Zbirka odločb sodne prakse

SKLEPNI PREDLOGI GENERALNEGA PRAVOBRANILCA
MANUELA CAMPOSA SÁNCHEZ-BORDONE,
predstavljeni 15. januarja 2020 [1]

Združeni zadevi C-511/18 in C-512/18

La Quadrature du Net,
French Data Network,
Fédération des fournisseurs d'accès à Internet associatifs,
Igwan.net (C-511/18)
proti
Premier ministre,
Garde des Sceaux, ministre de la Justice,
Ministre de l'Intérieur,
Ministre des Armées

(Predlog za sprejetje predhodne odločbe, ki ga je vložil Conseil d'État (državni svet, Francija))

„Predlog za sprejetje predhodne odločbe – Obdelava osebnih podatkov in varstvo zasebnega življenja v sektorju elektronskih komunikacij – Zaščita nacionalne varnosti in boj proti terorizmu – Direktiva 2002/58/ES – Področje uporabe – Člen 1(3) – Člen 15(3) – Člen 4(2) PEU – Listina Evropske unije o temeljnih pravicah – Členi 6, 7, 8, 11, 47 in 52(1) – Splošna in neselektivna hramba podatkov o povezavi in podatkov, ki omogočajo identifikacijo ustvarjalcev vsebin – Zbiranje podatkov o prometu in lokaciji – Dostop do podatkov“

1. Sodišče je v zadnjih letih v zvezi z hrambo in dostopom do osebnih podatkov izoblikovalo ustaljeno sodno prakso, v okviru katere so bile prelomne zlasti te sodbe:

– sodba z dne 8. aprila 2014, Digital Rights Ireland in drugi [2], v kateri je bila Direktiva 2006/24/ES [3] razglašena za neveljavno, ker je bilo na njeni podlagi omogočeno nesorazmerno poseganje v pravice, priznane s členoma 7 in 8 Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina);

– sodba z dne 21. decembra 2016, Tele2 Sverige in Watson ter drugi [4], v kateri je bil predmet razlage člen 15(1) Direktive 2002/58/ES [5];

– sodba z dne 2. oktobra 2018, Ministerio Fiscal [6], v kateri je bila potrjena razlaga navedene določbe Direktive 2002/58.

1 Jezik izvirnika: španščina.

2 Zadevi C-293/12 in C-594/12, v nadaljevanju: sodba Digital Rights, EU:C:2014:238.

3 Direktiva Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL 2006, L 105, str. 54).

4 Zadevi C-203/15 in C-698/15, v nadaljevanju: sodba Tele2 Sverige in Watson, EU:C:2016:970.

5 Direktiva Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514).

6 Zadeva C-207/16, v nadaljevanju: Ministerio Fiscal, EU:C:2018:788.

2. Te sodbe (zlasti drugonavedena) vzbujajo skrb organov nekaterih držav članic, saj ti menijo, da so zaradi njih ostali brez orodja, ki ga po njihovem mnenju potrebujejo za zaščito nacionalne varnosti ter boj proti kriminaliteti in terorizmu. Nekatere od teh držav članic se zato zavzemajo za preklic ali prilagoditev te sodne prakse.

3. Nekatera sodišča držav članic so to skrb izrazila v štirih predlogih za sprejetje predhodne odločbe [7], v zvezi s katerimi so s tem istim datumom predstavljeni moji sklepni predlogi.

4. V teh štirih zadevah se postavlja predvsem vprašanje uporabe Direktive 2002/58 za dejavnosti, ki so povezane z nacionalno varnostjo in bojem proti terorizmu. Če se navedena direktiva v tem okviru uporabi, bo treba razjasniti, v kolikšnem obsegu lahko države članice omejijo pravice do zasebnosti, ki so z njo varovane. Nazadnje bo treba preučiti, v kolikšnem obsegu so različne nacionalne ureditve (britanska [8], belgijska [9] in francoska [10]) tega področja skladne s pravom Unije, kot ga je razlagalo Sodišče.

I. Pravni okvir

A. Pravo Unije

1. Direktiva 2002/58

5. Člen 1 („Področje in cilj“) določa:

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

[…]

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

6. Člen 3 („Storitve“) določa:

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

7 Poleg dveh tu obravnavanih zadev (C-511/18 in C-512/18) še zadevi C-623/17, Privacy International, in C-520/18, Ordre des barreaux francophones et germanophone in drugi.

8 Zadeva Privacy International, C-623/17.

9 Zadeva Ordre des barreaux francophones et germanophone in drugi, C-520/18.

10 Zadevi La Quadrature du Net in drugi, C-511/18 in C-512/18

7. V odstavku 1 člena 5 („Zaupnost sporočil“) je določeno:

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

8. Člen 6 („Podatki o prometu“) določa:

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

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

9. V odstavku 1 člena 15 („Uporaba nekaterih določb Direktive 95/46/ES[11]“) je določeno:

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

2. Direktiva 2000/31/ES[12]

10. Člen 14 določa:

„1. Države članice zagotovijo, da ponudnik storitve, če se storitev informacijske družbe nanaša na shranjevanje podatkov, ki jih zagotovi prejemnik storitve, ni odgovoren za podatek, ki ga je shranil na zahtevo prejemnika storitve, pod pogojem, da:

[…]

3. Ta člen ne posega v možnost, da sodišče ali upravni organ skladno s pravnimi sistemi držav članic od ponudnika storitve zahteva ustavitev ali preprečitev kršitve, in tudi ne v možnost, da države članice določijo postopke, ki urejajo odstranitev ali onemogočenje dostopa do podatkov.“

11 Direktiva Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 15, str. 355).

12 Direktiva Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 25, str. 399).

11. Člen 15 določa:

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

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

3. Uredba (EU) 2016/679[13]

12. Člen 2 („Področje uporabe“) določa:

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

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

a) v okviru dejavnosti zunaj področja uporabe prava Unije;

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

c) s strani fizične osebe med potekom popolnoma osebne ali domače dejavnosti;

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

[…]“

13. Odstavek 1 člena 23 („Omejitve“) določa:

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

a) državne varnosti;

b) obrambe;

c) javne varnosti;

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

13 Uredba Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL 2016, L 119, str. 1).

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

f) varstva neodvisnosti sodstva in sodnega postopka;

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

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

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

j) uveljavljanja civilnopravnih zahtevkov."

14. Člen 95 („Razmerje z Direktivo 2002/58/ES") določa:

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

B. Nacionalno pravo

1. Code de la sécurité intérieure (zakonik o notranji varnosti)

15. Člen L. 851-1 določa:

„Pod pogoji, določenimi v poglavju 1 naslova II te knjige, je mogoče odobriti, da se od operaterjev elektronskih komunikacij, oseb, navedenih v členu L. 34-1 code des postes et des communications électroniques (zakonik o pošti in elektronskih komunikacijah), in oseb, navedenih v členu 6(I), točki 1 in 2, loi n° 2004-575 […] pour la confiance dans l'économie numérique (zakon št. 2004-575 […] o zaupanju v digitalno gospodarstvo), pridobijo podatki ali dokumenti, ki so bili obdelani ali hranjeni v okviru njihovih mrež ali služb elektronskih komunikacij, vključno s tehničnimi podatki, ki se nanašajo na identifikacijo naročniških številk ali številk za povezavo s službami elektronskih komunikacij, popis vseh naročniških številk ali številk za povezavo zadevne osebe, lokalizacijo uporabljene terminalske opreme ter komunikacije naročnika v zvezi s seznamom številk odhodnih in dohodnih klicev, trajanjem in datumom komunikacij […]."

16. V členih L. 851-2 in L. 851-4 je glede na različne namene in načine urejen upravni dostop v realnem času do tako shranjenih podatkov o povezavi.

17. Na podlagi člena L. 851-2 je izključno zaradi preprečevanja terorizma dovoljeno, da se od teh oseb pridobijo informacije ali dokumenti iz člena L. 851-1. To pridobivanje, ki se nanaša zgolj na eno ali več oseb, ki so predhodno opredeljene kot osebe, ki bi bile lahko povezane s teroristično grožnjo, se izvede v realnem času. Podobno lahko v skladu s členom L. 851-4 istega zakonika operaterji v realnem času prenesejo zgolj tehnične podatke, ki se nanašajo na lokalizacijo terminalske opreme. [14]

14 Predložitveno sodišče navaja, da zaradi teh metod za ponudnike storitev ne nastane obveznost dodatne hrambe, ki presega to, kar je nujno za zaračunavanje in trženje njihovih storitev ter zagotavljanje storitev z dodano vrednostjo.

18. Na podlagi člena L. 851-3 se lahko operaterjem elektronskih komunikacij in izvajalcem tehničnih storitev naloži obveznost, da „na svojih omrežjih izvajajo avtomatizirane obdelave podatkov na podlagi parametrov, navedenih v dovoljenju, pri čemer je cilj teh obdelav odkrivanje povezav, ki lahko pomenijo teroristično grožnjo“. [15]

19. Člen L. 851-5 določa, da se pod določenimi pogoji „lahko dovoli uporaba tehnične naprave, ki omogoča lokalizacijo neke osebe, vozila ali predmeta v realnem času“.

20. V skladu s členom L. 851-6(I) se lahko pod določenimi pogoji „z aparatom ali tehnično napravo iz odstavka 1 člena 226-3 code pénal [(kazenski zakonik)] neposredno zbirajo tehnični podatki o povezavi, ki omogočajo identifikacijo terminalske opreme ali naročniške številke njenega uporabnika, in podatki o lokaciji uporabljene terminalske opreme“.

2. Zakonik o pošti in elektronskih komunikacijah

21. Člen L. 34-1 v različici, v kateri se uporabi za dejansko stanje, določa:

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

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

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

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

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

[…]

15 V skladu z navedbami predložitvenega sodišča je namen te metode, pri kateri se ne izvaja splošna in neselektivna hramba, izključno to, da se v omejenem obdobju izmed vseh podatkov o povezavi, ki jih obdelajo te osebe, zberejo tisti podatki, ki bi bili lahko povezani s tovrstnim hudim kaznivim dejanjem.

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

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

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

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

22. V skladu s členom R. 10-13(I) morajo operaterji za namene preiskovanja, ugotavljanja in pregona kaznivih dejanj hraniti te podatke:

„a) podatke, ki omogočajo identifikacijo uporabnika;

b) podatke o uporabljeni komunikacijski terminalski opremi;

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

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

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

23. V skladu z odstavkom II navedenega člena mora pri dejavnostih telefonije operater poleg tega hraniti podatke, ki omogočajo določitev izvora in lokacije komunikacije.

24. V skladu z odstavkom III tega člena je treba navedene podatke hraniti eno leto od njihove shranitve.

3. Loi n.º 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (zakon št. 2004-575 z dne 21. junija 2004 o zaupanju v digitalno gospodarstvo)

25. Člen 6(II), prvi pododstavek, zakona št. 2004-575 določa, da osebe, katerih dejavnost je zagotavljanje dostopa do javnih spletnih komunikacijskih storitev, in fizične ali pravne osebe, ki za dostop javnosti prek javnih spletnih komunikacijskih storitev zagotavljajo, četudi brezplačno, hrambo vsakršnih signalov, pisnega in slikovnega gradiva, zvokov ali sporočil, ki se pridobijo od naslovnikov teh storitev, „vodijo in hranijo podatke, ki omogočajo identifikacijo vsakogar, ki je prispeval k ustvarjanju vsebine ali ene od vsebin storitev, ki jih navedene osebe ponujajo".

