Zbornik sudske prakse

MIŠLJENJE NEZAVISNOG ODVJETNIKA
MANUELA CAMPOSA SÁNCHEZ-BORDONE
od 15. siječnja 2020.[1]

Spojeni predmeti C-511/18 i C-512/18

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

(zahtjev za prethodnu odluku koji je uputio Conseil d'État (Državno vijeće, Francuska))

„Zahtjev za prethodnu odluku – Obrada osobnih podataka i zaštita privatnog života u području elektroničkih komunikacija – Zaštita nacionalne sigurnosti i borba protiv terorizma – Direktiva 2002/58/EZ – Područje primjene – Članak 1. stavak 3. – Članak 15. stavak 3. – Članak 4. stavak 2. UEU-a – Povelja Europske unije o temeljnim pravima – Članci 6., 7., 8., 11., 47. i članak 52. stavak 1. – Opće i neselektivno zadržavanje podataka o vezi i podataka koji omogućuju identifikaciju stvaratelja sadržaja – Prikupljanje podataka o prometu i lokaciji – Pristup podacima"

1. Sud posljednjih godina primjenjuje ustaljenu sudsku praksu u pogledu zadržavanja osobnih podataka i pristupa tim podacima, a njezine su istaknute presude sljedeće:

– Presuda od 8. travnja 2014., Digital Rights Ireland i dr.[2], u kojoj je presudio da je Direktiva 2006/24/EZ[3] nevaljana jer se njome dopušta neproporcionalno miješanje u prava priznata člancima 7. i 8. Povelje Europske unije o temeljnim pravima (u daljnjem tekstu: Povelja).

– Presuda od 21. prosinca 2016., Tele2 Sverige i Watson i dr.[4], u kojoj je tumačio članak 15. stavak 1. Direktive 2002/58/EZ[5].

– Presuda od 2. listopada 2018., Ministerio Fiscal[6], u kojoj je potvrdio tumačenje te odredbe Direktive 2002/58.

1 Izvorni jezik: španjolski

2 Predmeti C-293/12 i C-594/12, u daljnjem tekstu: presuda Digital Rights, EU:C:2014:238

3 Direktiva Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ (SL 2006., L 105, str. 54.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 50., str. 30.)

4 Predmeti C-203/15 i C-698/15, u daljnjem tekstu: presuda Tele2 Sverige i Watson, EU:C:2016:970

5 Direktiva Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL 2002., L 201, str. 37.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 52., str. 111.)

6 Predmet C-207/16, u daljnjem tekstu: presuda Ministerio Fiscal, EU:C:2018:788

2. Tijela nekih država članica zabrinuta su zbog tih presuda (osobito drugonavedene presude) jer je, prema njihovu shvaćanju, njihova posljedica oduzeti im instrument koji smatraju nužnim za zaštitu nacionalne sigurnosti i borbu protiv kriminaliteta i terorizma. Zbog toga neke od tih država članica zagovaraju opoziv ili prilagodbu te sudske prakse.

3. Određeni sudovi država članica istu su zabrinutost izrazili u četiri zahtjeva za prethodnu odluku [7], u čijim predmetima istoga dana iznosim svoje mišljenje i istu zabrinutost.

4. U sva četiri predmeta pojavljuje se, prije svega, problem primjene Direktive 2002/58 na aktivnosti povezane s nacionalnom sigurnosti i borbom protiv terorizma. Ako se Direktiva može primijeniti u tom kontekstu, nakon toga treba razjasniti u kojoj mjeri države članice mogu ograničiti prava privatnosti zaštićena tom direktivom. U konačnici, treba analizirati do koje su mjere različiti nacionalni propisi (britanski [8], belgijski [9] i francuski [10]) u tom području u skladu s pravom Unije, kako ga je Sud protumačio.

I. Pravni okvir

A. Pravo Unije

1. Direktiva 2002/58

5. Na temelju članka 1. („Područje primjene i cilj”):

„1. Direktiva osigurava usklađenost nacionalnih odredbi koje su potrebne kako bi se osigurala odgovarajuća razina zaštite osnovnih prava i sloboda, a posebno prava na privatnost i povjerljivost, s obzirom na obradu osobnih podataka u području elektroničkih komunikacija, te kako bi se osiguralo slobodno kretanje takvih podataka i elektroničke komunikacijske opreme i usluga u Zajednici.

[…]

3. Ova se Direktiva ne primjenjuje na aktivnosti koje su izvan područja primjene Ugovora o osnivanju Europske Zajednice, poput onih obuhvaćenih glavama V. i VI. Ugovora o Europskoj uniji, te, u svakom slučaju, na aktivnosti koje se odnose na javnu sigurnost, obranu, državnu sigurnost (uključujući gospodarsku dobrobit države kada se aktivnosti odnose na pitanja državne sigurnosti) te na aktivnosti države u području kaznenog prava.”

6. Člankom 3. („Usluge”) predviđa se:

„Ova se Direktiva primjenjuje na obradu osobnih podataka vezanih uz pružanje javno dostupnih usluga elektroničkih komunikacija na javno dostupnim komunikacijskim mrežama u Zajednici, uključujući javne komunikacijske mreže koje podržavaju prikupljanje podataka i naprava za identifikaciju.”

7 Osim ova dva predmeta (C-511/18 i C-512/18), predmeti C-623/17, Privacy International, i C-520/18, Ordre des barreaux francophones et germanophone i dr.

8 Predmet Privacy International, C-623/17

9 Predmet Ordre des barreaux francophones et germanophone i dr., C-520/18

10 Predmeti La Quadrature du Net i dr., C-511/18 i C-512/18

7. Članak 5. stavak 1. („Povjerljivost komunikacija”) glasi kako slijedi:

„Države članice putem svojih zakonodavstava osiguravaju povjerljivost komunikacija i s time povezanih podataka o prometu koji se šalju preko javne komunikacijske mreže i javno dostupnih elektroničkih komunikacijskih usluga. One posebno zabranjuju svim osobama koje nisu korisnici slušanje, prisluškivanje, pohranjivanje ili druge oblike presretanja odnosno nadzora nad komunikacijama i s time povezanim podacima o prometu, bez pristanka korisnika, osim u slučaju kada imaju zakonsko dopuštenje da to učine u skladu s člankom 15. stavkom 1. Ovaj stavak ne sprečava tehničko pohranjivanje koje je nužno za prijenos komunikacije, ne dovodeći u pitanje načelo povjerljivosti.”

