívania maloletých.

86 Zatiaľ čo Conseil d'État (Štátna rada) a Cour constitutionnelle (Ústavný súd) vychádzajú z predpokladu, že vnútroštátne právne predpisy dotknuté vo veciach samých, ktoré upravujú uchovávanie údajov o prenose dát a polohe, ako aj prístup vnútroštátnych orgánov k týmto údajom na účely stanovené v článku 15 ods. 1 smernice 2002/58, ako napríklad ochrana národnej bezpečnosti, patria do pôsobnosti tejto smernice, niektorí účastníci konania vo veci samej a niektoré členské štáty, ktoré predložili Súdnemu dvoru písomné pripomienky, majú v tomto bode rozdielny názor, najmä pokiaľ ide o článok 1 ods. 3 uvedenej smernice. Je teda potrebné najskôr preskúmať, či uvedené právne predpisy patria do pôsobnosti tej istej smernice.

O pôsobnosti smernice 2002/58

87 La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International a Center for Democracy and Technology s odvolaním sa na judikatúru Súdneho dvora týkajúcu sa pôsobnosti smernice 2002/58 v podstate uvádzajú, že uchovávanie údajov a prístup k uchovávaným údajom patria do tejto pôsobnosti, či už sa tento prístup uskutočňuje v reálnom čase alebo až po určitom čase. Keďže cieľ ochrany národnej bezpečnosti je výslovne uvedený v článku 15 ods. 1 tejto smernice, sledovanie tohto cieľa teda nespôsobuje, že sa táto smernica neuplatní. Článok 4 ods. 2 ZEÚ, na ktorý poukazujú vnútroštátne súdy, nemá na toto posúdenie žiadny vplyv.

88 Pokiaľ ide o spravodajské opatrenia, ktoré príslušné francúzske orgány vykonávajú priamo bez toho, aby upravovali činnosti poskytovateľov elektronických komunikačných služieb tým, že by im ukladali osobitné povinnosti, Center for Democracy and Technology poznamenáva, že tieto opatrenia nevyhnutne patria do pôsobnosti smernice 2002/58 a Charty, pretože ide o výnimky zo zásady dôvernosti zaručenej článkom 5 tejto smernice. Uvedené opatrenia by teda mali byť v súlade s požiadavkami vyplývajúcimi z článku 15 ods. 1 tejto smernice.

89 Naproti tomu francúzska, česká a estónska vláda, Írsko, ako aj cyperská, maďarská, poľská a švédska vláda a vláda Spojeného kráľovstva v podstate tvrdia, že smernica 2002/58 sa neuplatňuje na také vnútroštátne právne predpisy, o aké ide vo veciach samých, keďže ich cieľom je ochrana národnej bezpečnosti. Činnosti spravodajských služieb v rozsahu, v akom sa týkajú udržiavania verejného poriadku, ako aj ochrany vnútornej bezpečnosti a územnej celistvosti, sú súčasťou základných funkcií členských štátov a v dôsledku toho patria do ich výlučnej právomoci, o čom svedčí najmä článok 4 ods. 2 tretia veta ZEÚ.

90 Tieto vlády a Írsko tiež odkazujú na článok 1 ods. 3 smernice 2002/58, ktorý vylučuje z pôsobnosti tejto smernice činnosti týkajúce sa verejnej bezpečnosti, obrany a bezpečnosti štátu, ako to už v minulosti stanovil článok 3 ods. 2 prvá zarážka smernice 95/46. V tejto súvislosti sa opierajú o výklad tohto posledného uvedeného ustanovenia uvedený v rozsudku z 30. mája 2006, Parlament/Rada a Komisia (C-317/04 a C-318/04, EU:C:2006:346).

91 V tomto smere treba uviesť, že podľa článku 1 ods. 1 smernice 2002/58 táto smernica stanovuje najmä harmonizáciu vnútroštátnych ustanovení požadovaných na zabezpečenie primeranej úrovne ochrany základných práv a slobôd, a najmä práva na súkromie a dôvernosť, z hľadiska spracúvania osobných údajov v elektronickom komunikačnom sektore.

92 Článok 1 ods. 3 tejto smernice vylučuje z jej pôsobnosti „činnosti štátu“ v oblastiach, ktoré sú v ňom vymenované, medzi ktorými sa nachádzajú činnosti štátu v oblasti trestného práva a činnosti týkajúce sa verejnej bezpečnosti, obrany, bezpečnosti štátu vrátane ekonomického blahobytu štátu, keď sa činnosti týkajú záležitostí bezpečnosti štátu. Činnosti demonštratívne uvedené v tomto ustanovení sú v každom prípade činnosti patriace štátu alebo štátnym orgánom a nepatria do oblasti činností jednotlivcov (rozsudok z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 32 a citovaná judikatúra).

93 Článok 3 smernice 2002/58 ďalej uvádza, že táto smernica sa vzťahuje na spracúvanie osobných údajov v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach v Únii vrátane verejných komunikačných sietí, ktoré podporujú zariadenia na zber údajov a identifikáciu (ďalej len „elektronické komunikačné služby“). Z toho vyplýva, že uvedenú smernicu treba považovať za upravujúcu činnosti poskytovateľov takých služieb (rozsudok z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 33 a citovaná judikatúra).

94 V tejto súvislosti článok 15 ods. 1 smernice 2002/58 umožňuje členským štátom prijať za podmienok, ktoré stanovuje, „legislatívne opatrenia na obmedzenie rozsahu práv a povinností uvedených v článku 5, článku 6, článku 8 ods. 1, 2, 3 a 4 a článku 9 tejto smernice“ (rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 71).

95 Článok 15 ods. 1 smernice 2002/58 pritom nevyhnutne predpokladá, že v ňom uvedené vnútroštátne opatrenia patria do jej pôsobnosti, pretože táto smernica výslovne dovoľuje členským štátom prijať také opatrenia len v prípade splnenia podmienok, ktoré sú v nej stanovené. Okrem toho na účely uvedené v tomto ustanovení takéto opatrenia upravujú činnosť poskytovateľov elektronických komunikačných služieb (rozsudok z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 34 a citovaná judikatúra).

96 Súdny dvor najmä vzhľadom na tieto úvahy rozhodol, že článok 15 ods. 1 smernice 2002/58 v spojení s jej článkom 3 sa má vykladať v tom zmysle, že do pôsobnosti tejto smernice patrí nielen legislatívne opatrenie, ktoré poskytovateľom elektronických komunikačných služieb ukladá povinnosť uchovávať údaje o prenose dát a polohe, ale takisto aj legislatívne opatrenie, ktoré im ukladá povinnosť poskytnúť príslušným vnútroštátnym orgánom prístup k týmto údajom. Takéto legislatívne opatrenia totiž nevyhnutne zahŕňajú spracúvanie týchto údajov uvedenými poskytovateľmi a nemožno ich v rozsahu, v akom upravujú činnosti týchto poskytovateľov, zamieňať s činnosťami štátu uvedenými v článku 1 ods. 3 uvedenej smernice (pozri v tomto zmysle rozsudok z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, body 35 a 37, ako aj citovanú judikatúru).

97 Okrem toho vzhľadom na úvahy uvedené v bode 95 tohto rozsudku a všeobecnú štruktúru smernice 2002/58 výklad tejto smernice, podľa ktorého sú legislatívne opatrenia uvedené v jej článku 15 ods. 1 vyňaté z pôsobnosti uvedenej smernice z dôvodu, že ciele, ktoré musia takéto opatrenia sledovať, sa výrazne prekrývajú s cieľmi sledovanými činnosťami uvedenými v článku 1 ods. 3 tej istej smernice, by zbavil článok 15 ods. 1 všetkého potrebného účinku (pozri v tomto zmysle rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 72 a 73).

98 Pojem „činnosti“ uvedený v článku 1 ods. 3 smernice 2002/58 teda nemožno, ako v podstate uviedol generálny advokát v bode 75 svojich návrhov v spojených veciach La Quadrature du Net a i. (C-511/18 a C-512/18, EU:C:2020:6), vykladať tak, že sa vzťahuje na legislatívne opatrenia uvedené v článku 15 ods. 1 tejto smernice.

99 Ustanovenia článku 4 ods. 2 ZEÚ, na ktoré odkazujú vlády uvedené v bode 89 tohto rozsudku, nemôžu tento záver vyvrátiť. Podľa ustálenej judikatúry Súdneho dvora, hoci členským štátom prináleží, aby vymedzili svoje hlavné bezpečnostné záujmy a prijali vhodné opatrenia na zaistenie svojej vnútornej a vonkajšej bezpečnosti, samotná skutočnosť, že určité vnútroštátne opatrenie je prijímané v záujme národnej bezpečnosti, nemôže viesť k tomu, že sa neuplatní právo Únie a členské štáty budú zbavené

povinnosti nevyhnutne dodržiavať toto právo [pozri v tomto zmysle rozsudky zo 4. júna 2013, ZZ, C-300/11, EU:C:2013:363, bod 38; z 20. marca 2018, Komisia/Rakúsko (Štátna tlačiareň), C-187/16, EU:C:2018:194, body 75 a 76, ako aj z 2. apríla 2020, Komisia/Poľsko, Maďarsko a Česká republika (Dočasný mechanizmus premiestnenia žiadateľov o medzinárodnú ochranu), C-715/17, C-718/17 a C-719/17, EU:C:2020:257, body 143 a 170].

100 Je pravda, že v rozsudku z 30. mája 2006, Parlament/Rada a Komisia (C-317/04 a C-318/04, EU:C:2006:346, body 56 až 59), Súdny dvor rozhodol, že prenos osobných údajov leteckými spoločnosťami orgánom verejnej moci tretieho štátu na účely predchádzania terorizmu a iným závažným trestným činom a boja proti nim nepatrí podľa článku 3 ods. 2 prvej zarážky smernice 95/46 do pôsobnosti tejto smernice, pretože tento prenos patrí do rámca vytvoreného orgánmi verejnej moci na účely verejnej bezpečnosti.

101 Vzhľadom na úvahy uvedené v bodoch 93, 95 a 96 tohto rozsudku však túto judikatúru nemožno uplatniť na výklad článku 1 ods. 3 smernice 2002/58. Ako v podstate uviedol generálny advokát v bodoch 70 až 72 svojich návrhov v spojených veciach La Quadrature du Net a i. (C-511/18 a C-512/18, EU:C:2020:6), článok 3 ods. 2 prvá zarážka smernice 95/46, ktorého sa týka uvedená judikatúra, totiž vo všeobecnosti vylučoval z pôsobnosti tejto poslednej uvedenej smernice „operácie spracovania týkajúce sa verejnej bezpečnosti, obrany, bezpečnosti štátu“, pričom sa nerozlišovali osoby, ktoré vykonávali dotknutú operáciu spracovania údajov. Naopak, v rámci výkladu článku 1 ods. 3 smernice 2002/58 sa takéto rozlišovanie javí ako nevyhnutné. Ako totiž vyplýva z bodov 94 až 97 tohto rozsudku, všetky operácie spracúvania osobných údajov vykonávané poskytovateľmi elektronických komunikačných služieb patria do pôsobnosti uvedenej smernice, vrátane operácií spracúvania vyplývajúcich z povinností uložených týmto poskytovateľom zo strany orgánov verejnej moci, hoci sa na tieto posledné uvedené operácie spracúvania prípadne mohla vzťahovať výnimka stanovená v článku 3 ods. 2 prvej zarážke smernice 95/46 vzhľadom na širšiu formuláciu tohto ustanovenia, ktoré sa vzťahovalo na všetky operácie spracúvania týkajúce sa verejnej bezpečnosti, obrany alebo bezpečnosti štátu, bez ohľadu na to, kto ich vykonával.

102 Okrem toho treba uviesť, že smernica 95/46 dotknutá vo veci, v ktorej bol vydaný rozsudok z 30. mája 2006, Parlament/Rada a Komisia (C-317/04 a C-318/04, EU:C:2006:346), bola na základe článku 94 ods. 1 nariadenia 2016/679 zrušená a nahradená týmto nariadením, a to s účinnosťou od 25. mája 2018. Hoci uvedené nariadenie vo svojom článku 2 ods. 2 písm. d) spresňuje, že sa nevzťahuje na operácie spracúvania vykonávané „príslušnými orgánmi“ najmä na účely predchádzania trestným činom a ich odhaľovania vrátane ochrany pred ohrozením verejnej bezpečnosti a jeho predchádzania, z článku 23 ods. 1 písm. d) a h) toho istého nariadenia vyplýva, že spracúvanie osobných údajov vykonávané jednotlivcami na rovnaké účely patrí do pôsobnosti tohto nariadenia. Z toho vyplýva, že vyššie uvedený výklad článku 1 ods. 3, článku 3 a článku 15 ods. 1 smernice 2002/58 je v súlade s vymedzením pôsobnosti nariadenia 2016/679, ktoré táto smernica dopĺňa a spresňuje.

103 Naproti tomu, ak členské štáty priamo vykonajú opatrenia, ktoré predstavujú výnimku zo zásady dôvernosti elektronických komunikácií, bez toho, aby ukladali povinnosť spracovávania poskytovateľom takýchto komunikačných služieb, na ochranu údajov dotknutých osôb sa nevzťahuje smernica 2002/58, ale len vnútroštátne právo, s výhradou uplatnenia smernice Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (Ú. v. EÚ L 119, 2016, s. 89), takže dotknuté opatrenia musia byť v súlade najmä s vnútroštátnym ústavným právom a požiadavkami EDĽP.

104 Z predchádzajúcich úvah vyplýva, že také vnútroštátne právne predpisy, o aké ide vo veciach samých, ktoré poskytovateľom elektronických komunikačných služieb ukladajú povinnosť uchovávať údaje o prenose dát a polohe na účely ochrany národnej bezpečnosti a boja proti trestnej činnosti, patria do pôsobnosti smernice 2002/58.

O výklade článku 15 ods. 1 smernice 2002/58

105 Na úvod je potrebné pripomenúť, že z ustálenej judikatúry vyplýva, že na účely výkladu ustanovenia práva Únie treba zohľadniť nielen jeho znenie, ale aj jeho kontext a ciele sledované právnou úpravou, ktorej je súčasťou, a najmä vývoj tejto právnej úpravy (pozri v tomto zmysle rozsudok zo 17. apríla 2018, Egenberger, C-414/16, EU:C:2018:257, bod 44).

106 Účelom smernice 2002/58, ako vyplýva najmä z jej odôvodnení 6 a 7, je chrániť používateľov elektronických komunikačných služieb pred rizikami pre osobné údaje a súkromie, ktoré vyplývajú z nových technológií a predovšetkým zo zvyšovania kapacity automatického uchovávania a spracovávania údajov. Uvedená smernica, ako stanovuje jej odôvodnenie 2, má za cieľ najmä plné zabezpečenie práv stanovených v článkoch 7 a 8 Charty. V tejto súvislosti z dôvodovej správy k návrhu smernice Európskeho parlamentu a Rady týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií [KOM(2000) 385 v konečnom znení], na základe ktorej bola prijatá smernica 2002/58, vyplýva, že normotvorca Únie chcel „zabezpečiť, aby aj naďalej bola zaručená vysoká úroveň ochrany osobných údajov a súkromia pre všetky elektronické komunikačné služby, bez ohľadu na použité technológie“.