26. Tretji pododstavek člena 6(II) določa, da lahko pravosodni organ od teh oseb zahteva predložitev podatkov iz prvega pododstavka.

27. Zadnji pododstavek člena 6(II) določa, da se z odlokom Conseil d'État (državni svet) „opredelijo podatki iz prvega pododstavka ter določijo trajanje in podrobna pravila o njihovi hrambi“.[16]

II. Dejansko stanje in vprašanja za predhodno odločanje

A. Zadeva C-511/18

28. Organizacije Quadrature du Net, French Data Network, Igwan.net in Fédération des fournisseurs d'accès à internet associatifs (v nadaljevanju: tožeče stranke) so pri Conseil d'État (državni svet) vložile tožbo, s katero so predlagale, naj se za nične razglasi več odlokov za izvajanje nekaterih določb zakonika o notranji varnosti.[17]

29. Tožeče stranke trdijo – če povzamem – da so izpodbijani odloki in zadevne določbe zakonika o notranji varnosti v nasprotju s pravicami do spoštovanja zasebnega življenja, varstva osebnih podatkov in učinkovitega pravnega sredstva, ki so zagotovljene s členi 7, 8 oziroma 47 Listine.

30. Conseil d'État (državni svet) je v teh okoliščinah Sodišču predložil ta vprašanja:

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

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

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

16 Opredelitev je bila izvedena z décret n.° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (odlok št. 2011-219 z dne 25. februarja 2011 o hrambi in predložitvi podatkov, ki omogočajo identifikacijo katere koli osebe, ki je prispevala k ustvarjanju vsebine, naložene v splet). Iz tega odloka je mogoče izpostaviti te določbe: (a) člen 1(1), v skladu s katerim morajo osebe, ki zagotavljajo dostop do spletnih komunikacijskih storitev, hraniti te podatke: identifikator povezave, identifikator, dodeljen naročniku, identifikator terminala, uporabljenega za povezavo, datum in čas začetka in konca povezave, značilnosti naročnikove linije; (b) na podlagi člena 1(2) morajo osebe, ki za dostop javnosti prek javnih spletnih komunikacijskih storitev zagotavljajo, četudi brezplačno, hrambo vsakršnih signalov, pisnega in slikovnega gradiva, zvokov ali sporočil, ki se pridobijo od naslovnikov teh storitev, v zvezi z vsako operacijo hraniti te podatke: identifikator povezave, s katero je bila komunikacija začeta, identifikator, dodeljen vsebini, ki je predmet operacije, vrste protokolov, uporabljenih za povezavo s storitvijo in za prenos podatkov, značaj operacije, datum in čas operacije, identifikator, ki ga je uporabil izvajalec operacije; in (c) člen 1(3) določa, da morajo osebe iz predhodnih dveh odstavkov hraniti te podatke, ki jih uporabnik posreduje ob podpisu pogodbe ali ustvaritvi računa: identifikator povezave ob ustvaritvi računa; ime, priimki ali ime družbe; povezani poštni naslovi; uporabljeni psevdonimi; naslovi povezane elektronske pošte ali povezanega računa; telefonske številke; posodobljeno geslo in podatki, ki omogočajo njegovo pridobitev ali spremembo.

17 Izpodbijani so bili ti odloki: (a) décret n.° 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (odlok št. 2015-1185 z dne 28. septembra 2015 o določitvi specializiranih obveščevalnih služb); (b) décret n.° 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (odlok št. 2015-1211 z dne 1. oktobra 2015 o pravnih sredstvih v zvezi z uporabo obveščevalnih metod, za katere je potrebno pridobiti dovoljenje, in datotek, ki zadevajo državno varnost); (c) décret n.° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure (odlok št. 2015-1639 z dne 11. decembra 2015 o določitvi služb, ki niso specializirane obveščevalne službe in ki so pooblaščene za uporabo metod, navedenih v naslovu V knjige VIII zakonika o notranji varnosti); in (d) décret n.° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (odlok št. 2016-67 z dne 29. januarja 2016 o metodah zbiranja podatkov).

B. Zadeva C-512/18

31. Tožeče stranke v sporu, ki je podlaga za zadevo C-511/18, razen organizacije Igwan.net, so Conseil d'État (državni svet) prav tako predlagale, naj razveljavi zavrnitev (zaradi molka upravnega organa) njihove zahteve za razveljavitev člena R. 10-13 code des postes et des communications électroniques (zakonik o pošti in elektronskih komunikacijah) in odloka št. 2011-219 z dne 25. februarja 2011.

32. Te tožeče stranke menijo, da se z izpodbijanimi določbami določa obveznost hrambe podatkov o prometu, lokaciji in povezavi, ki zaradi svoje splošnosti pomeni nesorazmeren poseg v pravice do spoštovanja zasebnega in družinskega življenja, varstva osebnih podatkov in svobode izražanja, ki so varovane s členi 7, 8 in 11 Listine, ter kršitev člena 15(1) Direktive 2002/58.

33. V okviru te zadeve je Conseil d'État (državni svet) predložil ti vprašanji za predhodno odločanje:

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

2. Ali je treba določbe Direktive [2000/13] ob upoštevanju členov 6, 7, 8 in 11 ter 52(1) Listine […] razlagati tako, da državi članici omogočajo, da sprejme nacionalno ureditev, ki osebam, katerih dejavnost je zagotavljanje dostopa do javnih spletnih komunikacijskih storitev, in fizičnim ali pravnim osebam, ki za dostop javnosti prek javnih spletnih komunikacijskih storitev zagotavljajo, četudi brezplačno, hrambo vsakršnih signalov, pisnega in slikovnega gradiva, zvokov ali sporočil, ki se pridobijo od naslovnikov teh storitev, nalaga hrambo podatkov, ki omogočajo identifikacijo vsakogar, ki je prispeval k ustvarjanju vsebine ali ene od vsebin storitev, ki jih navedene osebe ponujajo, da bi lahko pravosodni organ po potrebi zahteval predložitev teh podatkov za dosego spoštovanja pravil v zvezi s civilno ali kazensko odgovornostjo?“

III. Postopek pred Sodiščem in stališča strank

34. Sodno tajništvo Sodišča je vprašanja za predhodno odločanje prejelo 3. avgusta 2018.

35. Pisna stališča so predložile organizacije La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs in French Data Network ter nemška, belgijska, britanska, češka, ciprska, danska, španska, estonska, francoska, madžarska, irska, poljska in švedska vlada ter Komisija.

36. Obravnava je bila opravljena 9. septembra 2019, in sicer skupaj z obravnavama v zadevah C-623/17, Privacy International, in C-520/18, Ordre des barreaux francophones et germanophone in drugi; udeležile so se je stranke štirih postopkov za sprejetje predhodne odločbe, zgoraj navedene vlade in vladi Nizozemske in Norveške ter Komisija in Evropski nadzornik za varstvo podatkov.

IV. Analiza

37. Vprašanja Conseil d'État (državni svet) je mogoče preoblikovati v tri vprašanja:

– Prvič, ali je s pravom Unije v skladu nacionalna ureditev, s katero se ponudnikom elektronskih komunikacijskih storitev naloži obveznost splošne in neselektivne hrambe podatkov o povezavi (prvo vprašanje v zadevi C-511/18 in v zadevi C-512/18) ter zlasti podatkov, ki omogočajo identifikacijo ustvarjalcev vsebin, dostop do katerih zagotavljajo ti ponudniki (drugo vprašanje v zadevi C-512/18)?

– Drugič, ali je zakonitost postopkov zbiranja podatkov o povezavi v vsakem primeru pogojena z obveznostjo, da so zadevne osebe o tem obveščene, če se s tem ne ogrozijo preiskave (tretje vprašanje v zadevi C-511/18)?

– Tretjič, ali je zbiranje podatkov o prometu in lokaciji v realnem času brez obveznosti njihove hrambe v skladu – in če da, pod katerimi pogoji – z Direktivo 2002/58 (drugo vprašanje v zadevi C-511/18)?

38. Skratka, treba je ugotoviti, ali je s pravom Unije v skladu nacionalna ureditev, s katero sta ponudnikom elektronskih komunikacijskih storitev naloženi dve vrsti obveznosti, in sicer: (a) na eni strani, *zbiranje* nekaterih podatkov, ne pa tudi njihova hramba; (b) na drugi strani, *hramba* podatkov o povezavi in podatkov, ki omogočajo identifikacijo ustvarjalcev vsebin storitev, ki jih zagotavljajo ti ponudniki.

39. Najprej je treba – prav zaradi okvira [18], v katerem je bila ta nacionalna ureditev sprejeta (torej v okoliščinah, v katerih bi bila lahko ogrožena nacionalna varnost) – razjasniti, ali se uporabi Direktiva 2002/58.

A. Uporaba Direktive 2002/58

40. Predložitvenemu sodišču se ne zdi vprašljivo, da ureditev, ki je predmet spora, spada na področje uporabe Direktive 2002/58. To naj bi po njegovem mnenju izhajalo iz sodne prakse, ki je bila oblikovana v sodbi Tele2 Sverige in Watson in potrjena v sodbi Ministerio Fiscal.

41. Nekatere vlade, ki so se udeležile postopka, pa trdijo, da sporna zakonodaja ne spada na področje uporabe te direktive. V utemeljitev tega stališča poleg drugih argumentov navajajo sodbo z dne 30. maja 2006, Parlament/Svet in Komisija [19].

42. Strinjam se s Conseil d'État (državni svet), da je bilo s sodbo Tele2 Sverige in Watson to vprašanje razjasnjeno ter potrjeno, da se Direktiva 2002/58 načeloma uporabi, če so ponudniki elektronskih storitev na podlagi zakona obvezani hraniti podatke o svojih naročnikih in javnim organom omogočiti dostop do njih. Na to ugotovitev ne vpliva okoliščina, da so te obveznosti ponudnikom naložene iz razlogov nacionalne varnosti.

43. Naj že na tem mestu pojasnim, da je treba v primeru razhajanj med sodbo Tele2 Sverige in Watson ter predhodnimi sodbami primarno upoštevati prvonavedeno, ker je poznejša in je bila potrjena s sodbo Ministerio Fiscal. Vendar menim, da – kot bom skušal pojasniti – razhajanj ni.

1. Sodba Parlament/Svet in Komisija

44. Zadevi, rešeni s sodbo Parlament/Svet in Komisija, sta se nanašali na:

– Sporazum med Evropsko skupnostjo in Združenimi državami Amerike o obdelavi in prenosu podatkov PNR [Passenger Name Records (evidenca podatkov o potnikih)] s strani letalskih prevoznikov organom Združenih držav [20];

18 V „okoliščinah hudega in trajnega ogrožanja nacionalne varnosti ter zlasti teroristične groženje", kot je navedeno v prvem vprašanju iz zadeve C-511/18.

19 Zadevi C-317/04 in C-318/04, v nadaljevanju: sodba Parlament/Svet in Komisija, EU:C:2006:346.

20 Sklep Sveta 2004/496/ES z dne 17. maja 2004 o sklenitvi Sporazuma med Evropsko skupnostjo in Združenimi državami Amerike o obdelavi in prenosu podatkov PNR s strani letalskih prevoznikov uradu za carine in varovanje meja pri ministrstvu Združenih držav za domovinsko varnost (UL 2004, L 183, str. 83, in popravek v UL 2005, L 255, str. 168) (zadeva C-317/04).