8. Člankom 6. („Podaci o prometu”) propisuje se:

„1. Podaci o prometu koji se odnose na pretplatnike i korisnike i koje je davatelj javne komunikacijske mreže ili javno dostupne elektroničke komunikacijske usluge obradio i pohranio moraju se obrisati ili učiniti anonimnima kada više nisu potrebni u svrhu prijenosa komunikacije, ne dovodeći u pitanje stavke 2., 3. i 5. ovog članka te članak 15. stavak 1.

2. Podaci o prometu koji su nužni u svrhu naplaćivanja usluge od pretplatnika te u svrhu plaćanja međusobnog povezivanja mogu se obraditi. Takva je obrada dopustiva isključivo do kraja razdoblja tijekom kojega se račun može pravno pobijati ili tijekom kojega se može zahtijevati plaćanje.”

9. U članku 15. („Primjena određenih odredaba Direktive 95/46/EZ[[11]]”) stavku 1. navodi se:

„Države članice mogu donijeti zakonske mjere kojima će ograničiti opseg prava i obveza koji pružaju članak 5., članak 6., članak 8. stavci 1., 2., 3. i 4., te članak 9. ove Direktive kada takvo ograničenje predstavlja nužnu, prikladnu i razmjernu mjeru unutar demokratskog društva s ciljem zaštite nacionalne sigurnosti (odnosno državne sigurnosti), obrane, javne sigurnosti te s ciljem sprečavanja, istrage, otkrivanja i progona kaznenih djela odnosno neovlaštene uporabe elektroničkog komunikacijskog sustava iz članka 13. stavka 1. Direktive 95/46/EZ. S tim u vezi, države članice mogu, između ostalog, donijeti zakonske mjere kojima se omogućuje zadržavanje podataka tijekom ograničenog razdoblja opravdane razlozima određenim u ovom stavku. Sve mjere iz ovog stavka moraju biti u skladu s općim načelima prava Zajednice, uključujući ona iz članka 6. stavaka 1. i 2. Ugovora o Europskoj uniji.”

2. Direktiva 2000/31/EZ [12]

10. Člankom 14. propisuje se:

„1. Kad se pružena usluga informacijskog društva sastoji od pohrane informacija dobivenih od primatelja usluge, države članice moraju osigurati da davatelj usluge nije odgovoran za informacije pohranjene na zahtjev primatelja usluge, pod uvjetom:

[…]

3. Ovaj članak ne utječe na mogućnost da sud ili upravno tijelo, u skladu s pravnim sustavom države članice, od davatelja usluge zahtijeva okončanje ili sprečavanje prekršaja i ne utječe na mogućnost da država članica utvrdi postupke kojima se uređuje uklanjanje ili onemogućavanje pristupa informacijama.”

11 Direktiva Europskog parlamenta i vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (SL 1995., L 281, str. 31.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 7., str. 88.)

12 Direktiva Europskog parlamenta i Vijeća od 8. lipnja 2000. o određenim pravnim aspektima usluga informacijskog društva na unutarnjem tržištu, posebno elektroničke trgovine (Direktiva o elektroničkoj trgovini) (SL 2000., L 178, str. 1.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 39., str. 58.)

11. U skladu s člankom 15.:

„1. Države članice ne mogu uvesti opću obvezu za davatelje usluga da pri pružanju usluga iz članaka 12., 13., i 14. prate informacije koje prenose ili pohranjuju niti opću obvezu da aktivno traže činjenice ili okolnosti koje bi ukazivale na protuzakonite aktivnosti.

2. Države članice mogu utvrditi obveze za davatelje usluga informacijskog društva da odmah obavijeste nadležna tijela javne vlasti o navodnim protuzakonitim aktivnostima ili informacijama koje poduzimaju odnosno pružaju primatelji njihove usluge ili obvezu da nadležnim tijelima na njihov zahtjev dostave informacije koje omogućuju identifikaciju primatelja njihovih usluga s kojima imaju sporazume o pohrani informacija."

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

12. U skladu s člankom 2. („Glavno područje primjene"):

„1. Ova se Uredba primjenjuje na obradu osobnih podataka koja se u cijelosti obavlja automatizirano te na neautomatiziranu obradu osobnih podataka koji čine dio sustava pohrane ili su namijenjeni biti dio sustava pohrane.

2. Ova se Uredba ne odnosi na obradu osobnih podataka:

(a) tijekom djelatnosti koja nije obuhvaćena opsegom prava Unije;

(b) koju obavljaju države članice kada obavljaju aktivnosti koje su obuhvaćene područjem primjene glave V. poglavlja 2. UEU-a;

(c) koju provodi fizička osoba tijekom isključivo osobnih ili kućnih aktivnosti;

(d) koju obavljaju nadležna tijela u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihova sprečavanja.

[…]"

13. Na temelju članka 23. stavka 1. („Ograničenja"):

„Na temelju prava Unije ili prava države članice kojem podliježu voditelj obrade podataka ili izvršitelj obrade zakonskom mjerom može se ograničiti opseg obveza i prava iz članaka od 12. do 22. i članka 34. te članka 5. ako te odredbe odgovaraju pravima i obvezama predviđenima u člancima od 12. do 22., ako se takvim ograničenjem poštuje bit temeljnih prava i sloboda te ono predstavlja nužnu i razmjernu mjeru u demokratskom društvu za zaštitu:

(a) nacionalne sigurnosti;

(b) obrane;

(c) javne sigurnosti;

13 Uredba Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL 2016., L 119, str. 1. i ispravak SL 2018., L 127, str. 2.)

(d) sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenopravnih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;

(e) drugih važnih ciljeva od općeg javnog interesa Unije ili države članice, osobito važnog gospodarskog ili financijskog interesa Unije ili države članice, što uključuje monetarna, proračunska i porezna pitanja, javno zdravstvo i socijalnu sigurnost;

(f) zaštite neovisnosti pravosuđa i sudskih postupaka;

(g) sprečavanja, istrage, otkrivanja i progona kršenja etike za regulirane struke;

(h) funkcije praćenja, inspekcije ili regulatorne funkcije koja je, barem povremeno, povezana s izvršavanjem službene ovlasti u slučajevima iz točaka od (a) do (e) i točke (g);

(i) zaštite ispitanika ili prava i sloboda drugih;

(j) ostvarivanja potraživanja u građanskim sporovima."

14. Članak 95. („Odnos s Direktivom 2002/58/EZ") glasi:

„Ovom Uredbom ne propisuju se dodatne obveze fizičkim ili pravnim osobama u pogledu obrade u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga u javnim komunikacijskim mrežama u Uniji povezanih s pitanjima u pogledu kojih vrijede posebne obveze s istim ciljem iz Direktive 2002/58/EZ."