107 Na tento účel článok 5 ods. 1 smernice 2002/58 zakotvuje zásadu dôvernosti elektronických komunikácií a príslušných údajov o prenose dát a okrem iného stanovuje, že sa akýmkoľvek iným osobám než používateľom v zásade zakazuje bez súhlasu týchto používateľov uchovávať tieto komunikácie a tieto údaje.

108 Pokiaľ ide konkrétne o spracúvanie a uchovávanie údajov o prenose dát poskytovateľmi elektronických komunikačných služieb, z článku 6 a odôvodnení 22 a 26 smernice 2002/58 vyplýva, že takéto spracúvanie je povolené len v rozsahu a na obdobie potrebné na účely marketingu služieb, ich fakturácie alebo poskytovania služieb s pridanou hodnotou. Po uplynutí tejto doby sa údaje, ktoré boli spracúvané a uchovávané, musia vymazať alebo anonymizovať. Pokiaľ ide o údaje o polohe iné ako údaje o prenose dát, článok 9 ods. 1 uvedenej smernice stanovuje, že takéto údaje sa môžu spracovávať len za určitých podmienok a po ich anonymizácii alebo po získaní súhlasu používateľov alebo účastníkov (rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 86 a citovaná judikatúra).

109 Prijatím tejto smernice tak normotvorca Únie konkretizoval práva zakotvené v článkoch 7 a 8 Charty, takže používatelia elektronických komunikačných prostriedkov majú v zásade právo očakávať, že ich komunikácia a s ňou súvisiace údaje zostanú v prípade chýbajúceho súhlasu z ich strany anonymizované a nebudú môcť byť predmetom zaznamenania.

110 Článok 15 ods. 1 smernice 2002/58 však umožňuje členským štátom zaviesť výnimky z povinnosti stanovenej v článku 5 ods. 1 uvedenej smernice, podľa ktorej sú tieto štáty povinné zabezpečiť dôvernosť osobných údajov, ako aj z príslušných povinností uvedených najmä v článkoch 6 a 9 uvedenej smernice, ak také obmedzenie predstavuje nevyhnutné, vhodné a primerané opatrenie v demokratickej spoločnosti na zabezpečenie národnej bezpečnosti, obrany, verejnej bezpečnosti a na zabránenie, vyšetrovanie, odhaľovanie a stíhanie trestných činov alebo neoprávnené používanie elektronického komunikačného systému. Na tento účel môžu členské štáty okrem iného prijať legislatívne opatrenia, ktoré stanovujú uchovávanie údajov na obmedzené obdobie, ak je to odôvodnené niektorým z týchto dôvodov.

111 Za týchto okolností možnosť odchýliť sa od práv a povinností stanovených v článkoch 5, 6 a 9 smernice 2002/58 nemôže odôvodniť, že výnimka zo zásadnej povinnosti zabezpečiť dôvernosť elektronických komunikácií a s ňou súvisiacich údajov, a najmä výnimka zo zákazu uchovávať tieto údaje výslovne uvedená v článku 5 tejto smernice, sa stane pravidlom (pozri v tomto zmysle rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 89 a 104).

112 Pokiaľ ide o ciele, ktoré môžu odôvodniť obmedzenie práv a povinností stanovených najmä v článkoch 5, 6 a 9 smernice 2002/58, Súdny dvor už rozhodol, že výpočet cieľov uvedených v článku 15 ods. 1 prvej vete tejto smernice je taxatívny, v dôsledku čoho musí legislatívne opatrenie prijaté na základe tohto ustanovenia skutočne a striktne zodpovedať jednému z týchto cieľov (pozri v tomto zmysle rozsudok z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 52 a citovanú judikatúru).

113 Z článku 15 ods. 1 tretej vety smernice 2002/58 okrem toho vyplýva, že členské štáty sú oprávnené prijať legislatívne opatrenia na obmedzenie rozsahu práv a povinností uvedených v článkoch 5, 6 a 9 tejto smernice len pri dodržaní všeobecných zásad práva Únie, vrátane zásady proporcionality, a základných práv zaručených Chartou. V tejto súvislosti Súdny dvor už rozhodol, že povinnosť uložená poskytovateľom elektronických komunikačných služieb zo strany členského štátu na základe vnútroštátnej právnej úpravy, podľa ktorej sú povinní uchovávať údaje o prenose dát na účely ich prípadného sprístupnenia príslušným vnútroštátnym orgánom, vyvoláva otázky týkajúce sa súladu nielen s článkami 7 a 8 Charty, ktoré sa týkajú ochrany súkromia a ochrany osobných údajov, ale aj s článkom 11 Charty týkajúcim sa slobody prejavu (pozri v tomto zmysle rozsudky z 8. apríla 2014, Digital Rights, C-293/12 a C-594/12, EU:C:2014:238, body 25 a 70, ako aj z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 91 a 92, ako aj citovanú judikatúru).

114 Pri výklade článku 15 ods. 1 smernice 2002/58 preto treba prihliadať nielen na význam práva na rešpektovanie súkromného života zaručeného v článku 7 Charty a práva na ochranu osobných údajov zaručeného v jej článku 8, ako vyplýva z judikatúry Súdneho dvora, ale aj na dôležitosť práva na slobodu prejavu, pričom toto základné právo zaručené v článku 11 Charty predstavuje jednu zo základných podstát demokratickej a pluralitnej spoločnosti a je súčasťou hodnôt, na ktorých je Únia v súlade s článkom 2 ZEÚ založená (pozri v tomto zmysle rozsudky zo 6. marca 2001, Connolly/Komisia, C-274/99 P, EU:C:2001:127, bod 39, ako aj z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 93 a citovanú judikatúru).

115 V tejto súvislosti treba spresniť, že samotné uchovávanie údajov o prenose dát a polohe predstavuje na jednej strane výnimku zo zákazu stanoveného v článku 5 ods. 1 smernice 2002/58, ktorým sa akejkoľvek inej osobe, než sú používatelia, zakazuje ukladať tieto údaje, a na druhej strane zásah do základných práv na rešpektovanie súkromného života a ochranu osobných údajov, ktoré sú zakotvené v článkoch 7 a 8 Charty, bez ohľadu na to, či predmetné informácie týkajúce sa súkromného života majú alebo nemajú citlivú povahu alebo či pre dotknuté osoby z dôvodu tohto zásahu vyplynuli alebo nevyplynuli prípadné nepriaznivé následky [pozri v tomto zmysle stanovisko 1/15 (Dohoda o PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, body 124 a 126, ako aj citovanú judikatúru); pozri analogicky, pokiaľ ide o článok 8 EDĽP, rozsudok ESĽP, 30. január 2020, Breyer v. Nemecko, CE:ECHR:2020:0130JUD005000112, § 81].

116 Je tiež irelevantné, či sa uchovávané údaje následne použijú alebo nie (pozri analogicky, pokiaľ ide o článok 8 EDĽP, rozsudky ESĽP, 16. februára 2000, Amann v. Švajčiarsko, CE:ECHR:2000:0216JUD002779895, § 69, a 13. februára 2020, Trjakovski a Chipovski v. Severné Macedónsko, CE:ECHR:2020:0213JUD005320513, § 51), keďže prístup k takýmto údajom predstavuje bez ohľadu na účel ich neskoršieho využitia samostatný zásah do základných práv uvedených v predchádzajúcom bode [pozri v tomto zmysle stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, body 124 a 126].

117 Tento záver je ešte opodstatnenejší vzhľadom na to, že údaje o prenose dát a polohe môžu odhaliť informácie o značnom počte aspektov súkromného života dotknutých osôb vrátane citlivých informácií, akými sú sexuálna orientácia, politické názory, náboženské, filozofické, spoločenské alebo iné presvedčenie a zdravotný stav, pričom takýmto údajom je navyše poskytnutá osobitná ochrana v práve Únie. Zo všetkých týchto údajov možno vyvodiť presné závery týkajúce sa súkromného života osôb, ktorých údaje boli uchovávané, ako ich každodenné zvyklosti, miesta ich trvalého alebo prechodného pobytu, denné alebo iné presuny, vykonávané činnosti, spoločenské vzťahy týchto osôb

a spoločenské kruhy, v ktorých sa pohybujú. Konkrétne takéto údaje poskytujú prostriedky na stanovenie profilu dotknutých osôb, čo je rovnako citlivá informácia, pokiaľ ide o právo na rešpektovanie súkromného života, ako samotný obsah komunikácií (pozri v tomto zmysle rozsudky z 8. apríla 2014, Digital Rights, C-293/12 a C-594/12, EU:C:2014:238, bod 27, a z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 99).

118 Preto na jednej strane uchovávanie údajov o prenose dát a polohe na policajné účely môže samo osebe zasahovať do práva na rešpektovanie komunikácie zakotveného v článku 7 Charty a odrádzať používateľov elektronických komunikačných prostriedkov od uplatňovania ich slobody prejavu zaručenej v článku 11 Charty (pozri v tomto zmysle rozsudky z 8. apríla 2014, Digital Rights, C-293/12 a C-594/12, EU:C:2014:238, bod 28, ako aj z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 101). Tento odrádzajúci účinok môže mať vplyv najmä na osoby, ktorých komunikácia podľa vnútroštátnych pravidiel podlieha služobnému tajomstvu, a oznamovateľov, ktorých činnosti sú chránené smernicou Európskeho parlamentu a Rady (EÚ) 2019/1937 z 23. októbra 2019 o ochrane osôb, ktoré nahlasujú porušenia práva Únie (Ú. v. EÚ L 305, 2019, s. 17). Okrem toho je tento účinok ešte závažnejší vzhľadom na veľké množstvo a rôznorodosť uchovávaných údajov.

119 Na druhej strane vzhľadom na značné množstvo údajov o prenose dát a polohe, ktoré možno nepretržite uchovávať na základe všeobecného opatrenia na ich uchovávanie, a citlivú povahu informácií, ktoré sa dajú z týchto údajov získať, už samotné uchovávanie uvedených údajov poskytovateľmi elektronických komunikačných služieb v sebe zahŕňa riziká zneužitia a neoprávneného prístupu.

120 Článok 15 ods. 1 smernice 2002/58 však tým, že umožňuje členským štátom zaviesť výnimky uvedené v bode 110 tohto rozsudku, odráža skutočnosť, že práva zakotvené v článkoch 7, 8 a 11 Charty nie sú absolútnymi výsadami, ale musia sa vnímať vo vzťahu k ich úlohe v spoločnosti (pozri v tomto zmysle rozsudok zo 16. júla 2020, Facebook Ireland a Schrems, C-311/18, EU:C:2020:559, bod 172, ako aj citovanú judikatúru).

121 Charta, ako vyplýva z jej článku 52 ods. 1, totiž pripúšťa obmedzenia výkonu týchto práv, pokiaľ sú tieto obmedzenia stanovené zákonom, rešpektujú podstatu uvedených práv a za predpokladu dodržiavania zásady proporcionality sú nevyhnutné a skutočne zodpovedajú cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo potrebe chrániť práva a slobody iných.

122 Na účely výkladu článku 15 ods. 1 smernice 2002/58 so zreteľom na Chartu je teda potrebné zohľadniť tiež význam práv zakotvených v článkoch 3, 4, 6 a 7 Charty a dôležitosť cieľov ochrany národnej bezpečnosti a boja proti závažnej trestnej činnosti, ktoré prispievajú k ochrane práv a slobôd iných.

123 V tejto súvislosti článok 6 Charty, na ktorý sa odvolávajú Conseil d'État (Štátna rada) a Cour constitutionnelle (Ústavný súd), zakotvuje právo každej osoby nielen na slobodu, ale aj na bezpečnosť a zaručuje práva zodpovedajúce tým, ktoré sú zaručené v článku 5 EDĽP (pozri v tomto zmysle rozsudky z 15. februára 2016, N., C-601/15 PPU, EU:C:2016:84, bod 47; z 28. júla 2016, JZ, C-294/16 PPU, EU:C:2016:610, bod 48, ako aj z 19. septembra 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, bod 42 a citovanú judikatúru).

124 Okrem toho je potrebné pripomenúť, že cieľom článku 52 ods. 3 Charty je zabezpečiť potrebnú súdržnosť medzi právami obsiahnutými v Charte a zodpovedajúcimi právami zaručenými EDĽP bez toho, aby tým bola narušená autonómia práva Únie a Súdneho dvora Európskej únie. Pri výklade Charty teda treba zohľadniť príslušné práva podľa EDĽP ako úroveň minimálnej ochrany [pozri v tomto zmysle rozsudky z 12. februára 2019, TC, C-492/18 PPU, EU:C:2019:108, bod 57, a z 21. mája 2019, Komisia/Maďarsko (Užívanie poľnohospodárskych pozemkov), C-235/17, EU:C:2019:432, bod 72 a citovanú judikatúru].

125 Pokiaľ ide o článok 5 EDĽP, ktorý zakotvuje „právo na slobodu“ a „právo na bezpečnosť“, jeho cieľom je podľa judikatúry Európskeho súdu pre ľudské práva chrániť jednotlivca pred svojvoľným alebo neodôvodneným odňatím slobody (pozri v tomto zmysle rozsudky ESĽP, 18. marca 2008, Ladent v. Poľsko, CE:ECHR:2008:0318JUD001103603, § 45 a 46; 29. marca 2010, Medvedev a i. v. Francúzsko, CE:ECHR:2010:0329JUD000339403, § 76 a 77, a 13. decembra 2012, El-Masri v. „Bývalá juhoslovanská republika Macedónsko“, CE:ECHR:2012:1213JUD003963009, § 239). Keďže sa však toto ustanovenie týka pozbavenia osobnej slobody zo strany orgánu verejnej moci, článok 6 Charty nemožno vykladať tak, že orgánom verejnej moci ukladá povinnosť prijať konkrétne opatrenia na účely stíhania niektorých trestných činov.

126 Na druhej strane, pokiaľ ide konkrétne o účinný boj proti trestným činom, ktorých obeťami sú najmä maloleté osoby a iné zraniteľné osoby, uvádzaný Cour constitutionnelle (Ústavný súd), treba zdôrazniť, že z článku 7 Charty môžu pre orgány verejnej moci vyplývať aj pozitívne povinnosti prijať právne opatrenia na ochranu súkromného a rodinného života [pozri v tomto zmysle rozsudok z 18. júna 2020, Komisia/Maďarsko (Transparentnosť združení), C-78/18, EU:C:2020:476, bod 123 a citovanú judikatúru Európskeho súdu pre ľudské práva]. Takéto povinnosti môžu tiež vyplývať z uvedeného článku 7 v prípade ochrany obydlia a komunikácie, ako aj z článkov 3 a 4, pokiaľ ide o ochranu fyzickej a duševnej integrity osôb a zákaz mučenia a neľudského alebo ponižujúceho zaobchádzania.