– ustreznost varstva osebnih podatkov, vsebovanih v evidenci imen letalskih potnikov, posredovani tem organom.[21]

45. Sodišče je ugotovilo, da pomeni prenos teh podatkov obdelavo, ki se nanaša na javno varnost in dejavnosti države na področju kazenskega prava. Sklep in odločba, ki sta bila sporna, v skladu s členom 3(2), prva alinea, Direktive 95/46 nista bila vključena v njeno področje uporabe.

46. Podatke so sprva zbrale letalske družbe v okviru dejavnosti – prodaja vozovnic – ki spada na področje uporabe prava Unije. Vendar njihova obdelava, kot je bila obravnavana v sporni odločbi, ni „potrebn[a] za opravljanje storitev, ampak se šteje za nujno za zaščito javne varnosti in za namene kazensk[ega] pregon[a]“.[22]

47. Sodišče je torej privzelo teleološki pristop in upoštevalo namen obdelave podatkov: ker je bila namenjena zaščiti nacionalne varnosti, je treba šteti, da je izključena iz področja uporabe Direktive 95/46. Vendar ta cilj ni bil edino in odločilno merilo,[23] zaradi česar je bilo v sodbi poudarjeno, da „spada […] v okvir, ki ga določijo javni organi, in se nanaša na javno varnost“.[24]

48. Iz sodbe Parlament/Svet in Komisija je torej razvidna razlika med izključitveno klavzulo in restriktivnimi oziroma omejitvenimi klavzulami iz Direktive 95/46 (ki so analogne tem iz Direktive 2002/58). Res je sicer, da se vse nanašajo na podobne cilje v splošnem interesu, zaradi česar nastane določena zmeda glede obsega vsake od njih, kot je nekoč opozoril generalni pravobranilec Y. Bot[25].

49. Ta zmeda je verjetno vzrok za stališče, ki ga zagovarjajo države članice, ki se zavzemajo za ugotovitev, da se Direktiva 2002/58 za ta okvir ne uporabi. Menijo, da se interes nacionalne varnosti zagotavlja le z izključitvijo, določeno v členu 1(3) Direktive 2002/58. Vendar je dejstvo, da so uresničevanju tega interesa namenjene tudi omejitve, dovoljene s členom 15(1) te direktive, med katerimi je tudi omejitev v zvezi z nacionalno varnostjo. Ta določba bi bila odveč, če bi vsakršno sklicevanje na nacionalno varnost že zadostovalo za neuporabo Direktive 2002/58.

2. Sodba Tele2 Sverige in Watson

50. Sodišče je v sodbi Tele2 Sverige in Watson obravnavalo vprašanje, ali sta s pravom Unije v skladu nacionalni ureditvi, na podlagi katerih so imeli ponudniki javno dostopnih elektronskih komunikacijskih storitev splošno obveznost hrambe podatkov v zvezi s temi komunikacijami. Primeri, preučeni v navedeni sodbi, so bili po vsebini torej enaki tem, ki so predmet zadevnih predlogov za sprejetje predhodne odločbe.

21 Odločba Komisije 2004/535/ES z dne 14. maja 2004 o ustreznem varstvu osebnih podatkov, vsebovanih v evidenci imen letalskih potnikov, posredovani uradu za carinsko in mejno zaščito Združenih držav Amerike (UL 2004, L 235, str. 11) (zadeva C-318/04).

22 Sodba Parlament/Svet in Komisija, točka 57. V točki 58 je poudarjeno, da posledica „dejstva, da so podatke […] zbrali zasebni subjekti za ekonomske namene in da jih ti prenesejo v tretjo državo,“ ni to, da ta prenos ne pomeni enega od primerov neuporabe Direktive 95/45 iz člena 3(2), prva alinea, te direktive, saj „spada ta prenos v okvir, ki ga določijo javni organi, in se nanaša na javno varnost“.

23 Tako je pozneje poudaril pokojni generalni pravobranilec Y. Bot v sklepnih predlogih, predstavljenih v zadevi Irska/Parlament in Svet (C-301/06, EU:C:2008:558). Navedel je, da sodba Parlament/Svet in Komisija „ne more pomeniti, da je mogoče o vključitvi obdelave osebnih podatkov na področje uporabe sistema za varstvo podatkov, vzpostavljenega z Direktivo 95/46, ali izključitvi take obdelave s področja uporabe tega sistema odločati samo na podlagi preizkusa namena obdelave zadevnih podatkov. Treba je preveriti tudi, v okviru katere vrste dejavnosti se izvaja obdelava podatkov. Taka obdelava je izključena iz sistema Skupnosti za varstvo osebnih podatkov, ki izhaja iz Direktive 95/46, samo če se izvaja za opravljanje dejavnosti, ki so značilne za države ali državne organe in niso povezane z dejavnostmi posameznikov, in sicer na podlagi člena 3(2), prva alinea, te direktive“ (točka 122).

24 Sodba Parlament/Svet in Komisija, točka 58. Glavni cilj Sporazuma je bil, da se letalskim družbam, ki izvajajo storitve prevoza potnikov med Unijo in Združenimi državami, naloži, da severnoameriškim organom omogočijo elektronski dostop do podatkov PNR iz evidenc imen letalskih potnikov, ki jih hranijo v svojih avtomatiziranih rezervacijskih in odpremnih nadzornih sistemih. Z njim se je torej vzpostavila oblika mednarodnega sodelovanja med Unijo in Združenimi državami zaradi boja proti terorizmu in drugim hudim kaznivim dejanjem, pri čemer se je skušalo ta cilj uskladiti s ciljem varstva osebnih podatkov potnikov. V tem okviru se obveznost, naložena družbam, ni zelo razlikovala od neposredne izmenjave podatkov med javnimi organi.

25 Sklepni predlogi generalnega pravobranilca Y. Bota, predstavljeni v zadevi Irska/Parlament in Svet (C-301/06, EU:C:2008:558, točka 127).

51. Sodišče je ob ponovni obravnavi vprašanja o uporabi prava Unije – tokrat tega iz Direktive 2002/58 – uvodoma navedlo, da „je treba pri presoji obsega področja uporabe Direktive 2002/58 upoštevati predvsem njeno splošno sistematiko“. [26]

52. Sodišče je s tega vidika opozorilo, da se „[z]akonski ukrepi iz člena 15(1) Direktive 2002/58 […] sicer nanašajo na dejavnosti držav ali drugih državnih organov, ki niso povezane s področji dejavnosti posameznikov […]. Poleg tega se nameni, ki jim morajo v skladu s to določbo slediti ti ukrepi, v tem primeru zaščita državne varnosti, […] v bistvenem prekrivajo z nameni, ki jih uresničujejo dejavnosti iz člena 1(3) te direktive“. [27]

53. Namen ukrepov, ki jih lahko v skladu s členom 15(1) Direktive 2002/58 države članice sprejmejo za omejitev pravice do zasebnosti, se torej (v tem delu) prekriva z namenom, na podlagi katerega je mogoče v skladu s členom 1(3) te direktive nekatere dejavnosti države izključiti iz njenega področja uporabe.

54. Vendar je Sodišče menilo, da „glede na splošno sistematiko Direktive 2002/58“ na podlagi te okoliščine „ni mogoče sklepati, da bi bili zakonski ukrepi iz člena 15(1) Direktive 2002/58 izključeni s področja uporabe te direktive, saj bi bil s tem tej določbi odvzet polni učinek. Ta določba namreč nujno predpostavlja, da nacionalni ukrepi, ki so v njej navedeni, […] spadajo na področje uporabe te direktive, ker zadnjenavedena državam članicam izrecno dopušča, da jih sprejmejo le ob upoštevanju pogojev, ki jih določa“. [28]

55. Poleg tega omejitve, dovoljene s členom 15(1) Direktive 2002/58, „za namene, navedene v tej določbi, urejajo dejavnost ponudnikov elektronskih komunikacijskih storitev“. To določbo je treba torej v povezavi s členom 3 te direktive „razlagati tako, da ti zakonski ukrepi spadajo na področje uporabe te direktive“. [29]

56. Sodišče je zato presodilo, da na področje uporabe Direktive 2002/58 spadata tako zakonski ukrep, s katerim je ponudnikom naložena obveznost, „da hranijo podatke o prometu in podatke o lokaciji, saj takšna dejavnost nujno zahteva, da ti ponudniki obdelajo osebne podatke“, [30] kot zakonski ukrep, s katerim je urejen dostop nacionalnih organov do podatkov, ki jih hranijo ti ponudniki. [31]

57. Sodišče je razlago Direktive 2002/58, ki jo je opravilo v sodbi Tele2 Sverige in Watson, potrdilo v sodbi Ministerio Fiscal.

58. Ali je mogoče reči, da pomeni sodba Tele2 Sverige in Watson v razmerju do sodbe Parlament/Svet in Komisija – bolj ali manj impliciten – obrat v sodni praksi? Tako sodi – na primer – vlada Irske, po mnenju katere je le zadnjenavedena sodba v skladu s pravno podlago Direktive 2002/58 in členom 4(2) PEU. [32]

26 Sodba Tele2 Sverige in Watson, točka 67.

27 Prav tam, točka 72.

28 Prav tam, točka 73.

29 Prav tam, točka 74.

30 Prav tam, točka 75.

31 Prav tam, točka 76.

32 Točki 15 in 16 pisnega stališča irske vlade.

59. Francoska vlada pa meni, da bi bilo to protislovje mogoče preseči, če se upošteva, da se sodna praksa iz sodbe Tele2 Sverige in Watson nanaša na dejavnosti držav članic na področju kazenskega prava, medtem ko je sodna praksa, oblikovana v sodbi Parlament/Svet in Komisija, povezana z državno varnostjo in obrambo. Tako naj se sodna praksa iz sodbe Tele2 Sverige in Watson ne bi uporabila za obravnavano zadevo, v kateri bi se bilo treba opreti na rešitev, sprejeto v sodbi Parlament/Svet in Komisija. [33]

60. Kot sem že navedel, menim, da je obe sodbi mogoče uskladiti s pristopom, ki se razlikuje od tega, ki ga predlaga francoska vlada. Z njenim pristopom se ne strinjam, saj je po mojem mnenju mogoče preudarke iz sodbe Tele2 Sverige in Watson, ki se izrecno nanašajo na boj proti terorizmu, [34] razširiti na kakršno koli drugo grožnjo nacionalni varnosti (ena od katerih je terorizem).

3. Možnost usklajene razlage sodbe Parlament/Svet in Komisija ter sodbe Tele2 Sverige in Watson

61. Menim, da je Sodišče v sodbah Tele2 Sverige in Watson ter Ministerio Fiscal upoštevalo smisel obstoja izključitvene in omejitvene klavzule ter sistematsko razmerje med tema vrstama klavzul.

62. Razlog za ugotovitev Sodišča v zadevi Parlament/Svet in Komisija, da obdelava podatkov ni zajeta s področjem uporabe Direktive 95/46, je bil, kot sem že spomnil, v tem, da je v okviru sodelovanja med Evropsko unijo in Združenimi državami, torej v tipično mednarodnem okviru, državna razsežnost dejavnosti morala prevladati nad dejstvom, da je imela ta obravnava tudi tržno ali zasebno razsežnost. Eno od vprašanj, ki so bila v navedeni zadevi obravnavana, je bilo ravno vprašanje ustrezne pravne podlage za sporno odločbo.