B. Nacionalno pravo

1. Code de la sécurité intérieure (Zakonik o unutarnjoj sigurnosti)

15. U skladu s člankom L. 851-1:

„U uvjetima utvrđenim u poglavlju 1. glave II. ove knjige, može se odobriti prikupljanje, od operatora elektroničkih komunikacija i osoba iz članka L. 34-1 Code des postes et des communications électroniques (Zakonik o pošti i elektroničkim komunikacijama) kao i osoba iz članka 6. stavka I. podstavaka 1. i 2. loi no 2004-575 […] pour la confiance dans l'économie numérique (Zakon br. 2004-575 za promicanje povjerenja u digitalnu ekonomiju), podataka ili dokumenata koje obrađuju ili zadržavaju njihove mreže ili elektroničke komunikacijske usluge, uključujući tehničkih podataka u pogledu identifikacije pretplatničkih brojeva i brojeva o vezi s uslugama elektroničkih komunikacija, prikazom svih pretplatničkih brojeva i brojeva o vezi određene osobe, lokaciji korištene terminalne opreme i komunikacijama pretplatnika, konkretno popis brojeva dolaznih i odlaznih poziva, datume i trajanje komunikacija […]".

16. Člancima L. 851-2 i L. 851-4 uređuje se, u druge svrhe i na druge načine, administrativni pristup u stvarnom vremenu podacima o vezi zadržanima na taj način.

17. Člankom L. 851-2 odobrava se, isključivo u svrhe sprečavanja terorizma, prikupljanje podataka ili dokumenata iz članka L. 851-1, od istih osoba. Takvo prikupljanje, koje se odnosi samo na jednog ili više unaprijed određenih pojedinaca za koje se sumnja da su povezani s terorističkom prijetnjom, obavlja se u stvarnom vremenu. Isto vrijedi i za članak L. 851-4, kojim se odobrava da operatori u

stvarnom vremenu prenose samo tehničke podatke u pogledu lokacije terminalne opreme[14].

18. Člankom L. 851-3 omogućuje se propisivanje operatorima elektroničkih komunikacija i pružateljima tehničkih usluga obveze da „na svojim mrežama uspostave automatizirane obrade podataka namijenjene, u uvjetima određenim u odobrenju, utvrđivanju veza koje mogu upućivati na terorističku prijetnju”[15].

19. Člankom L. 851-5 pojašnjava se da se, u određenim uvjetima, „može odobriti uporaba tehničke naprave koja omogućuje da se u stvarnom vremenu odredi lokacija neke osobe, vozila ili predmeta”.

20. U skladu s člankom L. 851-6 stavkom I., u određenim se uvjetima mogu „prikupiti […] izravno, s pomoću tehničkog uređaja ili naprave navedenih u članku 226-3 stavku 1. code pénal [(Kazneni zakonik)], tehnički podaci o vezi koji omogućuju identifikaciju terminalne opreme ili pretplatničkog broja njezina korisnika, kao i podaci u pogledu lokacije korištene terminalne opreme”.

2. Zakonik o pošti i elektroničkim komunikacijama

21. U skladu s člankom L. 34-1, u verziji koja se primjenjuje na činjenice iz glavnog postupka:

„I. Ovaj se članak primjenjuje na obradu osobnih podataka u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga; konkretno, primjenjuje se na mreže koje podržavaju naprave za prikupljanje podataka i identifikaciju.

II. Operatori elektroničkih komunikacija i osobito osobe čija je djelatnost nuditi pristup javnim internetskim komunikacijskim uslugama, brišu ili anonimiziraju sve podatke o prometu, ne dovodeći u pitanje odredbe stavaka III., IV., V. i VI.

Pružatelji javno dostupnih elektroničkih komunikacijskih usluga, u skladu s odredbama prethodnog podstavka, uspostavljaju unutarnje postupke za odgovaranje na zahtjeve nadležnih tijela.

Pružatelji koji, na temelju glavne ili sporedne profesionalne djelatnosti, pružaju javno dostupnu vezu koja omogućuje internetsku komunikaciju s pomoću pristupa mreži, čak i besplatno, obvezni su poštovati odredbe koje se primjenjuju na operatore elektroničkih komunikacija na temelju ovog članka.

III. U svrhu istrage, otkrivanja i progona kaznenih djela ili neispunjavanja obveze utvrđene u članku L. 336-3 code de la propriété intellectuelle [(Zakonik o intelektualnom vlasništvu)] ili u svrhu sprečavanja napada na sustave automatizirane obrade podataka koji se predviđaju i kažnjavaju člancima 323-1 do 323-3-1 Kaznenog zakonika, i s isključivim ciljem stavljanja na raspolaganje, po potrebi, sudskom tijelu ili visokom tijelu navedenom u članku L. 331-12 Zakonika o intelektualnom vlasništvu, ili pak nacionalnom tijelu nadležnom za sigurnost informacijskih sustava iz članka L. 2321-1 code de la défense [(Zakonik o obrani)], radnje brisanja ili anonimiziranja određenih kategorija tehničkih podataka mogu se odgoditi na razdoblje od najviše jedne godine. Uredbom koju je donio Conseil d'État (Državno vijeće), nakon što je dobiveno mišljenje Commission nationale de l'informatique et des libertés (Nacionalna komisija za informatiku i slobode), određuju se, u granicama utvrđenim u stavku VI., te kategorije podataka i trajanje njihova zadržavanja, ovisno o djelatnosti operatora i prirodi komunikacije te načinu naknade mogućih dodatnih odredivih i posebnih troškova usluga koje su u tom pogledu operatori pružali na zahtjev države.

14 Prema mišljenju suda koji je uputio zahtjeve, tim se tehnikama pružateljima usluga ne nalaže dodatna obveza zadržavanja u odnosu na ono što je nužno za naplaćivanje i stavljanje na tržište njihovih usluga, kao i za pružanje usluga s posebnom tarifom.

15 Prema mišljenju suda koji je uputio zahtjeve, cilj te tehnike, koja ne podrazumijeva opće i neselektivno zadržavanje, isključivo je prikupljanje, tijekom ograničenog razdoblja, samo onih podataka, između svih podataka o vezi koje obrađuju ti subjekti, koji mogu biti povezani s takvim teškim kaznenim djelom.

[…]

VI. Podaci koji se zadržavaju i obrađuju u uvjetima utvrđenim u stavcima III., IV. i V. odnose se isključivo na identifikaciju korisnika usluga koje pružaju operatori, na tehničke značajke komunikacija koje pružaju potonji operatori i na lokaciju terminalne opreme.

Ni u kojem se slučaju ne odnose na sadržaj razmijenjene prepiske ili informacije do kojih se dolazi, u bilo kojem obliku, u okviru tih komunikacija.

Podaci se zadržavaju i obrađuju u skladu s odredbama Zakona br. 78-17 od 6. siječnja 1978. o informatici, sustavima pohrane i slobodama.