127 Vzhľadom na tieto rôzne pozitívne povinnosti je teda potrebné pristúpiť k nevyhnutnému zosúladeniu rôznych dotknutých záujmov a práv.

128 Európsky súd pre ľudské práva totiž rozhodol, že pozitívne povinnosti vyplývajúce z článkov 3 a 8 EDĽP, ktorých zodpovedajúce záruky sú uvedené v článkoch 4 a 7 Charty, si vyžadujú najmä prijatie hmotnoprávnych a procesných ustanovení, ako aj praktických opatrení umožňujúcich účinný boj proti trestným činom páchaným na osobách prostredníctvom efektívneho vyšetrovania a trestného stíhania, pričom táto povinnosť je ešte dôležitejšia, ak je ohrozené fyzické a morálne blaho dieťaťa. Opatrenia, ktoré majú prijať príslušné orgány, však musia v plnej miere rešpektovať zákonné postupy a ďalšie záruky, ktoré môžu obmedziť rozsah právomocí v oblasti vyšetrovania trestných činov, ako aj iné slobody a práva. Podľa tohto súdu je predovšetkým potrebné vytvoriť právny rámec umožňujúci zosúladiť rôzne záujmy a práva, ktoré sa majú chrániť (rozsudky ESĽP, 28. októbra 1998, Osman v. Spojené kráľovstvo, CE:ECHR:1998:1028JUD002345294, § 115 a 116; 4. marca 2004, M.C. v. Bulharsko, CE:ECHR:2003:1204JUD003927298, § 151; 24. júna 2004, Von Hannover v. Nemecko, CE:ECHR:2004:0624JUD005932000, § 57 a 58, a 2. decembra 2008, K. Ú. v. Fínsko, CE:ECHR:2008:1202JUD 000287202, § 46, § 48 a § 49).

129 Pokiaľ ide o dodržiavanie zásady proporcionality, článok 15 ods. 1 prvá veta smernice 2002/58 stanovuje, že členské štáty môžu prijať opatrenie, ktoré predstavuje výnimku zo zásady dôvernosti komunikácie a príslušných údajov o prenose, ak ide o „nevyhnutné, vhodné a primerané opatrenie v demokratickej spoločnosti“, so zreteľom na ciele stanovené v tomto ustanovení. Odôvodnenie 11 tejto smernice spresňuje, že opatrenie tohto druhu musí byť „prísne“ proporcionálne vo vzťahu k zamýšľanému účelu.

130 V tejto súvislosti treba pripomenúť, že ochrana základného práva na rešpektovanie súkromného života v súlade s ustálenou judikatúrou Súdneho dvora vyžaduje, aby výnimky a obmedzenia v súvislosti s ochranou osobných údajov nepôsobili nad rámec toho, čo je prísne nevyhnutné. Okrem toho nemožno sledovať cieľ všeobecného záujmu bez zohľadnenia skutočnosti, že musí byť zosúladený so základnými právami dotknutými opatrením, a to náležitým vyvážením cieľa všeobecného záujmu a dotknutých práv [pozri v tomto zmysle rozsudky zo 16. decembra 2008, Satakunnan Markkinapörssi a Satamedia, C-73/07, EU:C:2008:727, bod 56; z 9. novembra 2010, Volker und Markus Schecke a Eifert, C-92/09 a C-93/09, EU:C:2010:662, body 76, 77 a 86, ako aj z 8. apríla 2014, Digital Rights, C-293/12 a C-594/12, EU:C:2014:238, bod 52; stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, bod 140].

131 Z judikatúry Súdneho dvora konkrétne vyplýva, že možnosť členských štátov odôvodniť obmedzenie práv a povinností stanovených najmä v článkoch 5, 6 a 9 smernice 2002/58 treba posudzovať prostredníctvom merania závažnosti zásahu, ktorý spôsobí takéto obmedzenie, a overenia, či je dôležitosť cieľa všeobecného záujmu sledovaného týmto obmedzením priamo úmerná takejto závažnosti (pozri v tomto zmysle rozsudok z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 55 a citovanú judikatúru).

132 Na účely splnenia požiadavky proporcionality musí právna úprava stanoviť jasné a presné pravidlá, ktoré budú upravovať rozsah a uplatnenie predmetného opatrenia a ukladať minimálne požiadavky tak, aby osoby, ktorých osobné údaje sú dotknuté, mali dostatočné záruky umožňujúce účinne chrániť tieto údaje pred rizikami zneužitia. Táto právna úprava musí byť podľa vnútroštátneho práva právne záväzná a musí najmä vymedziť okolnosti a podmienky, za akých možno prijať opatrenie upravujúce spracúvanie takýchto údajov, čím zaručí, aby zásah nešiel nad rámec toho, čo je striktne nevyhnutné. Nevyhnutnosť disponovať takými zárukami je o to dôležitejšia v prípade, keď sú osobné údaje spracúvané automaticky, najmä ak existuje značné riziko neoprávneného prístupu k týmto údajom. Tieto úvahy platia najmä vtedy, keď ide o ochranu osobitnej kategórie osobných údajov, ktorú tvoria citlivé údaje [pozri v tomto zmysle rozsudky z 8. apríla 2014, Digital Rights, C-293/12 a C-594/12, EU:C:2014:238, body 54 a 55, ako aj z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 117; stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, bod 141].

133 Právna úprava stanovujúca uchovávanie osobných údajov musí vždy spĺňať objektívne kritériá, ktoré vymedzujú vzťah medzi údajmi, ktoré majú byť uchovávané, a sledovaným cieľom [pozri v tomto zmysle stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, bod 191 ako aj citovanú judikatúru, ako aj rozsudok z 3. októbra 2019, A a i., C-70/18, EU:C:2019:823, bod 63].

– O legislatívnych opatreniach, ktoré na účely ochrany národnej bezpečnosti stanovujú preventívne uchovávanie údajov o prenose dát a polohe

134 Treba poznamenať, že Súdny dvor vo svojich rozsudkoch, ktorými sa vykladá smernica 2002/58, ešte osobitne neskúmal cieľ ochrany národnej bezpečnosti uvádzaný vnútroštátnymi súdmi a vládami, ktoré predložili pripomienky.

135 V tejto súvislosti treba na úvod uviesť, že článok 4 ods. 2 ZEÚ stanovuje, že národná bezpečnosť ostáva vo výlučnej zodpovednosti každého členského štátu. Táto zodpovednosť zodpovedá prvoradému záujmu chrániť základné funkcie štátu a základné záujmy spoločnosti a zahŕňa prevenciu a potláčanie aktivít, ktoré môžu vážne destabilizovať základné politické, ústavné, hospodárske alebo sociálne štruktúry krajiny a najmä priamo ohroziť spoločnosť, obyvateľstvo alebo samotný štát, akými sú napríklad teroristické aktivity.

136 Význam cieľa ochrany národnej bezpečnosti v spojení s článkom 4 ods. 2 ZEÚ tak presahuje význam ostatných cieľov uvedených v článku 15 ods. 1 smernice 2002/58, a to najmä cieľov boja proti trestnej činnosti vo všeobecnosti, hoci aj závažnej, a ochrany verejnej bezpečnosti. Také hrozby, ako sú hrozby uvedené v predchádzajúcom bode, sa totiž svojou povahou a osobitnou závažnosťou odlišujú od všeobecného či dokonca závažného rizika vzniku napätia alebo narušenia v oblasti verejnej bezpečnosti. Cieľ ochrany národnej bezpečnosti teda môže, pokiaľ sú splnené ostatné požiadavky stanovené v článku 52 ods. 1 Charty, odôvodniť opatrenia, ktoré zasahujú do základných práv závažnejšie než tie, ktoré by mohli byť odôvodnené týmito ostatnými cieľmi.

137 V situáciách ako sú tie, ktoré sú opísané v bodoch 135 a 136 tohto rozsudku, teda článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty v zásade nebráni legislatívnemu opatreniu, ktoré príslušným orgánom dovoľuje nariadiť poskytovateľom elektronických

komunikačných služieb, aby počas obmedzeného obdobia uchovávali údaje o prenose dát a polohe všetkých používateľov elektronických komunikačných prostriedkov, ak existujú dostatočne konkrétne okolnosti na to, aby bolo možné domnievať sa, že dotknutý členský štát čelí takej vážnej hrozbe pre národnú bezpečnosť, aká sa uvádza v bodoch 135 a 136 tohto rozsudku, pričom sa javí ako skutočná a aktuálna alebo predvídateľná. Aj keď sa takéto opatrenie uplatňuje nediferencovane na všetkých používateľov elektronických komunikačných prostriedkov bez toho, aby bola na prvý pohľad zrejmá spojitosť v zmysle judikatúry uvedenej v bode 133 tohto rozsudku medzi nimi a hrozbou pre národnú bezpečnosť tohto členského štátu, treba vychádzať z predpokladu, že takúto spojitosť môže vytvárať už samotná existencia takejto hrozby.

138 Príkaz na preventívne uchovávanie údajov všetkých používateľov elektronických komunikačných prostriedkov však musí byť časovo obmedzený na to, čo je striktne nevyhnutné. Hoci nemožno vylúčiť, že príkaz na uchovávanie údajov uložený poskytovateľom elektronických komunikačných služieb môže byť z dôvodu pretrvávania takejto hrozby obnovený, trvanie každého príkazu nemôže prekročiť predvídateľné časové obdobie. Takéto uchovávanie údajov musí navyše podliehať obmedzeniam a musí byť sprevádzané prísnymi zárukami, ktoré umožňujú účinne chrániť osobné údaje dotknutých osôb pred rizikami zneužitia. Toto uchovávanie teda nemôže mať systematickú povahu.

139 Vzhľadom na závažnosť zásahu do základných práv zakotvených v článkoch 7 a 8 Charty, ktorý je výsledkom takéhoto opatrenia na všeobecné a nediferencované uchovávanie údajov, je potrebné zabezpečiť, aby sa použitie tohto opatrenia v skutočnosti obmedzovalo na situácie, v ktorých existuje vážna hrozba pre národnú bezpečnosť, aká sa uvádza v bodoch 135 a 136 tohto rozsudku. Na tento účel je nevyhnutné, aby rozhodnutie, ktorým sa nariaďuje poskytovateľom elektronických komunikačných služieb vykonávať takéto uchovávanie údajov, mohlo byť účinne preskúmané zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, pričom cieľom tohto preskúmania je overiť existenciu jednej z týchto situácií, ako aj dodržanie podmienok a záruk, ktoré musia byť stanovené.

– O legislatívnych opatreniach, ktoré na účely boja proti trestnej činnosti a ochrany verejnej bezpečnosti stanovujú preventívne uchovávanie údajov o prenose dát a polohe

140 Pokiaľ ide o cieľ predchádzania, vyšetrovania, odhaľovania a stíhania trestných činov, v súlade so zásadou proporcionality môže len boj proti závažnej trestnej činnosti a predchádzanie vážnym hrozbám pre verejnú bezpečnosť odôvodniť také závažné zásahy do základných práv zakotvených v článkoch 7 a 8 Charty, akými sú zásahy, ktoré zahŕňajú uchovávanie údajov o prenose dát a polohe. Preto iba zásahy do uvedených základných práv, ktoré nemajú závažnú povahu, môžu byť odôvodnené cieľom predchádzania, vyšetrovania, odhaľovania a stíhania trestných činov vo všeobecnosti [pozri v tomto zmysle rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 102, ako aj z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, body 56 a 57; stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, bod 149].

141 Vnútroštátna právna úprava, ktorá stanovuje všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe na účely boja proti závažnej trestnej činnosti, ide nad rámec toho, čo je prísne nevyhnutné, a nemožno ju teda považovať za odôvodnenú v demokratickej spoločnosti, ako to vyžaduje článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty (pozri v tomto zmysle rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 107).

142 Vzhľadom na citlivú povahu informácií, ktoré môžu poskytovať údaje o prenose dát a polohe, je totiž dôvernosť týchto údajov nevyhnutná pre právo na rešpektovanie súkromného života. S prihliadnutím jednak na odrádzajúci účinok na výkon základných práv zakotvených v článkoch 7 a 11 Charty uvedený v bode 118 tohto rozsudku, ktorý môže vyplynúť z uchovávania týchto údajov, a jednak na závažnosť zásahu, ktorý spôsobí takéto uchovávanie, je teda v demokratickej spoločnosti potrebné, aby

uchovávanie bolo výnimkou a nie pravidlom, ako to stanovuje systém zavedený smernicou 2002/58, a aby tieto údaje nemohli byť uchovávané systematicky a nepretržite. Tento záver platí, aj pokiaľ ide o ciele boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť, ako aj dôležitosť, ktorú im treba priznať.

143 Okrem toho Súdny dvor zdôraznil, že právna úprava, ktorá stanovuje všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe zahŕňa elektronickú komunikáciu takmer celého obyvateľstva bez akéhokoľvek rozlíšenia, obmedzenia alebo výnimky na základe sledovaného cieľa. Takáto právna úprava sa v rozpore s požiadavkou pripomenutou v bode 133 tohto rozsudku globálne týka všetkých osôb používajúcich elektronické komunikačné služby bez toho, aby sa tieto osoby aspoň nepriamo nachádzali v situácii, ktorá by mohla viesť k trestnému stíhaniu. Uplatňuje sa teda aj na osoby, pri ktorých nie je dôvod domnievať sa, že by ich konanie mohlo mať aspoň nepriamu alebo vzdialenú súvislosť s týmto cieľom boja proti závažnej trestnej činnosti, a najmä bez toho, aby bola stanovená súvislosť medzi údajmi, ktorých uchovávanie sa umožňuje, a hrozbou pre verejnú bezpečnosť (pozri v tomto zmysle rozsudky z 8. apríla 2014, Digital Rights, C-293/12 a C-594/12, EU:C:2014:238, body 57 a 58, ako aj z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 105).

144 Konkrétne, ako už Súdny dvor rozhodol, takáto právna úprava nie je obmedzená na uchovávanie, ktoré by sa vzťahovalo na údaje z určitého časového obdobia a/alebo z určitej zemepisnej oblasti a/alebo na okruh osôb, ktorý by akýmkoľvek spôsobom bolo možné spájať so závažnými trestnými činmi, ani na osoby, ktorých uchovávané údaje by z iných dôvodov mohli prispieť k boju proti závažnej trestnej činnosti (pozri v tomto zmysle rozsudky z 8. apríla 2014, Digital Rights, C-293/12 a C-594/12, EU:C:2014:238, bod 59, a z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 106).