63. Sodišče je v zvezi z nacionalnimi ukrepi, ki jih je preučilo v sodbah Tele2 Sverige in Watson ter Ministerio Fiscal, v ospredje postavilo notranji obseg obdelave podatkov: pravni okvir, v katerem se je ta izvajala, je bil izključno nacionalen, zunanje razsežnosti, ki je bila značilna za predmet sodbe Parlament/Svet in Komisija, torej ni bilo.

64. Posledica različnega pomena mednarodne in notranje (trgovske in zasebne) razsežnosti obdelave podatkov je bila, da je v prvem primeru klavzula o izključitvi iz področja prava Unije prevladala kot najprimernejša za varstvo splošnega interesa, ki je bil nacionalna varnost. V drugem primeru pa je bilo mogoče temu interesu učinkovito zadostiti z omejitveno klavzulo iz člena 15(1) Direktive 2002/58.

65. Razvidno je še drugo razhajanje, povezano z drugačnim okvirom urejanja: Sodišče se je pri vsaki od obeh sodb osredotočilo na razlago ene od dveh določb, ki sta sicer podobno formulirani, vendar nista enaki.

66. Tako se je v sodbi Parlament/Svet in Komisija opredelilo o razlagi člena 3(2) Direktive 95/46, v sodbi Tele2 Sverige in Watson pa o členu 1(3) Direktive 2002/58. Iz podrobne preučitve teh določb je razvidna razlika, na podlagi katere je mogoče pojasniti, zakaj je Sodišče v enem primeru odločilo tako in v drugem drugače.

67. V skladu s členom 3(2) Direktive 95/46 se „[t]a direktiva […] *ne uporablja za obdelavo osebnih podatkov* […] med dejavnostjo, ki ne sodi na področje uporabe zakonodaje Skupnosti, […] in v vsakem primeru v postopkih *obdelave* v zvezi z javno varnostjo, obrambo, državno varnostjo (vključno z gospodarsko blaginjo države, kadar se postopek *obdelave* nanaša na zadeve državne varnosti) in pri dejavnostih države na področju kazenskega prava“. [35]

33 Točke od 34 do 50 pisnega stališča francoske vlade.

34 Sodba Tele2 Sverige in Watson, točke od 103 do 119.

35 Moj poudarek.

68. V skladu s členom 1(3) Direktive 2002/58 pa se ta „*ne uporablja za dejavnosti*, ki so zunaj obsega Pogodbe o ustanovitvi Evropske skupnosti, […] in v vsakem primeru *za dejavnosti* v zvezi z javno varnostjo, obrambo, državno varnostjo (vključno gospodarsko blaginjo države, kadar se *dejavnosti* nanašajo na zadeve v zvezi z državno varnostjo) ter dejavnosti države na področju kazenskega prava“. [36]

69. Medtem ko je s členom 3(2) Direktive 95/46 iz njenega področja uporabe izključena *obdelava podatkov*, katere predmet je – kar je pomembno v tem okviru – državna varnost, so s členom 1(3) Direktive 2002/58 izključene *dejavnosti*, namenjene zaščiti – kar je upoštevno v obravnavanem okviru – državne varnosti.

70. Razlika ni zanemarljiva. V Direktivi 95/46 je bila iz področja njene uporabe izključena dejavnost („obdelava osebnih podatkov“), ki jo lahko izvaja kdor koli. Iz te dejavnosti so bile izrecno izvzete obdelave, katerih namen je bil med drugim državna varnost. Ni pa bil pomemben značaj *subjekta*, ki je izvajal obdelavo podatkov. Pristop, uporabljen za opredelitev izključenih dejanj, je bil torej teleološki oziroma tak, pri katerem se upošteva njihov namen, to, kdo jih je izvedel, pa ne.

71. V zadevi Parlament/Svet in Komisija je Sodišče torej primarno upoštevalo namen, ki se uresničuje z obdelavo podatkov. „[D]ejstv[o], da so podatke […] zbrali zasebni subjekti za ekonomske namene in da jih ti prenesejo v tretjo državo“, ni bilo upoštevno, ker je bilo bistveno to, da „spada ta prenos v okvir, ki ga določijo javni organi, in se nanaša na javno varnost“. [37]

72. „Dejavnosti, katerih predmet je državna varnost“, ki niso zajete s področjem uporabe Direktive 2002/58, preučenim v zadevi Tele2 Sverige in Watson, pa ne more izvajati kateri koli subjekt, ampak le država sama. Poleg tega pri njih ne gre za izvajanje normativnih ali regulativnih funkcij države, temveč izključno za dejansko ukrepanje javnih oblasti.

73. *Dejavnosti* iz člena 1(3) Direktive 2002/58 so namreč „vedno dejavnosti držav ali drugih državnih organov, ki niso povezane s področji dejavnosti posameznikov“. [38] Vendar te „dejavnosti“ ne morejo biti normativne. Če bi bilo tako, bi bile vse določbe, ki jih države članice sprejmejo v zvezi z obdelavo osebnih podatkov, iz področja uporabe Direktive 2002/58 izključene že, če bi se skušale upravičiti s tem, da so potrebne za zagotovitev državne varnosti.

74. Po eni strani bi to pomenilo precejšnjo okrnitev polnega učinka te direktive, saj bi že zgolj sklicevanje na tako nedoločen pravni pojem, kot je nacionalna varnost, zadostovalo za to, da v razmerju do držav članic ne bi obvezovala jamstva, ki jih je zakonodajalec Unije zasnoval za varstvo osebnih podatkov državljanov. Te zaščite brez pomoči držav članic ni mogoče vzpostaviti, državljanom pa je zagotovljena tudi v razmerju do nacionalnih javnih oblasti.

75. Po drugi strani bi bil v primeru take razlage pojma „dejavnosti države“, da mednje spadajo tudi te, pri katerih gre za sprejemanje pravnih pravil in določb, izničen smisel člena 15 Direktive 2002/58, na podlagi katerega lahko ravno države članice – zaradi, med drugim, zaščite nacionalne varnosti – sprejmejo „zakonske ukrepe“ za omejitev obsega nekaterih pravic in obveznosti, določenih s to direktivo. [39]

36 Moj poudarek.

37 Parlament/Svet in Komisija, točka 58.

38 Sodba Ministerio Fiscal, točka 32. V istem smislu sodba Teje2 Sverige in Watson, točka 72..

39 Težko bi bilo namreč trditi, da je na podlagi člena 15(1) Direktive 2002/58 omejitev določenih pravic in obveznosti, ki je v njem urejena, mogoča na področju, ki je – kot državna varnost – na podlagi člena 1(3) te direktive načeloma zunaj njenega področja uporabe. Kot je Sodišče ugotovilo v točki 73 sodbe Tele2 Sverige in Watson, člen 15(1) Direktive 2002/58 „nujno predpostavlja, da nacionalni ukrepi, ki so v njej navedeni, […] spadajo na področje uporabe te direktive, ker zadnjenavedena državam članicam izrecno dopušča, da jih sprejmejo le ob upoštevanju pogojev, ki jih določa“.

76. Kot je Sodišče poudarilo v zadevi Tele2 Sverige in Watson, „je treba pri presoji obsega področja uporabe Direktive 2002/58 upoštevati predvsem njeno splošno sistematiko“.[40] S tega vidika je razlaga členov 1(3) in 15(1) Direktive 2002/58, s katero se ti določbi osmislita, ne da bi bil okrnjen njun učinek, ta, v skladu s katero je v prvonavedeni določbi opredeljena vsebinska izjema, ki se nanaša na *dejavnosti*, ki jih države članice opravljajo na področju nacionalne varnosti (in enakovrednih področjih), v drugonavedeni določbi pa pooblastilo za sprejemanje *zakonskih ukrepov* (torej splošno obvezujočih pravil), s katerimi se v interesu nacionalne varnosti posega v dejavnosti posameznikov, nad katerimi lahko države članice izvajajo javno oblast, in omejijo pravice, zagotovljene z Direktivo 2002/58.

4. Izključitev na podlagi nacionalne varnosti v Direktivi 2002/58

77. Nacionalna varnost (ali njen sinonim „državna varnost“, uporabljen v členu 15(1) Direktive 2002/58) je v tej direktivi upoštevana z dveh vidikov. Po eni strani je razlog za *izključitev* (iz področja uporabe te direktive) vseh teh dejavnosti držav članic, ki so konkretno z njo „v zvezi“. Po drugi strani pa pomeni razlog za *omejitev* – ki mora biti opredeljena z zakonom – pravic in obveznosti, določenih z Direktivo 2002/58, torej teh, ki se nanašajo na zasebne ali poslovne dejavnosti, ki niso povezane z oblastnimi dejavnostmi.[41]

78. Na katere dejavnosti se nanaša člen 1(3) Direktive 2002/58? Menim, da je sam Conseil d'État (državni svet) podal dober primer s tem, da je omenil določbe členov L. 851-5 in L. 851-6 zakonika o notranji varnosti, pri čemer se je skliceval na „metode pridobivanja informacij, ki jih neposredno izvaja država, ne da bi urejale dejavnosti ponudnikov elektronskih komunikacijskih storitev in jim nalagale posebne obveznosti“.[42]

79. Menim, da je v tem ključ za določitev obsega izključitve iz člena 1(3) Direktive 2002/58. Ureditev iz te direktive se ne uporablja za *dejavnosti*, ki so namenjene zaščiti nacionalne varnosti in jih javne oblasti izvajajo v svojem imenu, ne da bi pri tem zahtevale sodelovanje zasebnikov, ki jim torej ne naložijo obveznosti pri poslovnem upravljanju.

80. Vendar je treba seznam dejavnosti javnih oblasti, ki so izvzete iz splošne ureditve o obdelavi osebnih podatkov, razlagati ozko. Konkretno, pojma *nacionalne varnosti*, ki je v skladu s členom 4(2) PEU v izključni pristojnosti vsake države članice, ni mogoče razširiti na druge, bolj ali manj sorodne sektorje javnega življenja.

81. Ker je v okviru teh vprašanj za predhodno odločanje podana udeležba zasebnikov (torej subjektov, ki za uporabnike izvajajo elektronske komunikacijske storitve), in ne zgolj delovanje državnih organov, ni treba podrobno razpravljati o opredelitvi okvira nacionalne varnosti *stricto sensu*.

40 Sodba Tele2 Sverige in Watson, točka 67.

41 Kot je mimogrede navedel generalni pravobranilec H. Saugmandsgaard Øe v sklepnih predlogih v zadevi Ministerio Fiscal (C-207/16, EU:C:2018:300, točka 47), „se ne sme zamenjevati na eni strani osebnih podatkov, ki se obdelujejo *neposredno* v okviru oblastnih dejavnosti države na področju kazenskega prava, in na drugi strani osebnih podatkov, ki se obdelujejo v okviru poslovnih dejavnosti ponudnika elektronskih komunikacijskih storitev in ki jih *nato* uporabijo pristojni državni organi“.