Operatori poduzimaju sve mjere kako bi spriječili uporabu tih podataka u svrhe koje nisu predviđene ovim člankom."

22. Na temelju članka R. 10-13 stavka I., operatori u svrhu istrage, otkrivanja i progona kaznenih djela trebaju zadržati sljedeće podatke:

„(a) podatke kojima se identificira korisnik;

(b) podatke o korištenoj komunikacijskoj terminalnoj opremi;

(c) tehničke značajke, poput datuma, vremena i trajanja svake komunikacije;

(d) podatke o zatraženim ili upotrijebljenim dodatnim uslugama i njihovim pružateljima;

(e) podatke koji omogućuju identifikaciju jednog ili više primatelja komunikacije."

23. U skladu sa stavkom II. iste odredbe, u slučaju djelatnosti telefonije operator treba usto zadržati podatke koji omogućuju utvrđivanje izvora i lokacije komunikacije.

24. U skladu sa stavkom III. istog članka, navedeni podaci trebaju se čuvati jednu godinu od dana njihova zapisa.

3. La loi nº 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique (Zakon br. 2004-575 od 21. lipnja 2004. za promicanje povjerenja u digitalnu ekonomiju)

25. Prvim podstavkom stavka II. članka 6. Zakona br, 2004-575 utvrđuje se da osobe čija je djelatnost nuditi pristup javnim internetskim komunikacijskim uslugama i fizičke ili pravne osobe koje, čak i besplatno, za stavljanje na raspolaganje javnosti posredstvom javnih internetskih komunikacijskih usluga, osiguravaju pohranu bilo koje vrste signala, pisanog teksta, slika, zvukova ili poruka, a koji su dobiveni od primatelja tih usluga, „drže i zadržavaju podatke koji omogućuju identifikaciju bilo koje osobe koja je pridonijela stvaranju sadržaja ili jednog od sadržaja usluga koje pružaju".

26. Trećim podstavkom stavka II. iste odredbe propisuje se da sudsko tijelo može zatražiti da mu te osobe dostave podatke spomenute u prvom podstavku.

27. Posljednjim podstavkom stavka II. određuje se da se uredbom koju donosi Conseil d'État (Državno vijeće) „definiraju podaci spomenuti u prvom podstavku i određuje trajanje i načini njihova zadržavanja" [16].

II. Činjenice i prethodna pitanja

A. Predmet C-511/18

28. La Quadrature du Net, French Data Network, Igwan.net i Fédération des fournisseurs d'accès à internet associatifs (u daljnjem tekstu: tužitelji) zahtijevali su od Conseil d'État (Državno vijeće) poništenje različitih uredbi o provedbi određenih odredbi Zakonika o unutarnjoj sigurnosti [17].

29. Ukratko, tužitelji su tvrdili da su pobijane uredbe i odredbe Zakonika o unutarnjoj sigurnosti protivne pravu na poštovanje privatnog života, pravu na zaštitu osobnih podataka i pravu na djelotvoran pravni lijek, koja su redom zajamčena člancima 7., 8. i 47. Povelje.

30. U tim je okolnostima Conseil d'État (Državno vijeće) Sudu uputio sljedeća prethodna pitanja:

„1. Treba li obvezu općeg i neselektivnog zadržavanja podataka, koja se pružateljima usluga nalaže ovlašćujućim odredbama članka 15. stavka 1. Direktive 2002/58 […], u kontekstu koji uključuje ozbiljne i kontinuirane prijetnje nacionalnoj sigurnosti, i osobito rizik terorističkih napada, smatrati zadiranjem koje je opravdano pravom na sigurnost zajamčenim člankom 6. Povelje […] i zahtjevima nacionalne sigurnosti, za koje su odgovorne same države članice na temelju članka 4. [UEU-a]?

2. Treba li Direktivu 2002/58 […], u vezi s Poveljom […], tumačiti na način da dopušta zakonske mjere, poput mjera prikupljanja u stvarnom vremenu podataka o prometu i podataka o lokaciji određenih pojedinaca, koje im, iako utječu na prava i obveze pružatelja elektroničke komunikacijske usluge, ne nalažu posebnu obvezu zadržavanja njihovih podataka?

3. Treba li Direktivu 2002/58 […], u vezi s Poveljom […], tumačiti na način da su postupci prikupljanja podataka o vezi pravilni samo ako se osobe o kojima je riječ obavijesti onda kada te informacije više ne mogu ugroziti istrage koje provode nadležna tijela ili se takve postupke može smatrati pravilnima s obzirom na sva ostala postojeća postupovna jamstva, s obzirom na to da ona osiguravaju djelotvornost pravnog lijeka?"

16 Definirani su na temelju 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 (Uredba br. 2011-219 od 25. veljače 2011. o zadržavanju podataka koji omogućuju identifikaciju bilo koje osobe koja je doprinijela stvaranju sadržaja dostupnog na internetu). U toj se uredbi ističu: (a) članak 1. stavak 1. u skladu s kojim oni koji pružaju pristup uslugama internetske komunikacije trebaju zadržati sljedeće podatke: identifikator veze, identifikator dodijeljen pretplatniku, identifikator terminala koji se koristi za vezu, datum i vrijeme početka i završetka veze, značajke pretplatničke linije; (b) članak 1. stavak 2. u skladu s kojim oni koji, čak i besplatno, za stavljanje na raspolaganje javnosti putem javnih internetskih komunikacijskih usluga, osiguravaju pohranu bilo koje vrste signala, pisanog teksta, slika, zvukova ili poruka, a koji su dobiveni od primatelja tih usluga trebaju, za svaku radnju, zadržati sljedeće podatke: identifikator veze na izvoru komunikacije, identifikator dodijeljen sadržaju koji je predmet radnje, vrste protokola koje se koriste za vezu s uslugom i za prijenos sadržaja, prirodu radnje, datum i vrijeme radnje, identifikator kojim se koristi autor radnje; i (c) u konačnici, članak 1. stavak 3. kojim se propisuje da osobe navedene u dvama prethodnim stavcima trebaju zadržati sljedeće podatke koje je korisnik pružio prilikom sklapanja ugovora ili izrade računa: identifikator veze prilikom izrade računa; ime, prezime ili naziv društva; povezane poštanske adrese, korištene pseudonime, povezane adrese elektroničke pošte ili računa, brojeve telefona, ažuriranu ključnu riječ i podatke koji omogućuju njezinu verifikaciju ili izmjenu.