145 Dokonca ani pozitívne povinnosti členských štátov, ktoré môžu v závislosti od konkrétneho prípadu vyplývať z článkov 3, 4 a 7 Charty a ktoré sa týkajú, ako bolo uvedené v bodoch 126 a 128 tohto rozsudku, zavedenia pravidiel umožňujúcich účinný boj proti trestným činom, nemôžu viesť k odôvodneniu tak závažných zásahov, ako sú tie, ktoré spôsobuje právna úprava umožňujúca uchovávanie údajov o prenose dát a polohe, do základných práv takmer celého obyvateľstva zakotvených v článkoch 7 a 8 Charty bez toho, aby existovala aspoň nepriama súvislosť medzi údajmi o dotknutých osobách a sledovaným cieľom.

146 Na druhej strane, v súlade s tým, čo bolo uvedené v bodoch 142 až 144 tohto rozsudku, a vzhľadom na nevyhnutné zosúladenie dotknutých práv a záujmov, môžu ciele boja proti závažnej trestnej činnosti, predchádzania vážnym narušeniam verejnej bezpečnosti a *a fortiori* ochrany národnej bezpečnosti odôvodniť vzhľadom na ich dôležitosť a pozitívne povinnosti pripomenuté v predchádzajúcom bode, na ktoré odkazuje najmä Cour constitutionnelle (Ústavný súd), obzvlášť závažný zásah, ktorý predstavuje cielené uchovávanie údajov o prenose dát a polohe.

147 Ako už Súdny dvor rozhodol, článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty nebráni tomu, aby členský štát prijal právnu úpravu, ktorá preventívne umožňuje, aby sa cielene uchovávali údaje o prenose dát a polohe na účely boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť, ako aj na účely ochrany národnej bezpečnosti, a to pod podmienkou, že uchovávanie údajov bude, pokiaľ ide o kategórie uchovávaných údajov, príslušné komunikačné prostriedky, dotknuté osoby, ako aj dĺžku doby uchovávania, obmedzené na to, čo je prísne nevyhnutné (pozri v tomto zmysle rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 108).

148 Pokiaľ ide o vymedzenie, ktorému musí takéto opatrenie na uchovávanie údajov podliehať, je možné ho určiť najmä podľa kategórií dotknutých osôb, keďže článok 15 ods. 1 smernice 2002/58 nebráni právnej úprave založenej na objektívnych skutočnostiach, ktorá umožňuje zamerať sa na osoby, ktorých údaje o prenose dát a polohe môžu aspoň nepriamo súvisieť so závažnou trestnou činnosťou, prispieť

určitým spôsobom k boju proti závažnej trestnej činnosti alebo predchádzať vážnemu nebezpečenstvu pre verejnú bezpečnosť či dokonca nebezpečenstvu pre národnú bezpečnosť (pozri v tomto zmysle rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 111).

149 V tejto súvislosti treba spresniť, že takto vymedzenými osobami môžu byť najmä osoby, ktoré boli v rámci uplatniteľných vnútroštátnych postupov a na základe objektívnych skutočností vopred identifikované ako osoby, ktoré predstavujú hrozbu pre verejnú bezpečnosť alebo národnú bezpečnosť dotknutého členského štátu.

150 Vymedzenie opatrenia umožňujúceho uchovávanie údajov o prenose dát a polohe možno stanoviť aj pomocou geografického kritéria, pokiaľ sa príslušné vnútroštátne orgány na základe objektívnych a nediskriminačných skutočností domnievajú, že v jednej alebo viacerých zemepisných oblastiach existuje vysoké riziko prípravy alebo páchania závažných trestných činov (pozri v tomto zmysle rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 111). Medzi tieto oblasti môžu patriť najmä miesta s vysokým výskytom závažných trestných činov, miesta, ktoré sú v osobitnej miere vystavené páchaniu závažnej trestnej činnosti, akými sú miesta alebo infraštruktúry pravidelne navštevované veľkým počtom osôb, alebo tiež strategické miesta, akými sú letiská, stanice alebo oblasti platenia mýta.

151 S cieľom zabezpečiť, aby zásah, ktorý predstavujú opatrenia na cielené uchovávanie údajov opísané v bodoch 147 až 150 tohto rozsudku, bol v súlade so zásadou proporcionality, ich trvanie nemôže prekročiť dobu, ktorá je striktne nevyhnutná vzhľadom na sledovaný cieľ a okolnosti, ktoré odôvodňujú tieto opatrenia, pričom tým nie je dotknutá možnosť ich obnovenia z dôvodu pretrvávajúcej potreby takéhoto uchovávania údajov.

– O legislatívnych opatreniach, ktoré na účely boja proti trestnej činnosti a ochrany verejnej bezpečnosti stanovujú preventívne uchovávanie IP adries a údajov týkajúcich sa občianskej totožnosti

152 Je potrebné uviesť, že hoci sú IP adresy súčasťou údajov o prenose dát, generujú sa nezávisle od určitej komunikácie a slúžia hlavne na identifikáciu – prostredníctvom poskytovateľov elektronických komunikačných služieb – fyzickej osoby, ktorá je vlastníkom koncového zariadenia, z ktorého sa uskutočňuje internetová komunikácia. V oblasti elektronickej pošty a telefonovania cez internet, pokiaľ sa uchovávajú iba IP adresy zdroja komunikácie, a nie IP adresy adresáta komunikácie, tieto adresy ako také neobsahujú žiadnu informáciu o tretích osobách, ktoré boli v kontakte s osobou, ktorá začala komunikáciu. Táto kategória údajov je teda menej citlivá ako ostatné údaje o prenose dát.

153 Keďže však IP adresy možno použiť na vystopovanie kompletného prechádzania stránok používateľom internetu a následne jeho online aktivít, tieto údaje umožňujú vytvoriť podrobný profil tohto používateľa. Uchovávanie a analýza uvedených IP adries, ktoré sú potrebné na takéto sledovanie, tak predstavujú závažné zásahy do základných práv používateľa internetu zakotvených v článkoch 7 a 8 Charty, čo môže mať odrádzajúce účinky, aké sú uvedené v bode 118 tohto rozsudku.

154 Na účely nevyhnutného zosúladenia dotknutých práv a záujmov, ako to vyžaduje judikatúra uvádzaná v bode 130 tohto rozsudku, je však potrebné zohľadniť skutočnosť, že v prípade trestného činu spáchaného online môže IP adresa predstavovať jediný prostriedok vyšetrovania umožňujúci identifikáciu osoby, ktorej bola táto adresa pridelená v čase spáchania tohto trestného činu. K tomu sa pridáva skutočnosť, že uchovávanie IP adries poskytovateľmi elektronických komunikačných služieb po uplynutí obdobia, na ktoré sú tieto údaje pridelené, sa na účely fakturácie za príslušné služby v zásade nejaví ako potrebné, takže odhaľovanie trestných činov spáchaných online sa preto môže ukázať ako nemožné bez použitia legislatívneho opatrenia na základe článku 15 ods. 1 smernice 2002/58, čo niekoľko vlád uviedlo vo svojich pripomienkach predložených Súdnemu dvoru. Ako uviedli tieto vlády, môže k tomu dôjsť najmä v prípade obzvlášť závažných trestných činov v oblasti detskej pornografie, akými sú nadobúdanie, šírenie, ďalšie postupovanie alebo sprístupňovanie detskej pornografie online

v zmysle článku 2 písm. c) smernice Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV (Ú. v. EÚ L 335, 2011, s. 1).

155 Za týchto okolností, hoci je pravda, že legislatívne opatrenie stanovujúce uchovávanie IP adries všetkých fyzických osôb, ktoré vlastnia koncové zariadenie umožňujúce prístup na internet, by sa týkalo osôb, ktoré na prvý pohľad nemajú žiadnu spojitosť so sledovanými cieľmi v zmysle judikatúry uvádzanej v bode 133 vyššie, a že používatelia internetu majú v súlade s tým, čo bolo konštatované v bode 109 tohto rozsudku, právo očakávať na základe článkov 7 a 8 Charty, že ich totožnosť nebude v zásade odhalená, sa legislatívne opatrenie, ktoré stanovuje všeobecné a nediferencované uchovávanie výlučne IP adries pridelených zdroju spojenia, v zásade nejaví v rozpore s článkom 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty, pokiaľ táto možnosť podlieha prísnemu dodržiavaniu hmotnoprávnych a procesných podmienok, ktoré by mali upravovať použitie týchto údajov.

156 Vzhľadom na závažnosť zásahu do základných práv zakotvených v článkoch 7 a 8 Charty, ktorý predstavuje toto uchovávanie údajov, môže len boj proti závažnej trestnej činnosti a predchádzanie vážnym hrozbám pre verejnú bezpečnosť odôvodňovať takýto zásah. Okrem toho doba uchovávania nemôže trvať dlhšie, než je striktne nevyhnutné vzhľadom na sledovaný cieľ. Napokon musí opatrenie tejto povahy stanoviť prísne podmienky a záruky týkajúce sa použitia týchto údajov, najmä pri sledovaní pohybu na webe, v súvislosti s komunikáciou a aktivitami dotknutých osôb vykonávanými online.

157 Pokiaľ ide nakoniec o údaje týkajúce sa občianskej totožnosti používateľov elektronických komunikačných prostriedkov, tieto údaje samy osebe neumožňujú dozvedieť sa dátum, hodinu, trvanie a adresátov uskutočnených komunikácií, ani miesta, kde k týmto komunikáciám došlo alebo ich frekvenciu s určitými osobami počas daného obdobia, takže okrem kontaktných údajov týchto používateľov, ako napríklad ich adresy, neposkytujú žiadne informácie o danej komunikácii a v dôsledku toho ani o ich súkromnom živote. Zásah, ktorý predstavuje uchovávanie týchto údajov, tak v zásade nemožno kvalifikovať ako závažný (pozri v tomto zmysle rozsudok z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, body 59 a 60).

158 Z toho vyplýva, že v súlade s tým, čo bolo uvedené v bode 140 tohto rozsudku, legislatívne opatrenia týkajúce sa spracovania týchto údajov ako takých, najmä ich uchovávania a prístupu k nim výlučne na účely identifikácie dotknutého používateľa a bez toho, aby bolo možné uvedené údaje spojiť s informáciami o uskutočnených komunikáciách, môžu byť odôvodnené cieľom prevencie, vyšetrovania, odhaľovania a stíhania trestných činov vo všeobecnosti, na ktorý odkazuje článok 15 ods. 1 prvá veta smernice 2002/58 (pozri v tomto zmysle rozsudok z 2. októbra 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, bod 62).

159 Za týchto okolností a vzhľadom na nevyhnutné zosúladenie dotknutých práv a záujmov, ako aj z dôvodov uvedených v bodoch 131 a 158 tohto rozsudku treba dospieť k záveru, že aj v prípade neexistencie spojitosti medzi všetkými používateľmi elektronických komunikačných prostriedkov a sledovanými cieľmi, článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty nebráni legislatívnemu opatreniu, ktoré bez stanovenia konkrétnej lehoty ukladá poskytovateľom elektronických komunikačných služieb povinnosť uchovávať údaje týkajúce sa občianskej totožnosti všetkých používateľov elektronických komunikačných prostriedkov na účely predchádzania, vyšetrovania, odhaľovania a stíhania trestných činov a ochrany verejnej bezpečnosti, pričom nie je potrebné, aby boli trestné činy, hrozby alebo narušenia v oblasti verejnej bezpečnosti závažné.

– O legislatívnych opatreniach, ktoré na účely boja proti závažnej trestnej činnosti stanovujú urýchlené uchovanie údajov o prenose dát a polohe

160 Pokiaľ ide o údaje o prenose dát a polohe spracúvané a uchovávané poskytovateľmi elektronických komunikačných služieb na základe článkov 5, 6 a 9 smernice 2002/58 alebo na základe legislatívnych opatrení prijatých podľa článku 15 ods. 1 tejto smernice, ako sú opísané v bodoch 134 až 159 tohto rozsudku, treba uviesť, že tieto údaje sa v zásade musia podľa okolností vymazať alebo anonymizovať na konci zákonných lehôt, v rámci ktorých sa má uskutočniť ich spracovanie a uchovávanie v súlade s vnútroštátnymi ustanoveniami, ktorými sa táto smernica preberá.

161 Počas tohto spracúvania a uchovávania však môžu nastať situácie, keď je potrebné uchovať uvedené údaje aj po uplynutí týchto lehôt na účely objasnenia závažných trestných činov alebo narušení v oblasti národnej bezpečnosti, a to tak v situácii, keď už mohli byť tieto trestné činy alebo narušenia zistené, ako aj vtedy, keď po objektívnom preskúmaní všetkých relevantných okolností existuje o nich dôvodné podozrenie.

162 V tejto súvislosti je potrebné uviesť, že Dohovor Rady Európy o počítačovej kriminalite z 23. novembra 2001 (séria európskych zmlúv – č. 185), ktorý podpísalo 27 členských štátov a ratifikovalo 25 z nich a ktorého cieľom je uľahčiť boj proti trestným činom spáchaným prostredníctvom počítačových sietí, v článku 14 stanovuje, že zmluvné strany prijmú na účely konkrétneho vyšetrovania alebo trestného konania určité opatrenia týkajúce sa už uložených údajov o prenose dát, ako je napríklad urýchlené uchovanie týchto údajov. Konkrétne článok 16 ods. 1 tohto dohovoru stanovuje, že zmluvné strany prijmú potrebné legislatívne opatrenia, aby umožnili ich príslušným orgánom nariadiť alebo podobným spôsobom zabezpečiť urýchlené uchovanie údajov o prenose dát, ktoré boli uložené prostredníctvom počítačového systému, najmä ak existujú dôvody domnievať sa, že hrozí riziko straty alebo pozmenenia týchto údajov.

163 V situácii, aká je uvedená v bode 161 tohto rozsudku, je vzhľadom na nevyhnutné zosúladenie dotknutých práv a záujmov uvedené v bode 130 tohto rozsudku prípustné, aby členské štáty stanovili v právnej úprave prijatej na základe článku 15 ods. 1 smernice 2002/58 možnosť nariadiť prostredníctvom rozhodnutia príslušného orgánu, ktoré podlieha účinnému súdnemu preskúmaniu, poskytovateľom elektronických komunikačných služieb, aby urýchlene uchovali na potrebný čas údaje o prenose dát a polohe, ktoré majú k dispozícii.

164 Keďže účel takéhoto urýchleného uchovania už nezodpovedá účelu, na ktorý sa údaje pôvodne vyzbierali a uchovávali, a keďže každé spracovanie údajov musí podľa článku 8 ods. 2 Charty zodpovedať konkrétnym cieľom, členské štáty musia vo svojich právnych predpisoch spresniť, na aké účely môže dôjsť k urýchlenému uchovaniu údajov. Vzhľadom na závažnosť zásahu do základných práv zakotvených v článkoch 7 a 8 Charty, ktorý môže predstavovať takéto uchovávanie, môže tento zásah odôvodniť len boj proti závažnej trestnej činnosti a *a fortiori* ochrana národnej bezpečnosti. Okrem toho s cieľom zabezpečiť, aby sa zásah spôsobený opatrením tohto typu obmedzoval na to, čo je striktne nevyhnutné, je na jednej strane potrebné, aby sa povinnosť uchovávania týkala iba údajov o prenose dát a polohe, ktoré môžu prispieť k objasneniu závažného trestného činu alebo narušenia v oblasti príslušnej národnej bezpečnosti. Na druhej strane doba uchovávania údajov nesmie trvať dlhšie, než je striktne nevyhnutné, pričom však môže byť predĺžená, ak to odôvodňujú okolnosti a cieľ sledovaný uvedeným opatrením.