42 Točki 18 in 21 predložitvenega sklepa v zadevi C-511/18.

82. Vendar menim, da bi bilo kot smernica v zvezi s tem lahko koristno merilo iz Okvirnega sklepa 2006/960/PNZ[43], v členu 2(a) katerega se razlikuje med organi kazenskega pregona v širšem pomenu – ki vključujejo „državno policijo, carino ali drug organ, ki mu nacionalna zakonodaja daje pooblastila za odkrivanje, preprečevanje in preiskovanje kaznivih dejanj ali kriminalnih dejavnosti ter za izvajanje pooblastil in uporabo prisilnih ukrepov v okviru takšnih dejavnosti“ – na eni strani ter „[a]gencij[ami] ali enot[ami], ki se ukvarjajo posebej z vprašanji državne varnosti“, na drugi.[44]

83. V uvodni izjavi 11 Direktive 2002/58 je navedeno, da ta, „tako kot Direktiva 95/46/ES, ne obravnava vprašanj varstva temeljnih pravic in svoboščin, povezanih z dejavnostmi, ki jih ne ureja pravni red [Unije]“. Direktiva 2002/58 tako „ne spreminja obstoječega ravnotežja med posameznikovo pravico do zasebnosti in možnostjo držav članic, da sprejmejo ukrepe iz člena 15(1) te direktive, potrebne za zaščito […] državne varnosti“.

84. Glede pristojnosti držav članic v zvezi z nacionalno varnostjo je med Direktivo 95/46 in Direktivo 2002/58 namreč kontinuiteta. Nobena se ne nanaša na varstvo temeljnih pravic na tem konkretnem področju, na katerem dejavnosti držav članic „ne ureja pravni red [Unije]“.

85. „Ravnotežje“, omenjeno v tej uvodni izjavi, izhaja iz zahteve po spoštovanju pristojnosti držav članic na področju nacionalne varnosti, kadar jih te izvajajo *neposredno* in *z lastnimi sredstvi*. Okoliščina, da se – pa čeprav zaradi razlogov nacionalne varnosti – zahteva sodelovanje zasebnikov, ki se jim naložijo določene obveznosti, je podlaga za uvrstitev na področje (varstvo zasebnosti, ki ga morajo spoštovati ti zasebni subjekti), ki je urejeno s pravom Unije.

86. V direktivah 95/46 in 2002/58 se skuša to ravnotežje doseči z določitvijo, da se lahko pravice zasebnikov omejijo na podlagi zakonskih ukrepov, ki jih države sprejmejo na podlagi členov 13 (1) oziroma 15(1) omenjenih direktiv. Glede tega med njima ni nobenih razlik.

87. V Uredbi 2016/679, s katero je določen (nov) splošni okvir za varstvo osebnih podatkov, pa je s členom 2(2) njena uporaba izključena za „obdelavo osebnih podatkov“ s strani držav članic, kadar te „izvajajo dejavnosti, ki spadajo na področje uporabe poglavja 2 naslova V PEU“.

88. Medtem ko je bila v Direktivi 95/46 obdelava osebnih podatkov opredeljena le na podlagi njenega namena, ne glede na subjekt, ki jo izvaja, pa so v Uredbi 2016/679 obdelave, izključene iz njenega področja uporabe, opredeljene tako glede na njihov namen kot glede na subjekte, ki jih izvajajo: izvzete so obdelave, ki jih države članice izvajajo v okviru *dejavnosti* zunaj področja uporabe prava Unije (člen 2(2)(a) in (b)), in te, ki jih organi izvajajo *za namene preprečevanja kaznivih dejanj in varovanja* pred grožnjami javni varnosti.[45]

89. Opredelitev teh dejavnosti, ki jih opravlja javna oblast, mora biti ozka, saj se sicer okrni polni učinek prava Unije na področju varstva zasebnosti. V členu 23 Uredbe 2016/679 je – podobno kot v členu 15(1) Direktive 2002/58 – določena možnost, da se *z zakonodajnimi ukrepi* omejijo pravice in obveznosti, ki jih ta uredba določa, če je to potrebno za zagotavljanje, med drugim, državne varnosti, obrambe ali javne varnosti. In spet: če bi varstvo teh ciljev zadostovalo za izključitev iz področja uporabe Uredbe 2016/679, potem bi bila odveč določitev, da je na podlagi državne varnosti mogoče upravičiti to, da se z zakonodajnimi ukrepi omejijo pravice, zagotovljene s to uredbo.

43 Okvirni sklep Sveta z dne 18. decembra 2006 o poenostavitvi izmenjave informacij in obveščevalnih podatkov med organi kazenskega pregona držav članic Evropske unije (UL 10 L 386, str. 89).

44 V enakem smislu je člen 1(4) Okvirnega sklepa Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah (UL 2008, L 350, str. 60) določal, da ta okvirni sklep „ne posega v bistvene interese nacionalne varnosti in posebne obveščevalne dejavnosti na področju državne varnosti“.

45 Z Uredbo 2016/679 je namreč iz njenega področja uporabe poleg obdelave, ki jo organi izvajajo *za namene varovanja* javne varnosti, izključena obdelava podatkov, ki jo države članice izvedejo pri opravljanju *dejavnosti*, ki ne spada na področje uporabe prava Unije.

90. Enako kot v primeru Direktive 2002/58 ne bi bilo koherentno, da bi bili zakonodajni ukrepi iz člena 23 Uredbe 2016/679 (v skladu s katerim, ponavljam, lahko država iz razlogov državne varnosti določi omejitve pravic državljanov do zasebnosti) zajeti s področjem uporabe te uredbe, obenem pa bi bila lahko na podlagi sklicevanja na državno varnost brez nadaljnjega izključena uporaba same Uredbe, kar bi pomenilo, da z njo pravzaprav ni priznana nobena subjektivna pravica.

B. Potrditev in možnosti za izpopolnitev sodne prakse Tele2 Sverige in Watson

91. V sklepnih predlogih v zadevi C-520/18 sem opravil podrobno analizo [46] sodne prakse Sodišča na tem področju, na podlagi katere sem se zavzel za njeno potrditev, obenem pa predlagal razlagalni pristop za podrobnejši oris njene vsebine.

92. Napotujem torej na to analizo, ki se mi je v teh sklepnih predlogih že zaradi ekonomičnosti ne zdi nujno ponavljati. Spodnje preudarke v zvezi z vprašanji za predhodno odločanje, ki jih je predložil Conseil d'Etat (državni svet), je treba torej brati ob upoštevanju ustreznih odlomkov iz sklepnih predlogov v zadevi C-520/18.

C. Odgovor na vprašanja za predhodno odločanje

1. Obveznost hrambe podatkov (prvo vprašanje za predhodno odločanje v zadevah C-511/18 in C-512/18 ter drugo vprašanje za predhodno odločanje v zadevi C-512/18)

93. Predložitveno sodišče želi v zvezi z obveznostjo hrambe podatkov, ki je naložena ponudnikom elektronskih komunikacijskih storitev, izvedeti zlasti:

– ali ta obveznost, ki se lahko določi na podlagi člena 15(1) Direktive 2002/58, pomeni poseg, ki je utemeljen s „pravico do varnosti“, zagotovljeno s členom 6 Listine, in zahtevami nacionalne varnosti (prvo vprašanje v zadevah C-511/18 in C-512/18 ter tretje vprašanje v zadevi C-511/18);

– ali je v skladu z Direktivo 2000/31 dopustna hramba podatkov, na podlagi katerih je mogoča identifikacija oseb, ki so prispevale k ustvarjanju vsebin, ki so javno dostopne na spletu (drugo vprašanje v zadevi C-512/18).

a) Uvodni preudarek

94. Conseil d'État (državni svet) se sklicuje na temeljne pravice iz členov 7 (spoštovanje zasebnega in družinskega življenja), 8 (varstvo osebnih podatkov) in 11 (svoboda izražanja in obveščanja) Listine. To so namreč pravice, do posega v katere lahko po mnenju Sodišča pride zaradi obveznosti hrambe podatkov o prometu, ki jo nacionalni organi naložijo ponudnikom elektronskih komunikacijskih storitev. [47]

95. Predložitveno sodišče prav tako omenja pravico do varnosti, zagotovljeno s členom 6 Listine. Navaja jo predvsem kot dejavnik, s katerim bi bilo mogoče upravičiti naložitev te obveznosti, in ne toliko kot pravico, do posega v katero je morda prišlo.

46 Točke od 27 do 68.

47 Tako sodba Tele2 Sverige in Watson (točka 92), v kateri je po analogiji navedena sodba Digital Rights (točki 25 in 70).

96. Strinjam se s Komisijo, da je takšno sklicevanje na člen 6 Listine lahko zavajajoče. Podobno kot Komisija menim, da se ta določba ne sme razlagati tako, da se lahko na njeni podlagi „Uniji naloži pozitivna obveznost sprejetja ukrepov za varstvo oseb pred kaznivimi dejanji“. [48]

97. Pri varnosti, ki je zagotovljena s tem členom Listine, ne gre za javno varnost. Oziroma – z drugimi besedami – z njo je povezana toliko kot katera koli druga temeljna pravica, saj je javna varnost nujni pogoj za uživanje temeljnih pravic in svoboščin.

98. Kakor opozarja Komisija, člen 6 Listine ustreza – kot izhaja iz pripadajočih pojasnil – členu 5 Evropske konvencije o varstvu človekovih pravic (v nadaljevanju: EKČP). Iz besedila člena 5 EKČP izhaja, da je „varnost“, ki je z njim zaščitena, izključno osebna varnost, razumljena kot jamstvo pravice do fizične svobode pred samovoljnim pridržanjem ali odvzemom prostosti. Gre torej za varnost, da se nikomur ne sme odvzeti prostost, razen v primerih, pod pogoji in v skladu s postopki, ki so določeni z zakonom.

99. Gre torej za *osebno varnost*, ki se nanaša na pogoje, pod katerimi se lahko omeji fizična prostost oseb [49], in ne *javno varnost*, ki je neločljivo povezana z obstojem države in je v razviti družbi nujna predpostavka za to, da se izvajanje javne oblasti uskladi z uživanjem osebnostnih pravic.

100. Nekatere države pa se zavzemajo za to, da se bolj upošteva zadnjenavedeni smisel pravice do varnosti. Dejstvo je, da ga je Sodišče upoštevalo ter ga je v svojih sodbah [50] in mnenjih [51] celo izrecno omenilo. Nikoli ni zanikalo pomena ciljev v splošnem interesu zaščite nacionalne varnosti in javnega reda [52], boja proti mednarodnemu terorizmu za vzdrževanje mednarodnega miru in varnosti ter boja proti hudim kaznivim dejanjem zaradi zagotavljanja javne varnosti [53], za katerega je pravilno ugotovilo, da je „ključnega pomena“ [54]. Kot je navedlo, „zaščita javne varnosti prispeva k varstvu pravic in svoboščin drugih oseb“. [55]

101. Lahko bi se izkoristila priložnost, ki se ponuja v teh okviru obravnavanih predlogov za sprejetje predhodne odločbe, za oblikovanje jasnejšega pristopa k iskanju ravnotežja med pravico do varnosti na eni strani ter pravicama do zasebnosti in do varstva osebnih podatkov na drugi. Tako bi se odvrnile kritike, da se drugonavedenima daje prednost pred prvonavedeno.

102. Na to ravnotežje se po mojem mnenju napotuje v uvodni izjavi 11 in členu 15(1) Direktive 2002/58, ko se navaja, da morajo biti ukrepi potrebni in sorazmerni *v demokratični družbi*. Pravica do varnosti, poudarjam, je bistvena za obstoj in preživetje demokracije, zaradi česar je upravičeno, da se ta pravica v okviru presoje te sorazmernosti v celoti upošteva. Z drugimi besedami, čeprav je ohranitev načela zaupnosti podatkov ključnega pomena v demokratični družbi, pa se prav tako ne sme podcenjevati pomembnost njene varnosti.