17 Pobijale su se sljedeće uredbe: (a) décret n.° 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement (Uredba br. 2015-1185 od 28. rujna 2015. o uspostavi specijaliziranih službi za prikupljanje podataka); (b) décret n.° 2015-1211 du 1er octubre 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 (Uredba br. 2015-1211 od 1. listopada 2015. o sporovima o primjeni tehnika prikupljanja podataka podvrgnutih odobrenju i spisima u pogledu nacionalne sigurnosti); (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 libre VIII du code de la sécurité intérieure (Uredba br. 2015-1639 od 11. prosinca 2015. o uspostavi službi različitih od specijaliziranih službi za prikupljanje podataka, ovlaštenih koristiti tehnike iz glave V. knjige VIII. Zakonika o unutarnjoj sigurnosti); i (d) décret n.° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (Uredba br. 2016-67 od 29. siječnja 2016. o tehnikama prikupljanja podataka).

B. Predmet C-512/18

31. Tužitelji u sporu na kojem se temelji predmet C-511/18, osim društva Igwan.net, od Conseil d'État (Državno vijeće) također su zahtijevali da poništi odluku o odbijanju (zbog šutnje uprave) njihova zahtjeva za stavljanje izvan snage članka R. 10-13 Zakonika o pošti i elektroničkim komunikacijama i Uredbe br. 2011-219 od 25. veljače 2011.

32. Prema mišljenju tih tužitelja, pobijanim se pravilima propisuje obveza zadržavanja podataka o prometu, lokaciji i vezi, kojom se zbog njezine općenitosti neproporcionalno povređuje pravo na poštovanje privatnog i obiteljskog života, pravo na zaštitu osobnih podataka i pravo na slobodu izražavanja, zajamčena člancima 7., 8. i 11. Povelje, uz povredu članka 15. stavka 1. Direktive 2002/58.

33. U okviru te tužbe, Conseil d'État (Državno vijeće) uputio je sljedeća prethodna pitanja:

„1. Treba li obvezu općeg i neselektivnog zadržavanja podataka, koja se pružateljima usluga nalaže ovlašćujućim odredbama članka 15. stavka 1. Direktive 2002/58 […], osobito s obzirom na jamstva i kontrole koji se potom primjenjuju na prikupljanje i korištenje tih podataka o spajanju, smatrati zadiranjem koje je opravdano pravom na sigurnost zajamčenim člankom 6. Povelje […] i zahtjevima nacionalne sigurnosti, za koje su odgovorne same države članice na temelju članka 4. [UEU-a]?

2. Treba li odredbe Direktive 2000/31, kada ih se tumači s obzirom na članke 6., 7., 8. i 11. te članak 52. stavak 1. Povelje […], tumačiti na način da državi članici omogućavaju donošenje nacionalnog propisa kojim se osobama čija je djelatnost nuđenje pristupa javnim internetskim komunikacijskim uslugama i fizičkim ili pravnim osobama koje, čak i besplatno, za stavljanje na raspolaganje javnosti putem javnih internetskih komunikacijskih usluga, osiguravaju pohranu bilo koje vrste signala, pisanog teksta, slika, zvukova ili poruka, a koji su dobiveni od primatelja tih usluga, nalaže da zadrže podatke koji omogućuju identifikaciju bilo koje osobe koja je doprinijela stvaranju sadržaja ili jednog od sadržaja usluga koje pružaju, kako bi sudsko tijelo moglo, po potrebi, zatražiti da mu se taj sadržaj dostavi u svrhu osiguravanja poštovanja pravila vezanih uz građansku ili kaznenu odgovornost?"

III. Postupak pred Sudom i stajališta stranaka

34. Tajništvo Suda zaprimilo je zahtjeve za prethodnu odluku 3. kolovoza 2018.

35. Pisana očitovanja podnijeli su La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, French Data Network, belgijska, britanska, češka, ciparska, danska, estonska, francuska, irska, mađarska, njemačka, španjolska, poljska i švedska vlada te Komisija.

36. Na raspravi održanoj 9. rujna 2019., koja je održana i za predmete C-623/17, Privacy International, i C-520/18, Ordre des barreaux francophones et germanophone i dr., sudjelovale su stranke četiriju prethodnih postupaka, prethodno navedene vlade i nizozemska i norveška vlada, Komisija i Europski nadzornik za zaštitu osobnih podataka.

IV. Analiza

37. Pitanja koja je uputio Conseil d'État (Državno vijeće) mogu se podijeliti u tri skupine:

– Kao prvo, je li s pravom Unije usklađen nacionalni propis kojim se pružateljima elektroničkih komunikacijskih usluga propisuje obveza općeg i neselektivnog zadržavanja podataka o vezi (prvo pitanje u predmetu C-511/18 i predmetu C-512/18) i, osobito, podataka koji omogućuju identifikaciju stvaratelja sadržaja koje nude navedeni pružatelji (drugo pitanje u predmetu C-512/18).

– Kao drugo, je li zakonitost postupaka prikupljanja podataka o vezi u svakom slučaju uvjetovana obvezom obavješćivanja dotičnih osoba ako se ne ugrožavaju istrage (treće pitanje u predmetu C-511/18).

– Kao treće, je li prikupljanje u stvarnom vremenu podataka o prometu i lokaciji, bez obveze njihova zadržavanja, u skladu, i u kojim uvjetima, s Direktivom 2002/58 (drugo pitanje u predmetu C-511/18).

38. U konačnici, valja utvrditi je li s pravom Unije usklađen nacionalni propis kojim se pružateljima elektroničkih komunikacijskih usluga nalažu dvije vrste obveza: (a) s jedne strane, *prikupljanje* određenih podataka, ali ne i njihovo zadržavanje; (b) s druge strane, *zadržavanje* podataka o vezi i podataka koji omogućuju identifikaciju stvaratelja sadržaja usluga koje pružaju takvi pružatelji.

39. Najprije treba utvrditi primjenjuje li se Direktiva 2002/58 upravo u kontekstu [18] u kojem je taj nacionalni propis donesen (odnosno, u okolnostima moguće ugroze nacionalne sigurnosti).

A. Primjenjivost Direktive 2002/58

40. Sud koji je uputio zahtjeve smatra da je propis koji je predmet spora obuhvaćen područjem primjene Direktive 2002/58. Prema njegovu mišljenju, to proizlazi iz sudske prakse koja je uspostavljena presudom Tele2 Sverige i Watson te koja je potvrđena presudom Ministerio Fiscal.

41. Suprotno tomu, neke vlade koje su intervenirale u postupak tvrde da sporni propis nije obuhvaćen navedenim područjem primjene. Kako bi potkrijepili svoje stajalište, među ostalim argumentima navode presudu od 30. svibnja 2006., Parlament/Vijeće i Komisija [19].