165 V tejto súvislosti treba spresniť, že takéto urýchlené uchovanie sa nemusí obmedzovať na údaje osôb, ktoré sú konkrétne podozrivé zo spáchania trestného činu alebo narušenia v oblasti národnej bezpečnosti. Musí byť v súlade s rámcom stanoveným v článku 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty a vzhľadom na zistenia uvedené v bode 133 tohto rozsudku sa takéto opatrenie môže v závislosti od voľby zákonodarcu a pri dodržaní toho, čo je striktne nevyhnutné, rozšíriť na údaje o prenose dát a polohe týkajúce sa iných osôb, než sú osoby podozrivé z plánovania alebo spáchania závažného trestného činu alebo narušenia v oblasti národnej

bezpečnosti, pokiaľ tieto údaje môžu na základe objektívnych a nediskriminačných skutočností prispieť k objasneniu takéhoto trestného činu alebo narušenia v oblasti národnej bezpečnosti, ako sú napríklad údaje týkajúce sa obete takýchto skutkov, osôb z jej spoločenského alebo profesijného okolia alebo dokonca konkrétnych zemepisných oblastí, akými sú miesta spáchania alebo prípravy trestného činu alebo narušenia v oblasti príslušnej národnej bezpečnosti. Okrem toho sa prístup príslušných orgánov k takto uchovaným údajom musí uskutočňovať pri dodržaní podmienok, ktoré vyplývajú z judikatúry týkajúcej sa výkladu smernice 2002/58 (pozri v tomto zmysle rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, body 118 až 121 a citovanú judikatúru).

166 Treba ešte dodať, ako vyplýva najmä z bodov 115 a 133 tohto rozsudku, že prístup k údajom o prenose dát a polohe uchovávaným poskytovateľmi v súlade s opatrením prijatým na základe článku 15 ods. 1 smernice 2002/58 môže byť v zásade odôvodnený iba cieľom všeobecného záujmu, pre ktorý bolo poskytovateľom nariadené toto uchovávanie. Z toho predovšetkým vyplýva, že prístup k takýmto údajom na účely stíhania a sankcionovania bežného trestného činu nemožno v žiadnom prípade povoliť, ak bolo uchovávanie týchto údajov odôvodnené cieľom boja proti závažnej trestnej činnosti alebo *a fortiori* ochranou národnej bezpečnosti. Na druhej strane, v súlade so zásadou proporcionality, ako bola spresnená v bode 131 tohto rozsudku, prístup k údajom uchovávaným na účely boja proti závažnej trestnej činnosti môže byť za predpokladu dodržania hmotnoprávnych a procesných podmienok spojených s takýmto prístupom, ktoré sú uvedené v predchádzajúcom bode, odôvodnený cieľom ochrany národnej bezpečnosti.

167 V tejto súvislosti je prípustné, aby členské štáty vo svojich právnych predpisoch stanovili, že prístup k údajom o prenose dát a polohe sa môže pri dodržaní tých istých hmotnoprávnych a procesných podmienok povoliť na účely boja proti závažnej trestnej činnosti alebo ochrany národnej bezpečnosti, ak poskytovateľ uchováva tieto údaje v súlade s článkami 5, 6 a 9 alebo článkom 15 ods. 1 smernice 2002/58.

168 Vzhľadom na všetky predchádzajúce úvahy treba na prvé otázky vo veciach C-511/18 a C-512/18, ako aj na prvú a druhú otázku vo veci C-520/18 odpovedať tak, že článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty sa má vykladať v tom zmysle, že bráni legislatívnym opatreniam, ktoré na účely uvedené v tomto článku 15 ods. 1 stanovujú preventívne všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe. Naopak, uvedený článok 15 ods. 1 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty nebráni legislatívnym opatreniam, ktoré:

– umožňujú na účely ochrany národnej bezpečnosti nariadiť poskytovateľom elektronických komunikačných služieb, aby vykonali všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe v situáciách, keď dotknutý členský štát čelí vážnej hrozbe pre národnú bezpečnosť, ktorá sa javí ako skutočná a aktuálna alebo predvídateľná, ak rozhodnutie, ktorým sa vydáva takýto príkaz, môže byť účinne preskúmané zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, pričom cieľom tohto preskúmania je overiť existenciu jednej z týchto situácií a dodržanie podmienok a záruk, ktoré musia byť stanovené, a ak uvedený príkaz možno vydať len na časovo obmedzené obdobie, ktoré je striktne nevyhnutné, s možnosťou jeho predĺženia v prípade pretrvávania takejto hrozby,

– stanovujú na účely ochrany národnej bezpečnosti, boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť cielené uchovávanie údajov o prenose dát a polohe, ktoré je vymedzené na základe objektívnych a nediskriminačných faktorov, podľa kategórií dotknutých osôb alebo prostredníctvom geografického kritéria, na časovo obmedzené obdobie, ktoré je striktne nevyhnutné, s možnosťou jeho predĺženia,

– stanovujú na účely ochrany národnej bezpečnosti, boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť všeobecné a nediferencované uchovávanie IP adries pridelených zdroju spojenia na časovo obmedzené obdobie, ktoré je striktne nevyhnutné,

– stanovujú na účely ochrany národnej bezpečnosti, boja proti trestnej činnosti a ochrany verejnej bezpečnosti všeobecné a nediferencované uchovávanie údajov týkajúcich sa občianskej totožnosti používateľov elektronických komunikačných prostriedkov, a

– umožňujú na účely boja proti závažnej trestnej činnosti a *a fortiori* ochrany národnej bezpečnosti nariadiť prostredníctvom rozhodnutia príslušného orgánu, ktoré podlieha účinnému súdnemu preskúmaniu, poskytovateľom elektronických komunikačných služieb, aby urýchlene uchovali na potrebný čas údaje o prenose dát a polohe, ktoré majú k dispozícii,

pokiaľ tieto opatrenia prostredníctvom jasných a presných pravidiel zabezpečujú, že uchovávanie dotknutých údajov podlieha dodržiavaniu príslušných hmotnoprávnych a procesných podmienok a že dotknuté osoby majú účinné záruky proti rizikám zneužitia.

O druhej a tretej otázke vo veci C-511/18

169 Svojou druhou a treťou otázkou vo veci C-511/18 sa vnútroštátny súd v podstate pýta, či sa má článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá poskytovateľom elektronických komunikačných služieb ukladá povinnosť zaviesť vo svojich sieťach opatrenia, ktoré umožňujú jednak automatizovanú analýzu a zber údajov o prenose dát a polohe v reálnom čase, a jednak zber technických údajov v reálnom čase týkajúcich sa polohy použitých koncových zariadení, pričom nestanovuje požiadavku informovania osôb dotknutých týmto spracovaním a zberom.

170 Vnútroštátny súd poznamenáva, že metódy zberu spravodajských informácií stanovené v článkoch L. 851-2 až L. 851-4 CSI neukladajú poskytovateľom elektronických komunikačných služieb osobitnú povinnosť uchovávať údaje o prenose dát a polohe. Pokiaľ ide konkrétne o automatizovanú analýzu uvedenú v článku L. 851-3 CSI, tento súd uvádza, že cieľom tohto spracúvania je zistiť podľa kritérií stanovených na tento účel pripojenia, ktoré by mohli predstavovať teroristickú hrozbu. V prípade zberu v reálnom čase podľa článku L. 851-2 CSI, uvedený súd konštatuje, že sa týka len jednej alebo viacerých osôb, ktoré boli vopred identifikované ako osoby, ktoré môžu mať spojitosť s teroristickou hrozbou. Podľa toho istého súdu možno tieto dve metódy použiť len na účely predchádzania terorizmu, pričom zahŕňajú údaje uvedené v článkoch L. 851-1 a R. 851-5 CSI.

171 Na úvod treba poznamenať, že skutočnosť, že podľa článku L. 851-3 CSI automatizovaná analýza, ktorú upravuje, ako taká neumožňuje identifikáciu používateľov, ktorých údaje sú predmetom tejto analýzy, nebráni tomu, aby sa tieto údaje kvalifikovali ako „osobné údaje“. Keďže postup upravený v odseku IV toho istého ustanovenia umožňuje v neskoršom štádiu identifikovať jednu alebo viacero osôb, ktorých údaje vyhodnotila automatizovaná analýza tak, že môžu poukazovať na existenciu teroristickej hrozby, všetky osoby, ktorých údaje sú predmetom automatizovanej analýzy, zostávajú na základe týchto údajov identifikovateľné. Podľa definície osobných údajov obsiahnutej v článku 4 bode 1 nariadenia 2016/679 sú takýmito údajmi informácie týkajúce sa okrem iného aj identifikovateľnej osoby.

O automatizovanej analýze údajov o prenose dát a polohe

172 Z článku L. 851-3 CSI vyplýva, že automatizovaná analýza, ktorú upravuje, v podstate zodpovedá filtrácii všetkých údajov o prenose dát a polohe uchovávaných poskytovateľmi elektronických komunikačných služieb, ktorú vykonávajú títo poskytovatelia na žiadosť príslušných vnútroštátnych

orgánov a na základe parametrov, ktoré tieto orgány stanovili. Z toho vyplýva, že sa kontrolujú všetky údaje používateľov elektronických komunikačných prostriedkov, ktoré zodpovedajú týmto parametrom. Takúto automatizovanú analýzu treba preto považovať za analýzu, z ktorej vyplýva, že poskytovatelia elektronických komunikačných služieb vykonajú v mene príslušného orgánu všeobecné a nediferencované spracúvanie vo forme využívania údajov pomocou automatizovaného prostriedku v zmysle článku 4 bodu 2 nariadenia 2016/679, ktorý zahŕňa všetky údaje o prenose dát a polohe všetkých používateľov elektronických komunikačných prostriedkov. Toto spracúvanie je nezávislé od následného zberu údajov o osobách identifikovaných na základe automatizovanej analýzy, pričom tento zber je povolený na základe článku L. 851-3 ods. IV CSI.

173 Vnútroštátna právna úprava, ktorá povoľuje takúto automatizovanú analýzu údajov o prenose dát a polohe, sa odchyľuje od zásadnej povinnosti zabezpečiť dôvernosť elektronických komunikácií a s ňou súvisiacich údajov stanovenej v článku 5 smernice 2002/58. Takáto právna úprava tiež predstavuje zásah do základných práv zakotvených v článkoch 7 a 8 Charty bez ohľadu na to, ako sa tieto údaje následne použijú. Napokon uvedená právna úprava môže mať v súlade s judikatúrou uvedenou v bode 118 tohto rozsudku odrádzajúci účinok na výkon slobody prejavu zakotvenej v článku 11 Charty.

174 Okrem toho zásah vyplývajúci z automatizovanej analýzy údajov o prenose dát a polohe, o aký ide vo veci samej, sa zdá byť obzvlášť závažný, keďže sa všeobecne a bez rozdielu týka údajov osôb používajúcich elektronické komunikačné prostriedky. Toto konštatovanie platí o to viac, ak údaje, ako vyplýva z vnútroštátnej právnej úpravy dotknutej vo veci samej, ktoré sú predmetom automatizovanej analýzy, môžu odhaliť povahu informácií konzultovaných online. Navyše sa takáto automatizovaná analýza globálne týka všetkých osôb používajúcich elektronické komunikačné prostriedky, a teda aj osôb, pri ktorých nie je dôvod domnievať sa, že by ich konanie mohlo mať aspoň nepriamu alebo vzdialenú súvislosť s teroristickými aktivitami.

175 Pokiaľ ide o odôvodnenie takéhoto zásahu, treba poznamenať, že požiadavka stanovená v článku 52 ods. 1 Charty, podľa ktorej musí byť každé obmedzenie výkonu základných práv stanovené zákonom, predpokladá, že samotný právny základ, ktorý umožňuje tento zásah do týchto práv, musí vymedzovať rozsah obmedzenia výkonu dotknutého práva (pozri v tomto zmysle rozsudok zo 16. júla 2020, Facebook Ireland a Schrems, C-311/18, EU:C:2020:559, bod 175, ako aj citovanú judikatúru).

176 Okrem toho na účely splnenia požiadavky proporcionality pripomenutej v bodoch 130 a 131 tohto rozsudku, podľa ktorej výnimky a obmedzenia v súvislosti s ochranou osobných údajov nesmú pôsobiť nad rámec toho, čo je striktne nevyhnutné, musí vnútroštátna právna úprava upravujúca prístup príslušných orgánov k uchovávaným údajom o prenose dát a polohe dodržiavať požiadavky vyplývajúce z judikatúry uvedenej v bode 132 tohto rozsudku. Konkrétne sa takáto právna úprava nemôže obmedziť len na požiadavku, aby prístup orgánov k údajom zodpovedal cieľu sledovanému touto právnou úpravou, ale musí takisto stanoviť hmotnoprávne a procesné podmienky upravujúce toto využívanie [pozri analogicky stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, bod 192 a citovanú judikatúru].

177 V tejto súvislosti treba pripomenúť, že obzvlášť závažný zásah, ktorý predstavuje všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe, ako sa uvádza v zisteniach v bodoch 134 až 139 tohto rozsudku, a rovnako závažný zásah, ktorý predstavuje automatizovaná analýza týchto údajov, môžu spĺňať požiadavku proporcionality len v situáciách, keď dotknutý členský štát čelí vážnej hrozbe pre národnú bezpečnosť, ktorá sa javí ako skutočná a aktuálna alebo predvídateľná, a za predpokladu, že doba tohto uchovávania netrvá dlhšie, než je prísne nevyhnutné.

178 V situáciách ako sú tie, ktoré sú uvedené v predchádzajúcom bode, vykonávanie automatizovanej analýzy údajov o prenose dát a polohe všetkých používateľov elektronických komunikačných prostriedkov počas prísne obmedzeného obdobia možno považovať za odôvodnené z hľadiska požiadaviek vyplývajúcich z článku 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty.

179 S cieľom zabezpečiť, aby sa použitie takéhoto opatrenia skutočne obmedzilo na to, čo je striktne nevyhnutné na ochranu národnej bezpečnosti, a najmä na predchádzanie terorizmu, je však v súlade s konštatovaním uvedeným v bode 139 tohto rozsudku nevyhnutné, aby rozhodnutie, ktorým sa povoľuje automatizovaná analýza mohlo byť účinne preskúmané zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, pričom cieľom tohto preskúmania je overiť, či existuje situácia odôvodňujúca uvedené opatrenie, a či sú splnené podmienky a záruky, ktoré musia byť stanovené.