103. Okoliščine hudih in trajajočih groženj za nacionalno varnost in zlasti tveganje terorizma je – kot je bilo ugotovljeno v zadnjem stavku točke 119 sodbe Tele2 Sverige in Watson – torej treba upoštevati. Nacionalni sistem se lahko sorazmerno glede na njihovo naravo in intenzivnost odzove na grožnje, s katerimi se sooča, pri čemer ni nujno, da je ta odziv enak odzivu drugih držav članic.

48 Točka 37 pisnega stališča Komisije.

49 Tako jo razlaga ESČP. Glej zlasti sodbo z dne 5. julija 2016, Buzadji proti Republiki Moldaviji, ECHR:2016:0705 JUD002375507, v točki 84 katere je ugotovljeno, da je bistveni namen pravice, priznane s členom 5 EKČP, preprečitev samovoljnega ali neupravičenega odvzema prostosti.

50 Sodba Digital Rights, točka 42.

51 Mnenje 1/15 (Sporazum PNR EU-Kanada) z dne 26. julija 2017 (v nadaljevanju: mnenje 1/15) (EU:C:2017:592, točka 149 in navedena sodna praksa).

52 Sodba z dne 15. februarja 2016, N. (C-601/15 PPU, EU:C:2016:84, točka 53).

53 Sodba Digital Rights, točka 42 in navedena sodna praksa.

54 Prav tam, točka 51.

55 Mnenje 1/15, točka 149.

104. Naj dodam, da zgornji razmisleki niso ovira za to, da se v položajih, ki so prav zares *izjemni* in za katere je značilna neposredna nevarnost ali skrajno visoko tveganje, zaradi katerih je upravičena uradna razglasitev izrednih razmer v državi članici, z nacionalno zakonodajo določi možnost, da se za omejeno časovno obdobje naloži obveznost hrambe podatkov, ki je tako široka in splošna, kot je po presoji potrebno.[56]

105. Zato bi bilo treba prvo vprašanje za predhodno odločanje iz obeh obravnavanih zadev preoblikovati tako, da je treba razjasniti, ali je mogoče poseg upravičiti na podlagi razlogov nacionalne varnosti. Dvom bi se torej nanašal na to, ali je obveznost, naložena operaterjem elektronskih komunikacijskih storitev, v skladu s členom 15(1) Direktive 2002/58.

b) Presoja

1) Opredelitev nacionalnih določb, kot so predstavljene v dveh predlogih za sprejetje predhodne odločbe, glede na sodno prakso Sodišča

106. Kot izhaja iz predložitvenih sklepov, zakonodaja, sporna v postopkih v glavni stvari, določa, da morajo podatke hraniti:

– operaterji elektronskih komunikacij in zlasti ti, ki ponujajo dostop do javnih spletnih komunikacijskih storitev, in

– fizične ali pravne osebe, ki za dostop javnosti prek spleta zagotavljajo, četudi brezplačno, hrambo vsakršnih signalov, besedil, zvokov, slik ali sporočil, ki se pridobijo od naslovnikov teh storitev.[57]

107. Gospodarski subjekti morajo eno leto od dneva shranitve hraniti podatke, ki omogočajo identifikacijo uporabnika, podatke o uporabljeni komunikacijski terminalski opremi, tehnične značilnosti, datum, čas in trajanje vsakega klica, podatke o zahtevanih ali uporabljenih dodatnih storitvah in njihovih ponudnikih ter podatke, na podlagi katerih je mogoče identificirati namembnega prejemnika komunikacije ter – pri dejavnostih telefonije – izvor in lokacijo komunikacije.[58]

108. Zdi se, da se z nacionalno zakonodajo posebej v zvezi s storitvami dostopa do interneta in storitvami gostovanja zahteva hramba IP naslovov,[59] gesel za dostop in – v primeru podpisa pogodbe ali odprtja plačilnega računa – podatkov o vrsti izvedenega plačila ter sklicu, znesku, datumu in času transakcije.[60]

109. Ta obveznost hrambe je potrebna zaradi preiskovanja, ugotavljanja in pregona kaznivih dejanj.[61] Namen *hrambe* podatkov o prometu in lokaciji torej – drugače od, kot bo razvidno spodaj, obveznosti *zbiranja* podatkov o prometu in lokaciji – ni le preprečevanje terorizma.[62]

56 Glej točke od 105 do 107 mojih sklepnih predlogov v zadevi C-520/18.

57 Tako izhaja iz člena L. 851-1 zakonika o notranji varnosti, ki napotuje na člen L. 34-1 zakonika o pošti in elektronskih komunikacijah ter člen 6 zakona št. 2004-575 o zaupanju v digitalno gospodarstvo.

58 Tako določa člen R. 10-13 zakonika o pošti in elektronskih komunikacijah.

59 Ta podatek, o katerem so bila na obravnavi izražena razhajajoča se mnenja, mora preveriti predložitveno sodišče.

60 Člen 1 odloka št. 2011-219.

61 Člen R. 10-13 zakonika o pošti in elektronskih komunikacijah.

62 Organizaciji Quadrature du Net in Fédération des founisseurs d'accès á Internet associatifs poudarjata širokost okvira namenov hrambe, polje proste presoje, priznano organom, neobstoj objektivnih meril za njegovo opredelitev in pomen, pripisan oblikam kriminalitete, ki jih ni mogoče šteti za hude.

110. Iz podatkov iz spisa izhaja, da je *dostop* do podatkov, ki se hranijo, omogočen bodisi pod pogoji, ki veljajo v splošni ureditvi (posredovanje pravosodnega organa), bodisi le agentom, ki so posebej imenovani in pooblaščeni na podlagi dovoljenja, ki ga predsednik vlade izda na podlagi nezavezujočega mnenja neodvisnega upravnega organa [63].

111. Hitro je mogoče ugotoviti, kot je poudarila Komisija, [64] da so podatki, katerih hramba se zahteva v skladu z nacionalnimi določbami, v bistvu enaki tem, ki jih je Sodišče preučilo v sodbah Digital Rights ter Tele2 Sverige in Watson. [65] Kakor v omenjenih sodbah so ti podatki predmet „obveznosti splošne in neselektivne hrambe“, kot v začetku svojih vprašanj za predhodno odločanje povsem odkrito poudarja Conseil d'État (državni svet).

112. Če je tako, kar mora nazadnje presoditi predložitveno sodišče, je treba ugotoviti, da zadevna ureditev pomeni „[p]oseg [v] temeljni pravici, ki jih zagotavljata člena 7 in 8 Listine[, ki] se izkaže za širok in ga je treba obravnavati kot posebno resnega“. [66]

113. Nobena od strank, zastopanih v postopku, ni izrazila dvoma, da pomeni takšna ureditev poseg v te pravice. Tega tu ni treba obravnavati in skoraj odveč je spomniti, da se s posegom v te pravice neizogibno spodkopavajo temelji družbe, ki si prizadeva za spoštovanje – med drugimi vrednotami – zasebnosti, ki je varovana z Listino.

114. Posledica uporabe sodne praske, oblikovane v sodbi Tele2 Sverige in Watson ter potrjene v sodbi Ministerio Fiscal, bi bila seveda ugotovitev, da ureditev, kakršna je obravnavana, „presega meje nujno potrebnega in je torej ni mogoče šteti za upravičeno v demokratični družbi, kot to zahteva člen 15(1) Direktive 2002/58 glede na člene 7, 8, 11 in 52(1) Listine“. [67]

115. Enako kot ureditev, ki je bila obravnavana v sodbi Tele2 Sverige in Watson, tudi ta, ki je predmet preučitve v tej zadevi, „na splošno zajema vse naročnike in registrirane uporabnike in se nanaša na vsa elektronska komunikacijska sredstva in na vse podatke o prometu [ter] ne določa nobenega razlikovanja, omejitve ali izjeme glede na cilj, ki se ga poskuša doseči“. [68] Posledično se „uporablja tudi za osebe, v zvezi s katerimi ni nobenega indica, na podlagi katerega bi bilo mogoče sklepati, da obstaja povezava, čeprav posredna ali daljna, med njihovimi ravnanji in hudimi kaznivimi dejanji“, pri čemer ne dopušča nobene izjeme, „tako da se uporablja tudi za osebe, katerih komunikacije so v skladu z nacionalnimi predpisi poslovna skrivnost“. [69]

116. Tako sporna ureditev „ne zahteva nobene povezave med podatki, za katere se določa hramba, in grožnjo za javno varnost. Predvsem pa ni omejena na hrambo bodisi podatkov v zvezi z začasnim obdobjem in/ali določenim z geografskim območjem in/ali krogom oseb, ki so lahko tako ali drugače vpletene v hudo kaznivo dejanje, bodisi podatkov v zvezi z osebami, ki bi lahko iz drugih razlogov, s tem da bi se hranili njihovi podatki, prispevali k boju proti kriminalu.“ [70]

117. Iz navedenega izhaja, da ta ureditev „presega meje nujno potrebnega in je torej ni mogoče šteti za upravičeno v demokratični družbi, kot to zahteva člen 15(1) Direktive 2002/58 glede na člene 7, 8, 11 in 52(1) Listine“. [71]

63 La Commission nationale de contrôle des techniques de renseignement (nacionalna komisija za nadzor obveščevalnih metod). V zvezi s tem glej točke od 145 do 148 pisnega stališča francoske vlade.

64 Točka 60 pisnega stališča Komisije.

65 Dejansko je zahtevani okvir hrambe nekoliko večji, saj se zdi, da je v njem zajeta – v primeru storitev dostopa do interneta – tudi hramba naslovov IP ali gesel za dostop.

66 Sodba Tele2 Sverige in Watson, točka 100.

67 Prav tam, točka 107.

68 Prav tam, točka 105.

69 Prav tam.

70 Sodba Tele2 Sverige in Watson, točka 106.

71 Prav tam, točka 107.

118. To je zadoščalo, da je Sodišče ugotovilo, da ustrezne nacionalne določbe niso bile v skladu s členom 15(1) Direktive 2002/58, ker so „z namenom boja proti kriminalu določa[le] splošno in neselektivno hrambo vseh podatkov o prometu in podatkov o lokaciji vseh naročnikov in registriranih uporabnikov glede vseh elektronskih komunikacijskih sredstev“. [72]

119. Vprašanje, ki se postavlja zdaj, je, ali se ta sodna praksa Sodišča na področju hrambe osebnih podatkov lahko vsaj prilagodi, če ne že preoblikuje, kadar je namen te „splošne in neselektivne“ hrambe boj proti terorizmu. Prvo vprašanje iz zadeve C-511/18 je oblikovano prav „v okoliščinah hudega in trajnega ogrožanja nacionalne varnosti ter zlasti teroristične grožnje“.

120. Vendar čeprav je to *dejanski okvir*, v katerem se nalaga obveznost hrambe podatkov, pa se *normativni okvir* te hrambe brez dvoma ne nanaša le na terorizem. V okviru ureditve hrambe in dostopa do podatkov, ki je predmet postopka pred Conseil d'État, je ta obveznost določena za namene preiskovanja, ugotavljanja in pregona kaznivih dejanj na splošno.