42. Slažem se s mišljenjem Conseil d'État (Državno vijeće) u pogledu toga da je u presudi Tele2 Sverige i Watson riješen taj dio spora, pri čemu se potvrđuje da se Direktiva 2002/58 u načelu primjenjuje kad su pružatelji elektroničkih usluga zakonom obvezani zadržavati podatke svojih pretplatnika i dopustiti tijelima javne vlasti da pristupe tim podacima. Time se ne mijenja činjenica da se obveze nalažu pružateljima zbog razloga nacionalne sigurnosti.

43. Odmah moram istaknuti da, ako postoji neusklađenost između presude Tele2 Sverige i Watson i prethodnih presuda, treba dati prednost presudi Tele2 Sverige i Watson jer je novija i potvrđena presudom Ministerio Fiscal. Međutim, smatram da ta neusklađenost ne postoji, kao što ću to pokušati objasniti.

18 „[U] kontekstu koji uključuje ozbiljne i kontinuirane prijetnje nacionalnoj sigurnosti, i osobito rizik terorističkih napada", kako je navedeno u prvom pitanju u predmetu C-511/18.

19 Predmeti C-317/04 i C-318/04, u daljnjem tekstu: presuda Parlament/Vijeće i Komisija, EU:C:2006:346

1. Presuda Parlament/Vijeće i Komisija

44. Predmeti u kojima je donesena presuda Parlament/Vijeće i Komisija odnosili su se na sljedeće:

– Sporazum između Europske zajednice i Sjedinjenih Američkih Država o obradi i prijenosu podataka PNR [Passenger Name Records (podataka iz evidencije o putnicima)] zračnih prijevoznika tijelima Sjedinjenih Američkih Država [20].

– Prikladnost zaštite osobnih podataka iz evidencije podataka o putnicima, koji se prenose navedenim tijelima [21].

45. Sud je zaključio da prijenos tih podataka podrazumijeva obradu čiji su predmet javna sigurnost i aktivnosti države u području kaznenog prava. U skladu s člankom 3. stavkom 2. prvom alinejom Direktive 95/46, nijedna od spornih odluka nije obuhvaćena područjem primjene Direktive 95/46.

46. Podatke su prvotno prikupili zračni prijevoznici u okviru aktivnosti prodaje karata koja je obuhvaćena područjem primjene prava Unije. Međutim, njihova obrada, kako je predviđena spornom odlukom, „nije nužna za pružanje usluga, nego se smatra nužnom za zaštitu javne sigurnosti i u represivne svrhe” [22].

47. Sud je tako primijenio teleološki pristup, uzimajući u obzir svrhu koja se nastoji postići obradom podataka: ako se njome želi postići zaštita javne sigurnosti, treba smatrati da nije obuhvaćena područjem primjene Direktive 95/46. Međutim, ta svrha nije bila jedini odlučujući kriterij [23], zbog čega je u presudi istaknuto da je prijenos „uključen u okvir koji su uspostavila tijela javne vlasti i čiji je cilj zaštita javne sigurnosti” [24].

48. Stoga se na temelju presude Parlament/Vijeće i Komisija može utvrditi razlika između odredbe o isključenju i odredbi o restrikciji ili ograničenju Direktive 95/46 (koje su istovjetne odredbama Direktive 2002/58). Međutim, točno je da se jedne i druge odredbe odnose na slične ciljeve u općem interesu, što dovodi do određenih nejasnoća u pogledu njihova dosega, kao što je to svojedobno napomenuo nezavisni odvjetnik Y. Bot [25].

20 Odluka Vijeća 2004/496/EZ od 17. svibnja 2004. o sklapanju Sporazuma između Europske zajednice i Sjedinjenih Američkih Država o obradi i prijenosu podataka iz evidencije podataka o putnicima zračnih prijevoznika Ministarstvu domovinske sigurnosti, Uredu carine i pogranične sigurnosti Sjedinjenih Američkih Država (SL 2004., L 183, str. 83.) (predmet C-317/04)

21 Odluka Komisije 2004/535/EZ od 14. svibnja 2004. o prikladnosti zaštite osobnih podataka iz evidencije podataka o putnicima koji se prenose Uredu carine i pogranične sigurnosti Sjedinjenih Američkih Država (SL 2004., L 235, str. 11.) (predmet C-318/04)

22 Presuda Parlament/Vijeće i Komisija, t. 57. U točki 58. ustraje se na tome da „činjenica da podatke […] prikupljaju privatni operatori u trgovačke svrhe i da ti operatori organiziraju njihov prijenos trećoj državi” ne podrazumijeva da taj prijenos ne čini jedan od slučajeva neprimjene Direktive 95/46 navedenih u članku 3. stavku 2. prvoj alineji potonje direktive jer je „taj prijenos uključen u okvir koji su uspostavila tijela javne vlasti i čiji je cilj zaštita javne sigurnosti”.

23 To je, u konačnici, istaknuo cijenjeni nezavisni odvjetnik Y. Bot u svojem mišljenju u predmetu Irska/Parlament i Vijeće (C-301/06, EU:C:2008:558). Tvrdio je da presuda Parlament/Vijeće i Komisija „ne može značiti […] da je samo ispitivanje cilja koji se nastoji postići obradom osobnih podataka relevantno za uključivanje ili, ovisno o slučaju, isključivanje te obrade iz područja primjene sustava zaštite podataka utvrđenog Direktivom 95/46. Također valja provjeriti u okviru koje se vrste aktivnosti provodi obrada podataka. Samo u slučaju da je navedena obrada provedena radi obavljanja aktivnosti države ili državnih tijela koje ne ulaze u područje aktivnosti pojedinaca, ona se isključuje iz sustava Zajednice za zaštitu osobnih podataka utvrđenog Direktivom 95/46 i to u skladu s člankom 3. stavkom 2. prvom alinejom te direktive” (točka 122.).

24 Presuda Parlament/Vijeće i Komisija, t. 58. Glavni predmet Sporazuma bio je da se od zračnih prijevoznika koji pružaju usluge prijevoza putnika između Unije i Sjedinjenih Američkih Država zahtijeva da američkim tijelima omoguće elektronički pristup podacima PNR iz evidencije podataka o putnicima koji se nalaze u njihovu računalnom sustavu nadzora rezervacija i odlazaka. Stoga je njime uspostavljen jedan oblik međunarodne suradnje između Unije i Sjedinjenih Američkih Država za borbu protiv terorizma i drugih teških kaznenih djela, pri čemu se taj cilj pokušalo uskladiti s ciljem zaštite osobnih podataka putnika. U tom kontekstu, obveza propisana zračnim prijevoznicima nije se uvelike razlikovala od izravne razmjene podataka među tijelima javne vlasti.