180 V tejto súvislosti treba spresniť, že vopred stanovené vzory a kritériá, z ktorých tento typ spracúvania údajov vychádza, musia byť na jednej strane konkrétne a spoľahlivé, aby umožnili dosiahnuť výsledky označujúce jednotlivcov, vo vzťahu ku ktorým môže existovať dôvodné podozrenie z účasti na teroristických trestných činoch, a na druhej strane nediskriminačné [pozri v tomto zmysle stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, bod 172].

181 Ďalej je potrebné pripomenúť, že akákoľvek automatizovaná analýza vykonávaná na základe vzorov a kritérií založených na predpoklade, že rasový alebo etnický pôvod, politické názory, vierovyznanie alebo filozofické presvedčenie, členstvo v odborovej organizácii, zdravotný stav alebo sexuálny život osoby by mohli byť sami osebe a bez ohľadu na individuálne správanie tejto osoby relevantné z hľadiska predchádzania terorizmu, by bola v rozpore s právami zaručenými v článkoch 7 a 8 Charty v spojení s jej článkom 21. Vopred stanovené vzory a kritériá na účely automatizovanej analýzy zameranej na predchádzanie teroristickým aktivitám, ktoré predstavujú vážnu hrozbu pre národnú bezpečnosť, tak nemôžu byť založené iba na týchto citlivých údajoch [pozri v tomto zmysle stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, bod 165].

182 Navyše vzhľadom na to, že automatizované analýzy údajov o prenose dát a polohe nevyhnutne vykazujú určitú mieru odchýlky, musí byť každý pozitívny výsledok získaný v nadväznosti na automatizované spracovanie podrobený individuálnemu preskúmaniu prostredníctvom neautomatizovaných prostriedkov ešte pred prijatím individuálneho opatrenia, ktoré by malo na dotknuté osoby negatívny dopad, ako je napríklad následný zber údajov o prenose dát a polohe v reálnom čase, keďže takéto opatrenie sa nemôže rozhodujúcim spôsobom zakladať iba na výsledku automatizovaného spracúvania údajov. Rovnako na zabezpečenie toho, aby vopred stanovené vzory a kritériá, ich využívanie, ako aj používané databázy neboli v praxi diskriminačné a obmedzovali sa len na to, čo je striktne nevyhnutné z hľadiska cieľa predchádzať teroristickým aktivitám, ktoré predstavujú vážnu hrozbu pre národnú bezpečnosť, je potrebné, aby spoľahlivosť a aktuálnosť týchto vopred stanovených vzorov a kritérií, ako aj používaných databáz bola predmetom pravidelného prehodnocovania [pozri v tomto zmysle stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, body 173 a 174].

O zbere údajov o prenose dát a polohe v reálnom čase

183 Pokiaľ ide o zber údajov o prenose dát a polohe v reálnom čase uvedený v článku L. 851-2 CSI, treba uviesť, že tento zber možno individuálne povoliť, ak ide o „osob[u] vopred označen[ú] ako osoba, v prípade ktorej existuje podozrenie, že má väzbu s určitou [teroristickou] hrozbou“. Navyše podľa tohto ustanovenia, „ak existujú závažné dôvody domnievať sa, že jedna alebo viacero osôb patriacich do okolia osoby, ktorej sa týka povolenie, môžu poskytnúť informácie vzhľadom na účel, ktorý odôvodňuje povolenie, možno toto povolenie udeliť individuálne aj pre každú z týchto osôb“.

184 Údaje, ktoré sú predmetom takéhoto opatrenia, umožňujú príslušným vnútroštátnym orgánom nepretržite a v reálnom čase monitorovať počas doby platnosti povolenia osoby, s ktorými dotknuté osoby komunikujú, prostriedky, ktoré používajú, trvanie ich komunikácie, ako aj miesta ich pobytu a presuny. Rovnako sa zdá, že môžu odhaliť povahu informácií konzultovaných online. Tieto údaje ako celok umožňujú, ako vyplýva z bodu 117 tohto rozsudku, vyvodiť veľmi presné závery týkajúce sa súkromného života dotknutých osôb a poskytujú možnosti na vytvorenie profilu týchto osôb, pričom takáto informácia je z hľadiska práva na rešpektovanie súkromného života rovnako citlivá ako samotný obsah komunikácie.

185 Pokiaľ ide o zber údajov v reálnom čase uvedený v článku L. 851-4 CSI, toto ustanovenie povoľuje zber technických údajov týkajúcich sa polohy koncových zariadení a ich prenos v reálnom čase oddeleniu predsedu vlády. Zdá sa, že takéto údaje umožňujú príslušnému oddeleniu kedykoľvek počas doby platnosti povolenia lokalizovať nepretržite a v reálnom čase použité koncové zariadenia, ako napríklad mobilné telefóny.

186 Vnútroštátna právna úprava, ktorá povoľuje takýto zber údajov v reálnom čase, sa tak podobne ako právna úprava povoľujúca automatizovanú analýzu údajov, odchyľuje od zásadnej povinnosti zabezpečiť dôvernosť elektronických komunikácií a s ňou súvisiacich údajov stanovenej v článku 5 smernice 2002/58. Predstavuje teda tiež zásah do základných práv zakotvených v článkoch 7 a 8 Charty a môže mať odrádzajúci účinok na výkon slobody prejavu zaručenej v článku 11 Charty.

187 Treba zdôrazniť, že zásah, ktorý predstavuje zber údajov v reálnom čase umožňujúci lokalizovať koncové zariadenie, sa zdá byť obzvlášť závažný, keďže tieto údaje poskytujú príslušným vnútroštátnym orgánom možnosti presne a trvalo sledovať presuny používateľov mobilných telefónov. Pokiaľ sa teda majú tieto údaje považovať za osobitne citlivé, je potrebné odlíšiť prístup príslušných orgánov k takýmto údajom v reálnom čase od prístupu k nim až po určitom čase, pričom prvý je viac rušivý, keďže umožňuje takmer úplné monitorovanie týchto používateľov (pozri analogicky, pokiaľ ide o článok 8 EDĽP, rozsudok ESĽP, 8. februára 2018, Ben Faiza v. Francúzsko, CE:ECHR:2018:0208JUD003144612, § 74). Intenzita tohto zásahu sa okrem toho zvyšuje, ak sa zber v reálnom čase rozširuje aj na údaje o prenose dát dotknutých osôb.

188 Hoci cieľ spočívajúci v predchádzaní terorizmu, ktorý sleduje vnútroštátna právna úprava dotknutá vo veci samej, môže vzhľadom na jeho dôležitosť odôvodniť zásah vo forme zberu údajov o prenose dát a polohe v reálnom čase, takéto opatrenie možno vzhľadom na jeho osobitne rušivú povahu vykonať len vo vzťahu k osobám, v prípade ktorých existuje oprávnený dôvod k podozreniu, že sa takým či onakým spôsobom podieľali na teroristických aktivitách. Pokiaľ ide o osoby, ktoré nepatria do tejto kategórie, prístup k ich údajom možno získať až po určitom čase, pričom k takémuto prístupu môže podľa judikatúry Súdneho dvora dôjsť len v osobitných situáciách, ako sú tie, v ktorých ide o teroristické aktivity, a ak existujú objektívne skutočnosti, na základe ktorých sa možno domnievať, že tieto údaje môžu v konkrétnom prípade účinne prispieť k boju proti terorizmu (pozri v tomto zmysle rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 119 a citovanú judikatúru).

189 Okrem toho rozhodnutie, ktorým sa povoľuje zber údajov o prenose dát a polohe v reálnom čase, musí byť založené na objektívnych kritériách stanovených vo vnútroštátnej právnej úprave. Konkrétne, táto právna úprava musí v súlade s judikatúrou uvedenou v bode 176 tohto rozsudku vymedziť okolnosti a podmienky, za ktorých možno povoliť takýto zber údajov, a musí stanoviť, ako sa uvádza v predchádzajúcom bode, že týmto zberom môžu byť dotknuté len osoby, ktoré majú spojitosť s cieľom predchádzania terorizmu. Rozhodnutie o povolení zberu údajov o prenose dát a polohe v reálnom čase musí byť navyše založené na objektívnych a nediskriminačných kritériách stanovených vo vnútroštátnej právnej úprave. S cieľom zabezpečiť v praxi dodržiavanie týchto podmienok je nevyhnutné, aby vykonanie opatrenia, ktorým sa povoľuje zber v reálnom čase, podliehalo predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, pričom tento súd alebo orgán sa musia najmä ubezpečiť, že takýto

zber údajov v reálnom čase je povolený iba v medziach toho, čo je prísne nevyhnutné (pozri v tomto zmysle rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 120). V riadne odôvodnených naliehavých prípadoch sa musí preskúmanie uskutočniť v krátkom čase.

O informovaní osôb, ktorých údaje boli vyzbierané alebo analyzované

190 Je dôležité, aby príslušné vnútroštátne orgány vykonávajúce zber údajov o prenose dát a polohe v reálnom čase informovali o tejto skutočnosti dotknuté osoby v rámci uplatniteľných vnútroštátnych postupov v takom rozsahu a v takom okamihu, aby týmto oznámením nebolo možné ohroziť úlohy zverené týmto orgánom. Táto informácia je totiž pre tieto osoby *de facto* nevyhnutná na to, aby mohli vykonať svoje práva vyplývajúce z článkov 7 a 8 Charty, požiadať o prístup k ich osobným údajom, ktoré boli predmetom týchto opatrení, a prípadne o ich opravu alebo odstránenie, ako aj podať v súlade s článkom 47 prvým odsekom Charty účinný opravný prostriedok na súde, pričom takéto právo je navyše výslovne zaručené v článku 15 ods. 2 smernice 2002/58 v spojení s článkom 79 ods. 1 nariadenia 2016/679 [pozri v tomto zmysle rozsudok z 21. decembra 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 121 a citovanú judikatúru, ako aj stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, body 219 a 220].

191 Pokiaľ ide o požiadavku informovania v kontexte automatizovanej analýzy údajov o prenose dát a polohe, príslušný vnútroštátny orgán je povinný uverejniť informácie všeobecnej povahy týkajúce sa tejto analýzy bez toho, aby musel individuálne informovať dotknuté osoby. Na druhej strane, ak údaje zodpovedajú parametrom stanoveným v opatrení povoľujúcom automatizovanú analýzu a tento orgán vykoná identifikáciu dotknutej osoby na účely hlbšej analýzy údajov, ktoré sa jej týkajú, individuálne informovanie tejto osoby sa zdá byť nevyhnutné. K takémuto informovaniu však môže dôjsť len v takom rozsahu a v takom okamihu, aby ním nebolo možné ohroziť úlohy zverené týmto orgánom [pozri analogicky stanovisko 1/15 (Dohoda PNR medzi EÚ a Kanadou) z 26. júla 2017, EU:C:2017:592, body 222 až 224].

192 Vzhľadom na všetky vyššie uvedené úvahy treba na druhú a tretiu otázku vo veci C-511/18 odpovedať tak, že článok 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty sa má vykladať v tom zmysle, že nebráni vnútroštátnej právnej úprave, ktorá od poskytovateľov elektronických komunikačných služieb vyžaduje, aby použili jednak automatizovanú analýzu a zber najmä údajov o prenose dát a polohe v reálnom čase a jednak zber technických údajov v reálnom čase týkajúcich sa polohy použitých koncových zariadení, za predpokladu, že:

– použitie automatizovanej analýzy sa obmedzí na situácie, keď dotknutý členský štát čelí vážnej hrozbe pre národnú bezpečnosť, ktorá sa javí ako skutočná a aktuálna alebo predvídateľná, pričom použitie tejto analýzy môže byť predmetom účinného preskúmania zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, s cieľom overiť, či existuje situácia odôvodňujúca uvedené opatrenie a či sú splnené podmienky a záruky, ktoré musia byť stanovené, a že

– vykonanie zberu údajov o prenose dát a polohe v reálnom čase sa obmedzí na osoby, v prípade ktorých existuje oprávnený dôvod na podozrenie, že sa určitým spôsobom podieľajú na teroristických aktivitách, a podlieha predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, aby sa zabezpečilo, že takýto zber údajov v reálnom čase je povolený iba v medziach toho, čo je prísne nevyhnutné. V riadne odôvodnených naliehavých prípadoch sa musí preskúmanie uskutočniť v krátkom čase.

O druhej otázke vo veci C-512/18

193 Druhou otázkou vo veci C-512/18 sa vnútroštátny súd v podstate pýta, či sa ustanovenia smernice 2000/31 v spojení s článkami 6 až 8 a 11, ako aj s článkom 52 ods. 1 Charty majú vykladať v tom zmysle, že bránia vnútroštátnej právnej úprave, ktorá ukladá poskytovateľom prístupu verejnosti ku komunikačným službám online a poskytovateľom hostingových služieb povinnosť všeobecne a nediferencovane uchovávať najmä osobné údaje súvisiace s týmito službami.

194 Podľa vnútroštátneho súdu takéto služby patria skôr do pôsobnosti smernice 2000/31 ako do pôsobnosti smernice 2002/58, pričom zastáva názor, že článok 15 ods. 1 a 2 smernice 2000/31 v spojení s jej článkami 12 a 14 sám osebe nestanovuje zásadný zákaz uchovávania údajov týkajúcich sa tvorby obsahu, od ktorého by bolo možné sa odchýliť len výnimočne. Tento súd sa však pýta, či možno toto posúdenie prijať vzhľadom na nevyhnutné dodržanie základných práv zakotvených v článkoch 6 až 8 a 11 Charty.

195 Vnútroštátny súd okrem toho spresňuje, že jeho otázka je položená v súvislosti s povinnosťou uchovávania stanovenou v článku 6 LCEN v spojení s dekrétom č. 2011-219. Údaje, ktoré musia z tohto dôvodu uchovávať dotknutí poskytovatelia služieb, zahŕňajú najmä údaje týkajúce sa občianskej totožnosti osôb, ktoré využili tieto služby, akými sú ich meno, priezvisko, súvisiace poštové adresy, súvisiace e-mailové adresy a adresy účtu, ich heslá a v prípade, že je podpísanie zmluvy alebo vytvorenie účtu spoplatnené, druh použitej platby, referenčné číslo platby, suma, ako aj dátum a čas transakcie.

196 Údaje, ktoré sú predmetom povinnosti uchovávania, ďalej zahŕňajú identifikátory účastníkov, pripojení a použitých koncových zariadení, identifikátory priradené obsahu, dátumy a časy začatia a ukončenia pripojení a operácií, ako aj typy protokolov použitých na pripojenie k službe a na prenos obsahu. O prístup k týmto údajom, ktorých doba uchovávania je jeden rok, možno požiadať v trestnom a občianskom konaní, aby sa s zabezpečilo dodržiavanie pravidiel týkajúcich sa občianskoprávnej alebo trestnej zodpovednosti, ako aj v rámci opatrení na zber spravodajských informácií, na ktoré sa vzťahuje článok L. 851-1 CSI.