121. Sicer pa naj spomnim, da Sodišče v obrazložitvi sodbe Tele2 Sverige in Watson boja proti terorizmu ni prezrlo, čeprav je menilo, da v zvezi s to obliko kriminala ni potrebna nobena prilagoditev njegove sodne prakse. [73]

122. Zato načeloma menim, da je treba na vprašanje predložitvenega sodišča, ki se specifično nanaša na posebnost teroristične grožnje, odgovoriti v smislu, v kakršnem je Sodišče odločilo v sodbi Tele2 Sverige in Watson.

123. Kot sem navedel v sklepnih predlogih v zadevi Stichting Brein, „[g]otovost pri uporabi prava od sodišč sicer morda ne zahteva povsem doslednega upoštevanja vodila *stare decisis*, postulira pa pazljivost, da upoštevajo odločitve, ki so jih po tehtnem premisleku sama sprejela o danem pravnem vprašanju.“ [74]

2) Omejena hramba podatkov v primeru obstoja groženj državni varnosti, vključno s terorističnо

124. Toda ali bi bilo to sodno prakso glede na posledice, ki jih ima za boj proti terorizmu ali zaščito države pred drugimi podobnimi grožnjami nacionalni varnosti, mogoče prilagoditi ali dopolniti?

125. Poudaril sem že, da že sama hramba osebnih podatkov pomeni poseg v pravice, zagotovljene s členi 7, 8 in 11 Listine. [75] Ne glede na to, da je njen končni namen to, da se v nekem trenutku [76] omogoči *dostop* do – prej ali prav tedaj zbranih – podatkov, že sama hramba podatkov, ki presegajo te, ki so nujni za prenos sporočila ali zaračunavanje storitev, ki jih izvede ponudnik, pomeni nespoštovanje omejitev iz členov 5 in 6 Direktive 2002/58.

72 Prav tam, točka 112.

73 Prav tam, točka 103.

74 Zadeva C-527/15, EU:C:2016:938, točka 41.

75 Kot je spomnilo Sodišče v točki 124 mnenja 1/15, „gre pri sporočanju osebnih podatkov tretji osebi, kot je javni organ, za poseganje v temeljno pravico iz člena 7 Listine, ne glede na nadaljnjo uporabo sporočenih informacij. Enako velja za hrambo osebnih podatkov in za dostop do navedenih podatkov z namenom, da bi jih uporabljali javni organi. Glede tega ni pomembno, ali so informacije o zasebnem življenju občutljive, niti to, ali so bile zadevne osebe zaradi tega poseganja morda oškodovane.“

76 Kot je navedel generalni pravobranilec P. Cruz Villalón v sklepnih predlogih v zadevi Digital Rights (C-293/12 in C-594/12, EU:C:2013:845, točka 72), „zbiranje in zlasti hramba velikih količin podatkov, ki se ustvarjajo ali obdelujejo med večino vsakodnevnih elektronskih komunikacij državljanov Unije, v ogromnih podatkovnih zbirkah pomenita izrazito poseganje v njihovo zasebno življenje, čeprav se s tem zgolj ustvarjajo pogoji za naknaden nadzor nad njihovim osebnim in poklicnim delovanjem. Z zbiranjem teh podatkov se ustvarjajo pogoji za nadzor, ki čeprav se izvaja šele z naknadno uporabo teh podatkov, vseeno med celotnim obdobjem hrambe teh podatkov trajno ogroža pravico državljanov Unije do tajnosti njihovega zasebnega življenja. Nedoločljiv občutek nadzora, ki ga to povzroča, še posebej izrazito sproža vprašanje obdobja hrambe podatkov.“

126. Uporabniki teh storitev (dejansko skoraj vsi državljani v bolj razvitih družbah) uživajo ali bi morali uživati upravičeno pričakovanje, da se brez njihovega soglasja ne hranijo nobeni drugi njihovi podatki kot ti, ki se hranijo v skladu s tema določbama. Izjeme iz člena 15(1) Direktive 2002/58 je treba razumeti ob upoštevanju te premise.

127. Sodišče je – kot sem že pojasnil – v sodbi Tele2 Sverige in Watson tudi v zvezi z bojem proti terorizmu zavrnilo splošno in neselektivno hrambo osebnih podatkov.[77]

128. V zvezi s kritikami glede sodne prakse iz te sodbe menim, da ta sodna praksa ne podcenjuje teroristične grožnje kot posebej resne oblike kriminala, katere izrecni namen je spodkopavanje avtoritete države in destabilizacija ali uničenje njenih institucij. Boj proti terorizmu je – dobesedno – življenjskega pomena za državo, njegova uspešnost pa cilj v splošnem interesu, ki je nujen za obstoj pravne države.

129. Skoraj vse vlade, ki so se udeležile postopka, in Komisija so opozorile, da bi le ob delni in selektivni hrambi osebnih podatkov – tudi če se odmislijo s to hrambo povezane tehnične težave – nacionalne obveščevalne službe ostale brez možnosti dostopa do informacij, ki so nujne za odkrivanje groženj javni varnosti in obrambo države ter pregon storilcev terorističnih napadov.[78]

130. V zvezi s tem stališčem se mi zdi pomembno poudariti, da se pri oblikovanju pristopa k boju proti terorizmu ne sme misliti le na učinkovitost tega boja. To je razlog za njegovo težavnost, ampak tudi za njegovo dovršenost, če so zanj uporabljena sredstva in metode v skladu z zahtevami pravne države, ki pomeni predvsem to, da sta oblast in moč podvrženi omejitvam prava in zlasti pravnemu redu, katerega razlog in smoter obstoja je varstvo temeljnih pravic.

131. Če je pri terorizmu edino merilo upravičenosti uporabljenih sredstev izključno (kar največja) učinkovitost napadov na ustaljeni red, se pri pravni državi učinkovitost presoja po merilih, v skladu s katerimi za njeno obrambo ni mogoče opustiti postopkov in jamstev, ki jo opredeljujejo kot legitimen pravni red. Če bi se pravna država brez nadaljnjega osredotočila le na učinkovitost, bi izgubila lastnost, ki je zanjo značilna, in utegnila bi – v skrajnih primerih – sama postati grožnja za državljana. Nikakor ni mogoče zagotoviti, da javna oblast, če bi se ji za pregon kaznivih dejanj priznala pretirano močna orodja, s katerimi bi lahko obšla ali oslabila temeljne pravice, s svojim nenadzorovanim in povsem neomejenim delovanjem nazadnje ne bi posegla v svobodo vseh.

132. Javna oblast pri povečevanju svoje učinkovitosti ne more čez oviro, ki jo pomenijo temeljne pravice državljanov, katerih omejitve se lahko, kot je določeno v členu 52(1) Listine, predpišejo le z zakonom in ob spoštovanju njihove bistvene vsebine, „če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih“.[79]

133. V zvezi s pogoji, pod katerimi bi bila – v skladu s sodbo Tele2 Sverige in Watson – dopustna *selektivna* hramba podatkov, napotujem na moje sklepne predloge v zadevi C-520/18[80].

77 Sodba Tele2 Sverige in Watson, točka 103: tak cilj „ne more upravičiti tega, da se nacionalna ureditev, ki določa splošno in neselektivno hrambo vseh podatkov o prometu in podatkov o lokaciji, šteje za potrebno za namen tega boja“.

78 Tako razloguje na primer francoska vlada, ki je to trditev ponazorila s konkretnimi primeri uporabnosti splošne hrambe podatkov, ki je omogočila odziv države na hude teroristične napade, do katerih je v zadnjih letih prišlo v njeni državi (točka 107 in točke od 122 do 126 pisnega stališča francoske vlade).

79 Sodba z dne 15. februarja 2016, N. (C-601/15 PPU, EU:C:2016:84, točka 50). Gre torej za zahtevno ravnovesje med javnim redom in svobodo, ki sem ga že omenil in h kateremu načeloma stremi vsa zakonodaja Unije. Primer je lahko Direktiva (EU) 2017/541 Evropskega parlamenta in Sveta z dne 15. marca 2017 o boju proti terorizmu in nadomestitvi Okvirnega sklepa Sveta 2002/475/PNZ ter o spremembi Sklepa Sveta 2005/671/PNZ (UL 2017, L 88, str. 6). Medtem ko je v členu 20(1) te direktive določeno, da morajo države članice zagotoviti, da imajo subjekti, pristojni za preiskovanje ter pregon kaznivih dejanj v zvezi s terorizmom, „na voljo učinkovita preiskovalna orodja“, pa je v uvodni izjavi 21 navedeno, da bi morala biti uporaba teh orodij „ciljno usmerjena in upoštevati načelo sorazmernosti ter naravo in težo preiskovanih kaznivih dejanj ter spoštovati pravico do varstva osebnih podatkov“.

80 Točke od 87 do 95.

134. Okoliščine, v katerih je na podlagi informacij, s katerimi razpolagajo varnostne službe, mogoče izhajati iz utemeljenega suma, da se pripravlja teroristični napad, lahko pomenijo primer, v katerem je upravičeno mogoče naložiti obveznost hrambe nekaterih podatkov. To velja še toliko bolj, če dejansko pride do napada. A medtem ko lahko v zadnjenavedenem primeru storitev kaznivega dejanja sama po sebi pomeni utemeljitven dejavnik za sprejetje tega ukrepa, mora biti v primeru, če je podan zgolj sum o tem, da se pripravlja morebitni napad, v zvezi z okoliščinami, na podlagi katerih je ukrep utemeljen, podana neka minimalna stopnja verjetnosti, ki je nujna za objektivno tehtanje indicev, zaradi katerih bi bil lahko ta ukrep upravičen.

135. Natančna in na podlagi objektivnih meril opravljena opredelitev kategorij podatkov, katerih hramba se šteje za nujno, in kroga zadevnih oseb je zahtevna, ne pa tudi nemogoča. Seveda bi bila najbolj *praktična in učinkovita* splošna hramba vseh podatkov, ki jih lahko zberejo ponudniki elektronskih komunikacijskih storitev, vendar sem že opozoril, da se vprašanje ne more reševati ob upoštevanju *praktične učinkovitosti*, temveč ob upoštevanju *pravne učinkovitosti* in v okviru pravne države.

136. Ta opredelitev se tipično opravi v okviru zakonodaje, izvesti pa se mora ob upoštevanju omejitev iz sodne prakse Sodišča. Spet napotujem na preudarke, ki sem jih v zvezi s tem opravil v sklepnih predlogih v zadevi C-520/18 [81].

3) Dostop do hranjenih podatkov

137. Ob predpostavki, da so operaterji podatke zbrali ob spoštovanju določb Direktive 2002/58 in da je bila njihova hramba izvedena ob upoštevanju člena 15(1) [82] te direktive, lahko pristojni organi do teh podatkov dostopajo pod pogoji, ki morajo biti izpolnjeni v skladu s sodno prakso Sodišča in ki sem jih analiziral v sklepnih predlogih v zadevi C-520/18, na katere napotujem. [83]

138. Zato je treba tudi v tem primeru z nacionalno ureditvijo določiti vsebinske in postopkovne pogoje, ki urejajo dostop pristojnih nacionalnih organov do hranjenih podatkov. [84] V okviru teh predlogov za sprejetje predhodne odločbe bi bil v skladu s temi pogoji dovoljen dostop do podatkov oseb, ki so osumljene, da načrtujejo ali da bodo storile teroristično dejanje, ali ki so storile ali ki bi bile lahko vpletene v teroristično dejanje. [85]

139. Vendar je bistveno to, da za dostop do zadevnih podatkov, razen v nujnih primerih, ki so ustrezno utemeljeni, sodišče ali neodvisen upravni organ opravi predhoden nadzor in da se odločba tega sodišča ali tega organa izda na obrazloženi predlog pristojnih organov. [86] Tako je v primerih, ki se ne morejo rešiti s presojo *in abstracto* na podlagi zakona, zagotovljena presoja *in concreto* tega neodvisnega organa, ki je enako zavezan zagotavljanju državne varnosti in varovanju temeljnih pravic državljanov.