25 Mišljenje nezavisnog odvjetnika Y. Bota u predmetu Irska/Parlament i Vijeće (C-301/06, EU:C:2008:558, t. 127.)

49. Iz tih nejasnoća vjerojatno proizlazi stajalište koje zagovaraju države članice koje smatraju da Direktiva 2002/58 nije primjenjiva na taj kontekst. Prema njihovu mišljenju, interes nacionalne sigurnosti osigurava se samo isključenjem iz članka 1. stavka 3. Direktive 2002/58. Međutim, točno je da tom interesu služe i ograničenja odobrena člankom 15. stavkom 1. navedene direktive, među kojima je ograničenje u pogledu nacionalne sigurnosti. Potonja bi odredba bila suvišna kad se Direktiva 2002/58 ne bi primjenjivala prilikom bilo kakvog pozivanja na nacionalnu sigurnost.

2. Presuda Tele2 Sverige i Watson

50. U presudi Tele2 Sverige i Watson razmatralo se jesu li s pravom Unije usklađeni određeni nacionalni sustavi kojima se pružateljima javno dostupnih elektroničkih komunikacijskih usluga propisuje opća obveza zadržavanja podataka o navedenim komunikacijama. Slučajevi su stoga bili u bitnome istovjetni onima koji se rješavaju u predmetnim prethodnim postupcima.

51. Budući da se ponovno postavlja pitanje primjenjivosti prava Unije, ovaj put u okviru Direktive 2002/58, Sud je za početak istaknuo da se „područje primjene Direktive 2002/58 mora ocjenjivati vodeći računa osobito o njezinoj općoj strukturi” [26].

52. U tom je pogledu Sud napomenuo da se, „[d]oista, zakonske mjere iz članka 15. stavka 1. Direktive 2002/58 odnose […] na državne aktivnosti ili aktivnosti državnih tijela, koje nisu svojstvene aktivnostima pojedinaca […]. Nadalje, ciljevi kojima na temelju te odredbe takve mjere moraju težiti – u predmetnom slučaju zaštita nacionalne sigurnosti […] – u biti se preklapaju s ciljevima aktivnosti iz članka 1. stavka 3. te direktive” [27].

53. Stoga je svrha mjera koje, u skladu s člankom 15. stavkom 1. Direktive 2002/58, države članice mogu donijeti radi ograničavanja prava na privatnost istovjetna (u tom pogledu) svrsi kojom se opravdava isključenje određenih državnih aktivnosti iz sustava Direktive, u skladu s člankom 1. stavkom 3.

54. Međutim, Sud je smatrao da, „s obzirom na opću strukturu Direktive 2002/58”, ta okolnost ne omogućuje „zaključak da su zakonske mjere iz njezina članka 15. stavka 1. isključene iz područja primjene te direktive jer bi u suprotnom navedena odredba ostala bez ikakva korisnog učinka. Ta odredba nužno pretpostavlja da nacionalne mjere koje su njome predviđene […] spadaju u područje primjene spomenute direktive jer potonja izričito ovlašćuje države članice da ih donesu samo uz poštovanje uvjeta koje predviđa” [28].

55. Uz prethodno navedeno, ističe se da ograničenja odobrena člankom 15. stavkom 1. Direktive 2002/58 „uređuju, u svrhu spomenutu u toj odredbi, aktivnosti pružatelja elektroničkih komunikacijskih usluga”. Slijedom toga, navedenu odredbu, u vezi s člankom 3. Direktive, „valja tumačiti na način da takve zakonske mjere spadaju u područje njezine primjene” [29].

56. Sud je stoga tvrdio da u područje primjene Direktive 2002/58 spada zakonska mjera kojom se pružateljima „nalaže zadržavanje podataka o prometu i lokaciji jer se takva aktivnost nužno odnosi na to da oni obrađuju osobne podatke” [30] i zakonska mjera o pristupu tijela podacima koje su zadržali ti pružatelji [31].

26 Presuda Tele2 Sverige i Watson, t. 67.

27 *Ibidem*, t. 72.

28 *Ibidem*, t. 73.

29 *Ibidem*, t. 74.

30 *Ibidem*, t. 75.

31 *Ibidem*, t. 76.

57. Tumačenje Direktive 2002/58 koje je Sud primijenio u presudi Tele2 Sverige i Watson ponavlja se u presudi Ministerio Fiscal.

58. Može li se tvrditi da presuda Tele2 Sverige i Watson predstavlja više ili manje implicitan zaokret u odnosu na sudsku praksu uspostavljenu presudom Parlament/Vijeće i Komisija? Na primjer, irska vlada smatra da može te smatra da je samo potonja presuda u skladu s pravnom osnovom Direktive 2002/58 i s člankom 4. stavkom 2. UEU-a [32].

59. Francuska vlada pak smatra da se proturječje može opravdati ako se utvrdi da se u sudskoj praksi uspostavljenoj presudom Tele2 Sverige i Watson upućuje na aktivnosti država članica u području kaznenog prava, a da se sudska praksa uspostavljena presudom Parlament/Vijeće i Komisija odnosi na nacionalnu sigurnost i obranu. Stoga se sudska praksa uspostavljena presudom Tele2 Sverige i Watson ne bi primjenjivala na slučaj koji se sada razmatra, a u kojem bi trebalo primijeniti rješenje iz presude Parlament/Vijeće i Komisija [33].

60. Kao što sam već istaknuo, smatram da se može pronaći način da se te dvije presude integriraju, a koji se razlikuje od načina koji zagovara francuska vlada. Ne slažem se s potonjim mišljenjem jer smatram da se razmatranja iz presude Tele2 Sverige i Watson koja se izričito odnose na borbu protiv terorizma [34] mogu proširiti na bilo koju drugu prijetnju nacionalnoj sigurnosti (a terorizam je samo jedna od njih).

3. Mogućnost usklađenog tumačenja presude Parlament/Vijeće i Komisija i presude Tele2 Sverige i Watson

61. Prema mojem mišljenju, Sud je u presudama Tele2 Sverige i Watson te Ministerio Fiscal uzeo u obzir svrhu odredbi o isključenju i ograničenju, kao i sustavnu povezanost tih dviju vrsta odredbi.

62. To što je Sud u predmetu Parlament/Vijeće i Komisija utvrdio da obrada podataka nije obuhvaćena područjem primjene Direktive 95/46, bilo je zato što je, kao što sam već podsjetio, u kontekstu suradnje između Europske unije i Sjedinjenih Američkih Država, koja se uobičajeno odvija u međunarodnom okviru, trebala prevladati državna dimenzija aktivnosti u odnosu na činjenicu da ta obrada podrazumijeva i trgovačku ili privatnu dimenziju. Jedno od tada spornih pitanja odnosilo se upravo na pravnu osnovu koja je prikladna za donošenje sporne odluke.