197 V tejto súvislosti treba uviesť, že smernica 2000/31 podľa jej článku 1 ods. 2 harmonizuje určité vnútroštátne ustanovenia o službách informačnej spoločnosti uvedených v jej článku 2 písm. a).

198 Je pravda, že medzi tieto služby patria tie, ktoré sú poskytované na diaľku prostredníctvom elektronických zariadení na spracovanie a ukladanie údajov, na individuálnu žiadosť príjemcu služieb a zvyčajne za úhradu, ako sú napríklad služby poskytujúce prístup na internet alebo ku komunikačnej sieti a hostiteľské služby (pozri v tomto zmysle rozsudky z 24. novembra 2011, Scarlet Extended, C-70/10, EU:C:2011:771, bod 40; zo 16. februára 2012, SABAM, C-360/10, EU:C:2012:85, bod 34; z 15. septembra 2016, Mc Fadden, C-484/14, EU:C:2016:689, bod 55, ako aj zo 7. augusta 2018, SNB-REACT, C-521/17, EU:C:2018:639, bod 42 a citovanú judikatúru).

199 Článok 1 ods. 5 písm. b) smernice 2000/31 však stanovuje, že táto smernica sa neuplatňuje na otázky týkajúce sa služieb informačnej spoločnosti, na ktoré sa vzťahujú smernice 95/46 a 97/66. Z odôvodnení 14 a 15 smernice 2000/31 v tejto súvislosti vyplýva, že ochranu dôvernosti komunikácie a jednotlivcov v súvislosti so spracovaním osobných údajov v rámci služieb informačnej spoločnosti upravujú výlučne smernice 95/46 a 97/66, pričom táto posledná uvedená smernica v článku 5 zakazuje na účely ochrany dôvernosti komunikácie akúkoľvek formu odpočúvania alebo dohľadu nad komunikáciami.

200 Otázky týkajúce sa ochrany dôvernosti komunikácie a osobných údajov tak treba posudzovať z hľadiska smernice 2002/58 a nariadenia 2016/679, ktoré v príslušnom poradí nahradili smernicu 97/66 a smernicu 95/46, pričom je potrebné spresniť, že ochrana, ktorú má zabezpečiť smernica 2000/31,

nemôže v žiadnom prípade porušovať požiadavky vyplývajúce zo smernice 2002/58 a z nariadenia 2016/679 (pozri v tomto zmysle rozsudok z 29. januára 2008, Promusicae, C-275/06, EU:C:2008:54, bod 57).

201 Povinnosť uložená vnútroštátnou právnou úpravou uvedenou v bode 195 tohto rozsudku poskytovateľom prístupu verejnosti ku komunikačným službám online a poskytovateľom hostingových služieb, ktorá od nich vyžaduje uchovávať osobné údaje týkajúce sa týchto služieb, sa teda musí posúdiť, ako v podstate uviedol generálny advokát v bode 141 svojich návrhov v spojených veciach La Quadrature du Net a i. (C-511/18 a C-512/18, EU:C:2020:6), z hľadiska smernice 2002/58 alebo nariadenia 2016/679.

202 Poskytovanie služieb, na ktoré sa vzťahuje táto vnútroštátna právna úprava, sa teda v závislosti od toho, či patrí alebo nepatrí do pôsobnosti smernice 2002/58, bude riadiť buď touto smernicou, konkrétne jej článkom 15 ods. 1 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty, alebo nariadením 2016/679, konkrétne jeho článkom 23 ods. 1 v spojení s tými istými ustanoveniami Charty.

203 V prejednávanej veci nemožno vylúčiť, ako uviedla Európska komisia vo svojich písomných pripomienkach, že niektoré služby, na ktoré sa vzťahuje vnútroštátna právna úprava uvedená v bode 195 tohto rozsudku, predstavujú elektronické komunikačné služby v zmysle smernice 2002/58, čo prináleží overiť vnútroštátnemu súdu.

204 V tejto súvislosti treba uviesť, že smernica 2002/58 sa vzťahuje na elektronické komunikačné služby, ktoré spĺňajú podmienky stanovené v článku 2 písm. c) smernice 2002/21, na ktorý odkazuje článok 2 smernice 2002/58 a ktorý vymedzuje elektronickú komunikačnú službu ako „službu bežne poskytovanú za úhradu, ktorá pozostáva úplne alebo prevažne z prenosu signálov v elektronických komunikačných sieťach, vrátane telekomunikačných služieb a prenosových služieb v sieťach používaných na vysielanie“. Pokiaľ ide o služby informačnej spoločnosti, ktoré sú uvedené v bodoch 197 a 198 tohto rozsudku a na ktoré sa vzťahuje smernica 2000/31, tieto služby predstavujú elektronické komunikačné služby, pokiaľ pozostávajú úplne alebo prevažne z prenosu signálov v elektronických komunikačných sieťach (pozri v tomto zmysle rozsudok z 5. júna 2019, Skype Communications, C-142/18, EU:C:2019:460, body 47 a 48).

205 Služby prístupu na internet, na ktoré sa zrejme vzťahuje vnútroštátna právna úprava uvedená v bode 195 tohto rozsudku, tak predstavujú, ako to potvrdzuje odôvodnenie 10 smernice 2002/21, elektronické komunikačné služby v zmysle tejto smernice (pozri v tomto zmysle rozsudok z 5. júna 2019, Skype Communications, C-142/18, EU:C:2019:460, bod 37). To platí aj pre internetové e-mailové služby, pri ktorých podľa všetkého nie je vylúčené, že sa na ne rovnako vzťahuje táto vnútroštátna právna úprava, keďže z technického hľadiska predpokladá úplne alebo hlavne prenos signálov v elektronických komunikačných sieťach (pozri v tomto zmysle rozsudok z 13. júna 2019, Google, C-193/18, EU:C:2019:498, body 35 a 38).

206 Pokiaľ ide o požiadavky vyplývajúce z článku 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty, treba odkázať na všetky zistenia a posúdenia vykonané v rámci odpovede na prvé otázky vo veciach C-511/18 a C-512/18, ako aj na prvú a druhú otázku vo veci C-520/18.

207 V prípade požiadaviek vyplývajúcich z nariadenia 2016/679, treba pripomenúť, že cieľom tohto nariadenia je najmä, ako vyplýva z jeho odôvodnenia 10, zaručiť vysokú úroveň ochrany fyzických osôb v rámci Únie a na tento účel zabezpečiť konzistentné a jednotné uplatňovanie pravidiel ochrany základných práv a slobôd týchto osôb v súvislosti so spracúvaním osobných údajov v celej Únii (pozri v tomto zmysle rozsudok zo 16. júla 2020, Facebook Ireland a Schrems, C-311/18, EU:C:2020:559, bod 101).

208 Na tento účel musí každé spracúvanie osobných údajov, okrem výnimiek prípustných v článku 23 nariadenia 2016/679, dodržiavať zásady spracúvania osobných údajov a práva dotknutej osoby stanovené v kapitolách II a III tohto nariadenia. Konkrétne musí každé spracúvanie osobných údajov na jednej strane byť v súlade so zásadami stanovenými v článku 5 uvedeného nariadenia a na druhej strane spĺňať podmienky týkajúce sa zákonnosti vymenované v článku 6 toho istého nariadenia (pozri analogicky, pokiaľ ide o smernicu 95/46, rozsudok z 30. mája 2013, Worten, C-342/12, EU:C:2013:355, bod 33 a citovanú judikatúru).

209 Pokiaľ ide konkrétne o článok 23 ods. 1 nariadenia 2016/679, treba uviesť, že tento článok, podobne ako je stanovené v článku 15 ods. 1 smernice 2002/58, umožňuje členským štátom obmedziť na účely cieľov, ktoré sleduje, a prostredníctvom legislatívnych opatrení rozsah povinností a práv, ktoré sú v ňom uvedené, „ak takéto obmedzenie rešpektuje podstatu základných práv a slobôd a je nevyhnutným a primeraným opatrením v demokratickej spoločnosti s cieľom zaistiť“ sledovaný cieľ. Každé legislatívne opatrenie prijaté na tomto základe musí predovšetkým spĺňať osobitné požiadavky stanovené v článku 23 ods. 2 tohto nariadenia.

210 Článok 23 ods. 1 a 2 nariadenia č. 2016/679 preto nemožno vykladať tak, že by členským štátom mohol priznávať právomoc narušiť rešpektovanie súkromného života v rozpore s článkom 7 Charty alebo iné záruky stanovené v tejto Charte (pozri analogicky, pokiaľ ide o smernicu 95/46, rozsudok z 20. mája 2003, Österreichischer Rundfunk a i., C-465/00, C-138/01 a C-139/01, EU:C:2003:294, bod 91). Konkrétne možno právomoc, ktorú členským štátom priznáva článok 23 ods. 1 nariadenia 2016/679, vykonávať, podobne ako to platí v prípade článku 15 ods. 1 smernice 2002/58, len pri dodržaní požiadavky proporcionality, podľa ktorej výnimky a obmedzenia v súvislosti s ochranou osobných údajov nesmú pôsobiť nad rámec toho, čo je prísne nevyhnutné (pozri analogicky, pokiaľ ide o smernicu 95/46, rozsudok zo 7. novembra 2013, IPI, C-473/12, EU:C:2013:715, bod 39 a citovanú judikatúru).

211 Z toho vyplýva, že zistenia a posúdenia vykonané v rámci odpovede na prvé otázky vo veciach C-511/18 a C-512/18, ako aj na prvú a druhú otázku vo veci C-520/18, sa uplatňujú *mutatis mutandis* aj na článok 23 nariadenia 2016/679.

212 Vzhľadom na predchádzajúce úvahy treba na druhú otázku vo veci C-512/18 odpovedať tak, že smernica 2000/31 sa má vykladať v tom zmysle, že nie je uplatniteľná v oblasti ochrany dôvernosti komunikácie a jednotlivcov v súvislosti so spracovaním osobných údajov v rámci služieb informačnej spoločnosti, pričom táto ochrana sa podľa okolností riadi smernicou 2002/58 alebo nariadením 2016/679. Článok 23 ods. 1 nariadenia 2016/679 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty sa má vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá ukladá poskytovateľom prístupu verejnosti ku komunikačným službám online a poskytovateľom hostingových služieb povinnosť všeobecne a nediferencovane uchovávať najmä osobné údaje súvisiace s týmito službami.

O tretej otázke vo veci C-520/18

213 Treťou otázkou vo veci C-520/18 sa vnútroštátny súd v podstate pýta, či môže vnútroštátny súd uplatniť ustanovenie vnútroštátneho práva, ktoré ho oprávňuje obmedziť časové účinky vyhlásenia protiprávnosti, ktoré mu prislúcha urobiť podľa tohto práva vo vzťahu k vnútroštátnej právnej úprave ukladajúcej poskytovateľom elektronických komunikačných služieb – okrem iného na účely sledovania cieľov ochrany národnej bezpečnosti a boja proti trestnej činnosti – povinnosť všeobecne a nediferencovane uchovávať údaje o prenose dát a polohe, a to z dôvodu, že toto uchovávanie je nezlučiteľné s článkom 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty.

214 Zásada prednosti práva Únie zakotvuje prednostné postavenie práva Únie pred právom členských štátov. Táto zásada preto ukladá všetkým orgánom členských štátov povinnosť zaručiť plný účinok jednotlivých noriem Únie, pričom právo členských štátov nemôže mať vplyv na účinok priznaný týmto rôznym normám na území uvedených štátov [rozsudky z 15. júla 1964, Costa, 6/64, EU:C:1964:66, s. 1159 a 1160, a z 19. novembra 2019, A. K. a i. (Nezávislosť disciplinárneho senátu Najvyššieho súdu), C-585/18, C-624/18 a C-625/18, EU:C:2019:982, body 157 a 158 a citovaná judikatúra].

215 Zásada prednosti práva Únie vyžaduje, aby v prípade nemožnosti vyložiť vnútroštátnu právnu úpravu v súlade s požiadavkami práva Únie vnútroštátny súd, ktorý je v rámci svojej právomoci poverený uplatňovať ustanovenia práva Únie, zabezpečil ich plný účinok, pričom v prípade potreby z vlastnej iniciatívy neuplatní akékoľvek odporujúce ustanovenie vnútroštátneho práva, hoci aj časovo následné, a to bez toho, aby musel požiadať alebo vyčkať na jeho predchádzajúce zrušenie zákonodarnou cestou alebo akýmkoľvek iným ústavným postupom [rozsudky z 22. júna 2010, Melki a Abdeli, C-188/10 a C-189/10, EU:C:2010:363, bod 43 a citovaná judikatúra; z 24. júna 2019, Popławski, C-573/17, EU:C:2019:530, bod 58, ako aj z 19. novembra 2019, A. K. a i. (Nezávislosť disciplinárneho senátu Najvyššieho súdu), C-585/18, C-624/18 a C-625/18, EU:C:2019:982, bod 160].

216 Iba Súdny dvor môže výnimočne a z naliehavých dôvodov právnej istoty priznať dočasné pozastavenie účinku vylúčenia vyplývajúceho z právneho predpisu Únie vo vzťahu k vnútroštátnemu právu, ktoré je v rozpore s týmto predpisom. Takéto obmedzenie časových účinkov výkladu tohto práva poskytnutého Súdnym dvorom možno pripustiť len v samotnom rozsudku, ktorým sa rozhoduje o požadovanom výklade [pozri v tomto zmysle rozsudky z 23. októbra 2012, Nelson a i., C-581/10 a C-629/10, EU:C:2012:657, body 89 a 91; z 23. apríla 2020, Herst, C-401/18, EU:C:2020:295, body 56 a 57, ako aj z 25. júna 2020, A a i. (Veterné elektrárne v Aalter a Nevele), C-24/19, EU:C:2020:503, bod 84 a citovaná judikatúra].

217 Ak by totiž vnútroštátne súdy mali právomoc priznať vnútroštátnym ustanoveniam prednosť pred právom Únie, ktorému tieto ustanovenia odporujú, hoci len dočasne, došlo by k narušeniu prednosti a jednotného uplatňovania práva Únie (pozri v tomto zmysle rozsudok z 29. júla 2019, Inter-Environnement Wallonie a Bond Beter Leefmile Vlaanderen, C-411/17, EU:C:2019:622, bod 177 a citovanú judikatúru).

218 Súdny dvor však vo veci, v ktorej išlo o zákonnosť opatrení prijatých v rozpore s povinnosťou podľa práva Únie vykonať predbežné posúdenie vplyvov projektu na životné prostredie a chránenú lokalitu, rozhodol, že vnútroštátny súd môže, ak to vnútroštátne právo umožňuje, výnimočne zachovať účinky takýchto opatrení, pokiaľ je toto zachovanie odôvodnené naliehavými dôvodmi spojenými s potrebou odvrátiť skutočnú a vážnu hrozbu prerušenia zásobovania dotknutého členského štátu elektrickou energiou, ktorej nemožno čeliť inými prostriedkami a alternatívnymi riešeniami najmä v rámci vnútorného trhu, pričom uvedené zachovanie môže pokrývať len časový úsek, ktorý je striktne nevyhnutný na odstránenie protiprávnosti (pozri v tomto zmysle rozsudok z 29. júla 2019, Inter-Environnement Wallonie a Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, body 175, 176, 179 a 181).