81 Točke od 100 do 107.

82 Pri čemer morajo biti seveda spoštovani pogoji, omenjeni v točki 122 sodbe Tele2 Sverige in Watson: Sodišče je navedlo, da člen 15(1) Direktive 2002/58 ne omogoča odstopanja od členov 4(1) in 4(1a) te direktive, ki določa, da morajo ponudniki sprejeti ukrepe, s katerimi se zagotovi varstvo hranjenih podatkov pred tveganjem zlorabe in nepooblaščenim dostopom do teh podatkov. V tem smislu je ugotovilo, da morajo „[g]lede na količino hranjenih podatkov, občutljivost teh podatkov in tveganje za nezakonit dostop do teh podatkov […] ponudniki elektronskih komunikacijskih storitev, da zagotovijo celovitost in zaupnost teh podatkov, zagotoviti zelo visoko raven varstva in varnosti z ustreznimi tehničnimi in organizacijskimi ukrepi. Zlasti mora nacionalna ureditev določiti hrambo na ozemlju Unije in nepreklicno uničenje teh podatkov po koncu obdobja njihove hrambe.“

83 Točke od 52 do 60.

84 Sodba Tele2 Sverige in Watson, točka 118.

85 Prav tam, točka 119.

86 Prav tam, točka 120.

4) Obveznost hrambe podatkov, ki omogočajo identifikacijo avtorjev vsebin, glede na Direktivo 2000/31 (drugo vprašanje za predhodno odločanje v zadevi C-512/18)

140. Predložitveno sodišče se na Direktivo 2000/31 sklicuje kot na podlago za ugotavljanje, ali je nekaterim osebam [87] in operaterjem, ki ponujajo javne spletne komunikacijske storitve, mogoče naložiti hrambo podatkov, „ki omogočajo identifikacijo vsakogar, ki je prispeval k ustvarjanju vsebine ali ene od vsebin storitev, ki jih navedene osebe ponujajo, da bi lahko pravosodni organ po potrebi zahteval predložitev teh podatkov za dosego spoštovanja pravil v zvezi s civilno ali kazensko odgovornostjo“.

141. Strinjam se s Komisijo, da ne bi bilo primerno preučiti skladnosti te obveznosti z Direktivo 2000/31 [88], saj so s členom 1(5)(b) te direktive iz njenega področja uporabe izključena „vprašanja v zvezi s storitvami informacijske družbe, ki jih zajemata direktivi 95/46/ES in 97/66/ES“, torej predpisa, ki zdaj ustrezata Uredbi št. 2006/679 in Direktivi 2002/58, [89] katerih člen 23(1) oziroma člen 15(1) je treba po mojem mnenju razlagati tako, kot sem pojasnil zgoraj.

2. Obveznost zbiranja podatkov o prometu in lokaciji v realnem času (drugo vprašanje za predhodno odločanje v zadevi C-511/18)

142. Predložitveno sodišče meni, da je na podlagi člena L. 851-2 zakonika o notranji varnosti dovoljeno – izključno za preprečevanje terorizma – zbiranje informacij o osebah, ki so bile predhodno opredeljene kot osebe, ki bi bile lahko povezane s teroristično grožnjo, v realnem času. Podobno je na podlagi člena L. 851-4 tega zakonika omogočeno, da operaterji v realnem času posredujejo tehnične podatke o lokaciji terminalske opreme.

143. V skladu z navedbami predložitvenega sodišča te metode ponudnikom ne nalagajo obveznosti dodatne hrambe, ki presega to, kar je nujno za zaračunavanje in trženje njihovih storitev.

144. Poleg tega se lahko v skladu s členom L. 851-3 zakonika o notranji varnosti operaterjem elektronskih komunikacij in ponudnikom tehničnih storitev naloži obveznost, da „na svojih omrežjih izvajajo avtomatizirane obdelave na podlagi parametrov, navedenih v dovoljenju, pri čemer je cilj teh obdelav odkrivanje povezav, ki lahko pomenijo teroristično grožnjo“. Za uporabo te metode ni potrebna splošna in neselektivna hramba podatkov, njen namen pa je, da se omejeno časovno obdobje zbirajo podatki o povezavi, ki bi bili lahko povezani s kaznivim dejanjem v zvezi s terorizmom.

145. Menim, da pogoji, ki morajo biti izpolnjeni za dostop do hranjenih osebnih podatkov, veljajo tudi za dostop v realnem času do podatkov, ki nastanejo med elektronskimi komunikacijami. Napotujem torej na preudarke, ki sem jih v zvezi s tem opravil zgoraj. To, ali gre za podatke, ki se hranijo, ali podatke, ki se pridobijo v danem trenutku, ni pomembno, saj v obeh primerih pride do seznanitve z osebnimi podatki, pri čemer to, ali so pretekli ali sedanji, ni upoštevno.

146. Natančneje, če bi bile razlog za dostop v realnem času povezave, zaznane zaradi izvajanja avtomatizirane obdelave, kakršna je ta iz člena L. 851-3 zakonika o notranji varnosti, morajo biti modeli in merila, ki so bili predhodno določeni za to obdelavo, specifični in zanesljivi ter nediskriminatorni, tako da omogočajo identifikacijo posameznikov, glede katerih bi bil lahko podan utemeljen sum vpletenosti v teroristične dejavnosti. [90]

87 Tem, ki „za dostop javnosti prek javnih spletnih komunikacijskih storitev zagotavljajo […] hrambo vsakršnih signalov, pisnega in slikovnega gradiva, zvokov ali sporočil, ki se pridobijo od naslovnikov teh storitev […]“.

88 Predložitveno sodišče to direktivo na splošno in brez navedbe katere koli določbe omenja v drugem vprašanju iz zadeve C-512/18.

89 Točki 112 in 113 pisnega stališča Komisije.

90 Sodba Digital Rights, točka 59.

3. Obveznost obvestitve zadevnih oseb (tretje vprašanje v zadevi C-511/18)

147. Sodišče je ugotovilo, da morajo organi, ki jim je bil odobren dostop do podatkov, o tej okoliščini zadevne osebe obvestiti, če zaradi tega niso ogrožene preiskave, ki še potekajo. Razlog za to dolžnost je, da je ta informacija nujna, da te osebe lahko uresničijo pravico do pravnega sredstva, ki je izrecno določena v členu 15(2) Direktive 2002/58, če bi bile njihove pravice kršene.[91]

148. Conseil d'État (državni svet) želi s tretjim vprašanjem v zadevi C-511/18 izvedeti, ali mora biti ta zahteva po obvestitvi izpolnjena v vsakem primeru ali pa jo je mogoče opustiti, če so določena druga jamstva, kakršna so ta, opisana v predložitvenem sklepu.

149. V skladu s pojasnili predložitvenega sodišča[92] gre pri omenjenih jamstvih v bistvu za možnost, da lahko vsakdo, ki želi preveriti, ali je bila obveščevalna metoda uporabljena nezakonito, pri Conseil d'État (državni svet) vloži pravno sredstvo. Ta organ lahko v okviru postopka, v katerem ni uveljavljeno načelo kontradiktornosti, ki je običajno za sodne postopke, po potrebi razveljavi dovoljenje za uporabo ukrepa in odredi uničenje zbranih podatkov.

150. Predložitveni organ meni, da s to ureditvijo pravica do učinkovitega pravnega sredstva ni kršena. Vendar bi po mojem mnenju to v teoriji lahko držalo za osebe, ki se odločijo preveriti, ali so predmet obveščevalne operacije. Ni pa ta pravica spoštovana, če osebe, ki so ali so bile predmet te operacije, o tem niso obveščene, saj se tedaj ne morejo niti vprašati, ali so bile njihove pravice kršene ali ne.

151. Zdi se, da so pravna jamstva, na katera se sklicuje predložitveno sodišče, odvisna od pobude osebe, ki sumi, da se v zvezi z njo zbirajo podatki. Vendar mora biti dostop do sodišča zaradi obrambe lastnih pravic zagotovljen vsem, kar pomeni, da mora biti osebi, katere osebni podatki so bili predmet obdelave, omogočeno, da v sodnem postopku izpodbija zakonitost te obdelave, in mora biti zato o njenem obstoju obveščena.

152. Kot izhaja iz predloženih podatkov, se sodni postopek sicer res lahko začne po uradni dolžnosti ali na podlagi prijave znotraj uprave, vendar pa mora imeti zadevna oseba v vsakem primeru možnost, da ga začne sama, za kar pa je potrebno, da se ji razkrije, da so bili njeni osebni podatki predmet določene obdelave. Obramba njenih pravic ne more biti odvisna od okoliščine, da za to obdelavo izve od tretjih oseb ali zaradi svojih prizadevanj.

153. Zadevno osebo je torej treba obvestiti o dostopu do hranjenih podatkov, če se s tem ne ogrozijo še trajajoče preiskave, zaradi katerih je bil ta dostop dovoljen.

154. Nekaj drugega pa je, da za sodni postopek, ki se sproži na podlagi zahteve za pravno varstvo, ki jo zadevna oseba uveljavlja po tem, ko je bila obveščena o tem, da se je dostopalo do njenih podatkov, veljajo zahteve zaupnosti in tajnosti, ki so neločljivo povezane s preverjanjem delovanja javnih organov na občutljivih področjih, kakršno je področje varnosti in obrambe države. Vendar se to vprašanje v okviru obravnavanih predlogov za sprejetje predhodne odločbe ne postavlja, zaradi česar se Sodišče po mojem mnenju o njem ne bi smelo opredeliti.

91 Sodba Tele2 Sverige in Watson, točka 121.

92 Točke od 8 do 11 predložitvenega sklepa.

V. Predlog

155. Glede na navedeno Sodišču predlagam, naj Conseil d'État (državni svet, Francija) odgovori tako:

Člen 15(1) Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) v povezavi s členi 7, 8, 11 in 52(1) Listine Evropske unije o temeljnih pravicah je treba razlagati tako, da:

1. nasprotuje nacionalni ureditvi, s katero se v okoliščinah hudega in trajnega ogrožanja nacionalne varnosti ter zlasti teroristične grožnje operaterjem in ponudnikom elektronskih komunikacijskih storitev naloži obveznost splošne in neselektivne hrambe podatkov o prometu in lokaciji vseh naročnikov ter podatkov, ki omogočajo identifikacijo ustvarjalcev vsebin, dostop do katerih ponujajo izvajalci teh storitev;

2. nasprotuje nacionalni ureditvi, ki ne določa zahteve, da je treba zadevne osebe o obdelavi njihovih osebnih podatkov, ki so jo izvedli pristojni organi, informirati, razen če bi bilo zaradi tega ogroženo delovanje teh organov;

3. ne nasprotuje nacionalni ureditvi, v skladu s katero je dopustno zbiranje podatkov o prometu in lokaciji posameznih oseb v realnem času, če se ti ukrepi izvajajo v skladu s postopki, ki so določeni za dostop do osebnih podatkov, ki se zakonito hranijo, in ob enakih jamstvih.