219 Na rozdiel od opomenutia procesnej povinnosti, akou je predchádzajúce posúdenie vplyvov projektu v konkrétnej oblasti ochrany životného prostredia, porušenie článku 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty nemožno napraviť postupom, ktorý je porovnateľný s postupom uvedeným v predchádzajúcom bode. Zachovanie účinkov vnútroštátnej právnej úpravy, o akú ide vo veci samej, by totiž znamenalo, že táto právna úprava by naďalej ukladala poskytovateľom elektronických komunikačných služieb povinnosti, ktoré sú v rozpore s právom Únie a ktoré závažným spôsobom zasahujú do základných práv osôb, ktorých údaje boli uchovávané.

220 Vnútroštátny súd preto nemôže uplatniť ustanovenie vnútroštátneho práva, ktoré ho oprávňuje obmedziť časové účinky vyhlásenia protiprávnosti, ktoré mu prislúcha urobiť podľa tohto práva, pokiaľ ide o vnútroštátnu právnu úpravu dotknutej vo veci samej.

221 Za týchto okolností VZ, WY a XX vo svojich pripomienkach predložených Súdnemu dvoru tvrdia, že tretia otázka implicitne, ale nevyhnutne nastoľuje otázku, či právo Únie bráni tomu, aby sa v rámci trestného konania použili informácie a dôkazy získané prostredníctvom všeobecného a nediferencovaného uchovávania údajov o prenose dát a polohe, ktoré je nezlučiteľné s týmto právom.

222 V tejto súvislosti a s cieľom poskytnúť vnútroštátnemu súdu užitočnú odpoveď treba pripomenúť, že za súčasného stavu práva Únie v zásade prináleží iba vnútroštátnemu právu, aby v rámci trestného konania vedeného proti osobám podozrivým zo závažnej trestnej činnosti určilo pravidlá týkajúce sa prípustnosti a posúdenia informácií a dôkazov získaných takýmto uchovávaním údajov, ktoré je v rozpore s právom Únie.

223 Z ustálenej judikatúry totiž vyplýva, že v prípade neexistencie pravidiel Únie v danej oblasti prináleží vnútroštátnemu právnemu poriadku každého členského štátu, aby na základe zásady procesnej autonómie upravil procesné podmienky žalôb určených na zabezpečenie ochrany práv, ktoré osobám podliehajúcim súdnej právomoci vyplývajú z práva Únie, avšak pod podmienkou, že nie sú menej výhodné ako procesné podmienky, ktoré upravujú podobné situácie podľa vnútroštátneho práva (zásada ekvivalencie), a nevedú k praktickému znemožneniu alebo nadmernému sťaženiu výkonu práv priznaných právom Únie (zásada efektivity) (pozri v tomto zmysle rozsudky zo 6. októbra 2015, Târşia, C-69/14, EU:C:2015:662, body 26 a 27; z 24. októbra 2018, XC a i., C-234/17, EU:C:2018:853, body 21 a 22, ako aj citovanú judikatúru, a z 19. decembra 2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, bod 33).

224 Pokiaľ ide o zásadu ekvivalencie, prináleží vnútroštátnemu súdu, ktorý rozhoduje v trestnom konaní založenom na informáciách alebo dôkazoch získaných v rozpore s požiadavkami vyplývajúcimi zo smernice 2002/58, aby overil, či vnútroštátne právo, ktorým sa riadi toto konanie, stanovuje menej priaznivé pravidlá, pokiaľ ide o prípustnosť a využitie takýchto informácií a dôkazov, než sú pravidlá upravujúce informácie a dôkazy získané v rozpore s vnútroštátnym právom.

225 V súvislosti so zásadou efektivity treba uviesť, že cieľom vnútroštátnych pravidiel týkajúcich sa prípustnosti a použitia informácií a dôkazov je v súlade so zámermi vnútroštátneho práva zabrániť tomu, aby informácie a dôkazy, ktoré boli získané protiprávne, neprimerane poškodili osobu podozrivú zo spáchania trestných činov. Tento cieľ možno podľa vnútroštátneho práva dosiahnuť nielen zákazom využívania takýchto informácií a dôkazov, ale aj vnútroštátnymi pravidlami a postupmi, ktoré upravujú posúdenie a vyváženie informácií a dôkazov, či dokonca zohľadnením ich protiprávnosti pri určovaní trestu.

226 Z judikatúry Súdneho dvora však vyplýva, že pri rozhodovaní o potrebe vylúčiť informácie a dôkazy získané v rozpore s požiadavkami práva Únie sa musí zohľadniť najmä riziko, ktoré predstavuje pripustenie takýchto informácií a dôkazov pre dodržanie zásady kontradiktórnosti, a teda aj práva na spravodlivý proces (pozri v tomto zmysle rozsudok z 10. apríla 2003, Steffensen, C-276/01, EU:C:2003:228, body 76 a 77). Ak súd dospeje k záveru, že účastník konania nie je schopný účinne sa vyjadriť k dôkaznému prostriedku, ktorý patrí do oblasti mimo znalostí súdu a ktorý môže mať podstatný vplyv na posúdenie skutkového stavu, musí konštatovať porušenie práva na spravodlivý proces a vylúčiť tento dôkaz s cieľom zabrániť takémuto porušovaniu (pozri v tomto zmysle rozsudok z 10. apríla 2003, Steffensen, C-276/01, EU:C:2003:228, body 78 a 79).

227 Zásada efektivity preto vyžaduje, aby vnútroštátny trestný súd v rámci trestného konania vedeného proti osobám podozrivým z trestnej činnosti vylúčil informácie a dôkazy získané prostredníctvom všeobecného a nediferencovaného uchovávania údajov o prenose dát a polohe, ktoré je nezlučiteľné s právom Únie, ak tieto osoby nie sú schopné účinne sa vyjadriť k týmto informáciám a dôkazom, ktoré pochádzajú z oblasti mimo znalostí súdu a ktoré môžu mať podstatný vplyv na posúdenie skutkového stavu.

228 Vzhľadom na predchádzajúce úvahy treba na tretiu otázku vo veci C-520/18 odpovedať tak, že vnútroštátny súd nemôže uplatniť ustanovenie vnútroštátneho práva, ktoré ho oprávňuje obmedziť časové účinky vyhlásenia protiprávnosti, ktoré mu prislúcha urobiť podľa tohto práva vo vzťahu k vnútroštátnej právnej úprave ukladajúcej poskytovateľom elektronických komunikačných služieb – najmä na účely ochrany národnej bezpečnosti a boja proti trestnej činnosti – povinnosť vyžadujúcu všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe, ktoré je nezlučiteľné s článkom 15 ods. 1 smernice 2002/58 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty. Tento článok 15 ods. 1 vykladaný z hľadiska zásady efektivity vyžaduje, aby vnútroštátny trestný súd v rámci trestného konania vedeného proti osobám podozrivým z trestnej činnosti vylúčil informácie a dôkazy získané prostredníctvom všeobecného a nediferencovaného uchovávania údajov o prenose dát a polohe, ktoré je nezlučiteľné s právom Únie, ak tieto osoby nie sú schopné účinne sa vyjadriť k týmto informáciám a dôkazom, ktoré pochádzajú z oblasti mimo znalostí súdu a ktoré môžu mať podstatný vplyv na posúdenie skutkového stavu.

O trovách

229 Vzhľadom na to, že konanie pred Súdnym dvorom má vo vzťahu k účastníkom konania vo veci samej incidenčný charakter a bolo začaté v súvislosti s prekážkou postupu v konaní pred vnútroštátnymi súdmi, o trovách konania rozhodnú tieto vnútroštátne súdy. Iné trovy konania, ktoré vznikli v súvislosti s predložením pripomienok Súdnemu dvoru a nie sú trovami uvedených účastníkov konania, nemôžu byť nahradené.

Z týchto dôvodov Súdny dvor (veľká komora) rozhodol takto:

1. **Článok 15 ods. 1 smernice Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), zmenenej smernicou Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty základných práv Európskej únie sa má vykladať v tom zmysle, že bráni legislatívnym opatreniam, ktoré na účely uvedené v tomto článku 15 ods. 1 stanovujú preventívne všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe. Naopak, článok 15 ods. 1 smernice 2002/58, zmenenej smernicou 2009/136, v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty základných práv nebráni legislatívnym opatreniam, ktoré:**

   – **umožňujú na účely ochrany národnej bezpečnosti nariadiť poskytovateľom elektronických komunikačných služieb, aby vykonali všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe v situáciách, keď dotknutý členský štát čelí vážnej hrozbe pre národnú bezpečnosť, ktorá sa javí ako skutočná a aktuálna alebo predvídateľná, ak rozhodnutie, ktorým sa vydáva takýto príkaz, môže byť účinne preskúmané zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, pričom cieľom tohto preskúmania je overiť existenciu jednej z týchto situácií a dodržanie podmienok a záruk, ktoré musia byť stanovené, a ak uvedený príkaz možno vydať len na časovo obmedzené obdobie, ktoré je striktne nevyhnutné, s možnosťou jeho predĺženia v prípade pretrvávania takejto hrozby,**

   – **stanovujú na účely ochrany národnej bezpečnosti, boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť cielené uchovávanie údajov o prenose dát a polohe, ktoré je vymedzené na základe objektívnych a nediskriminačných faktorov, podľa kategórií dotknutých osôb alebo prostredníctvom geografického kritéria, na časovo obmedzené obdobie, ktoré je striktne nevyhnutné, s možnosťou jeho predĺženia,**

– **stanovujú na účely ochrany národnej bezpečnosti, boja proti závažnej trestnej činnosti a predchádzania vážnym hrozbám pre verejnú bezpečnosť všeobecné a nediferencované uchovávanie IP adries pridelených zdroju spojenia na časovo obmedzené obdobie, ktoré je striktne nevyhnutné,**

– **stanovujú na účely ochrany národnej bezpečnosti, boja proti trestnej činnosti a ochrany verejnej bezpečnosti všeobecné a nediferencované uchovávanie údajov týkajúcich sa občianskej totožnosti používateľov elektronických komunikačných prostriedkov, a**

– **umožňujú na účely boja proti závažnej trestnej činnosti a *a fortiori* ochrany národnej bezpečnosti nariadiť prostredníctvom rozhodnutia príslušného orgánu, ktoré podlieha účinnému súdnemu preskúmaniu, poskytovateľom elektronických komunikačných služieb, aby urýchlene uchovali na potrebný čas údaje o prenose dát a polohe, ktoré majú k dispozícii,**

pokiaľ tieto opatrenia prostredníctvom jasných a presných pravidiel zabezpečujú, že uchovávanie dotknutých údajov podlieha dodržiavaniu príslušných hmotnoprávnych a procesných podmienok a že dotknuté osoby majú účinné záruky proti rizikám zneužitia.

2. **Článok 15 ods. 1 smernice 2002/58, zmenenej smernicou 2009/136, v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty základných práv sa má vykladať v tom zmysle, že nebráni vnútroštátnej právnej úprave, ktorá od poskytovateľov elektronických komunikačných služieb vyžaduje, aby použili jednak automatizovanú analýzu a zber najmä údajov o prenose dát a polohe v reálnom čase, a jednak zber technických údajov v reálnom čase týkajúcich sa polohy použitých koncových zariadení, za predpokladu, že:**

   – **použitie automatizovanej analýzy sa obmedzí na situácie, keď dotknutý členský štát čelí vážnej hrozbe pre národnú bezpečnosť, ktorá sa javí ako skutočná a aktuálna alebo predvídateľná, pričom použitie tejto analýzy môže byť predmetom účinného preskúmania zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, s cieľom overiť, či existuje situácia odôvodňujúca uvedené opatrenie a či sú splnené podmienky a záruky, ktoré musia byť stanovené, a že**

   – **vykonanie zberu údajov o prenose dát a polohe v reálnom čase sa obmedzí na osoby, v prípade ktorých existuje oprávnený dôvod na podozrenie, že sa určitým spôsobom podieľajú na teroristických aktivitách, a podlieha predchádzajúcemu preskúmaniu zo strany súdu alebo nezávislého správneho orgánu, ktorého rozhodnutie má záväzný účinok, aby sa zabezpečilo, že takýto zber údajov v reálnom čase je povolený iba v medziach toho, čo je prísne nevyhnutné. V riadne odôvodnených naliehavých prípadoch sa musí preskúmanie uskutočniť v krátkom čase.**

3. **Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode), sa má vykladať v tom zmysle, že nie je uplatniteľná v oblasti ochrany dôvernosti komunikácie a jednotlivcov v súvislosti so spracovaním osobných údajov v rámci služieb informačnej spoločnosti, pričom táto ochrana sa podľa okolností riadi smernicou 2002/58, zmenenou smernicou 2009/136, alebo nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46. Článok 23 ods. 1 nariadenia 2016/679 v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty základných práv sa má vykladať v tom zmysle, že bráni vnútroštátnej právnej úprave, ktorá ukladá poskytovateľom prístupu verejnosti ku komunikačným službám online a poskytovateľom hostingových služieb povinnosť všeobecne a nediferencovane uchovávať najmä osobné údaje súvisiace s týmito službami.**

4. Vnútroštátny súd nemôže uplatniť ustanovenie vnútroštátneho práva, ktoré ho oprávňuje obmedziť časové účinky vyhlásenia protiprávnosti, ktoré mu prislúcha urobiť podľa tohto práva, vo vzťahu k vnútroštátnej právnej úprave ukladajúcej poskytovateľom elektronických komunikačných služieb – najmä na účely ochrany národnej bezpečnosti a boja proti trestnej činnosti – povinnosť vyžadujúcu všeobecné a nediferencované uchovávanie údajov o prenose dát a polohe, ktoré je nezlučiteľné s článkom 15 ods. 1 smernice 2002/58, zmenenej smernicou 2009/136, v spojení s článkami 7, 8 a 11, ako aj s článkom 52 ods. 1 Charty základných práv. Tento článok 15 ods. 1 vykladaný z hľadiska zásady efektivity vyžaduje, aby vnútroštátny trestný súd v rámci trestného konania vedeného proti osobám podozrivým z trestnej činnosti vylúčil informácie a dôkazy získané prostredníctvom všeobecného a nediferencovaného uchovávania údajov o prenose dát a polohe, ktoré je nezlučiteľné s právom Únie, ak tieto osoby nie sú schopné účinne sa vyjadriť k týmto informáciám a dôkazom, ktoré pochádzajú z oblasti mimo znalostí súdu a ktoré môžu mať podstatný vplyv na posúdenie skutkového stavu.

Podpisy