63. Suprotno tomu, u odnosu na nacionalne mjere koje su se ispitivale u presudama Tele2 Sverige i Watson te Ministerio Fiscal, Sud je u prvi plan stavio nacionalni opseg obrade podataka: regulatorni okvir u kojem se ta obrada obavljala bio je isključivo nacionalni te stoga nije imao vanjsku dimenziju svojstvenu predmetu iz presude Parlament/Vijeće i Komisija.

64. Različita važnost međunarodne i nacionalne (trgovačke i privatne) dimenzije obrade podataka dovela je do toga da se, u prvom slučaju, propiše odredba o isključenju iz prava Unije, kao najprikladnija odredba za zaštitu općeg interesa nacionalne sigurnosti. U drugom slučaju, suprotno tomu, isti se interes mogao učinkovito zaštititi odredbom o ograničenju predviđenom u članku 15. stavku 1. Direktive 2002/58.

65. Još bi valjalo ocijeniti drugu razliku koja je povezana s različitim regulatornim okvirom: svaka od tih presuda usmjerena je na tumačenje dviju odredbi koje, osim naizgled, nisu iste.

32 Točke 15. i 16. pisanih očitovanja irske vlade

33 Točke 34. do 50. pisanih očitovanja francuske vlade

34 Presuda Tele2 Sverige i Watson, t. 103. i 119.

66. Tako se u presudi Parlament/Vijeće i Komisija odlučivalo o tumačenju članka 3. stavka 2. Direktive 95/46, a u presudi Tele2 Sverige i Watson o članku 1. stavku 3. Direktive 2002/58. Pažljivim čitanjem tih članaka otkrivaju se dovoljne razlike kako bi se potkrijepio smisao presuda Suda u jednom odnosno drugom slučaju.

67. U skladu s člankom 3. stavkom 2. Direktive 95/46, „[o]va se Direktiva *ne primjenjuje na obradu osobnih podataka* […] tijekom aktivnosti koja je izvan područja primjene prava Zajednice, […] i u svakom slučaju na *postupke obrade* koji se odnose na javnu sigurnost, obranu, nacionalnu sigurnost (uključujući gospodarsku dobrobit države kada se *operacija obrade* odnosi na pitanja nacionalne sigurnosti) i aktivnosti države u području kaznenog prava” [35].

68. Međutim, u skladu s člankom 1. stavkom 3. Direktive 2002/58, potonja se direktiva *„ne primjenjuje na aktivnosti* koje su izvan područja primjene Ugovora o osnivanju Europske Zajednice […], te, u svakom slučaju, *na aktivnosti* koje se odnose na javnu sigurnost, obranu, državnu sigurnost (uključujući gospodarsku dobrobit države kada se *aktivnosti* odnose na pitanja državne sigurnosti) te na aktivnosti države u području kaznenog prava” [36].

69. Dok se člankom 3. stavkom 2. Direktive 95/46 isključuju *postupci obrade* koji se odnose, za potrebe ovog predmeta, na nacionalnu sigurnost, člankom 1. stavkom 3. Direktive 2002/58 isključuju se *aktivnosti* kojima se želi, također za potrebe ovog predmeta, očuvati nacionalna sigurnost.

70. Razlika nije zanemariva. U skladu s Direktivom 95/46, njezinim područjem primjene nije obuhvaćena aktivnost („obrada osobnih podataka”) koju bilo tko može obavljati. Iz te su aktivnosti posebno izuzeti postupci obrade koji se odnose, među ostalim, na nacionalnu sigurnost. Priroda *subjekta* koji obavlja obradu podataka bila je pak nevažna. Pristup koji je primijenjen radi utvrđivanja isključenih aktivnosti stoga je bio teleološki ili svrsishodan, te se njime nisu razlikovale osobe koje su obavljale te aktivnosti.

71. Tako se u predmetu Parlament/Vijeće i Komisija smatra da je Sud primarno odlučivao o cilju koji se nastoji postići obradom podataka. Nije bila važna „činjenica da podatke […] prikupljaju privatni operatori u trgovačke svrhe i da ti operatori organiziraju njihov prijenos trećoj državi” jer je ključno bilo to da je „taj prijenos uključen u okvir koji su uspostavila tijela javne vlasti i čiji je cilj zaštita javne sigurnosti” [37].

72. Suprotno tomu, „aktivnosti koje se odnose na državnu sigurnost”, koje nisu obuhvaćene područjem primjene Direktive 2002/58 analiziranim u predmetu Tele2 Sverige i Watson, ne mogu se pripisati bilo kojem subjektu, nego isključivo samoj državi. Osim toga, u te se aktivnosti ne ubrajaju zakonodavne ili regulatorne funkcije države, nego isključivo materijalne aktivnosti tijela javne vlasti.

73. Naime, *aktivnosti* navedene u članku 1. stavku 3. Direktive 2002/58 „u svakom su slučaju aktivnosti država odnosno državnih tijela koje ne ulaze u područje aktivnosti pojedinaca” [38]. Međutim, te „aktivnosti” ne mogu biti regulatorne prirode. U tom slučaju, nijedna od odredbi koje države članice donose u odnosu na obradu osobnih podataka ne bi bila obuhvaćena područjem primjene Direktive 2002/58, osim ako bi ih se nastojalo opravdati kao nužne za osiguranje nacionalne sigurnosti.

35 Moje isticanje

36 Moje isticanje

37 Parlament/Vijeće i Komisija, t. 58.

38 Presuda Ministerio Fiscal, t. 32. U istom smislu presuda Tele2 Sverige i Watson, t. 72.

74. S jedne strane, to bi značilo znatan gubitak za učinkovitost navedene direktive jer bi puko pozivanje na tako neodređeni pravni pojam kao što je to pojam nacionalne sigurnosti bilo dovoljno da u odnosu na države članice postanu neprimjenjiva jamstva koja je zakonodavac Unije utvrdio kako bi se zaštitili osobni podaci građana. Ta zaštita nije moguća bez sudjelovanja država članica i njezino se jamstvo građanima osigurava i u odnosu na nacionalna tijela javne vlasti.

75. S druge strane, tumačenje pojma „državne aktivnosti" koje bi podrazumijevalo aktivnosti koje se očituju u donošenju pravnih pravila i odredbi, lišilo bi smisla članak 15. Direktive 2002/58, kojim se države članice upravo ovlašćuju, iz razloga zaštite, *inter alia*, nacionalne sigurnosti, za donošenje „zakonskih mjera" s ciljem da se smanji opseg određenih prava i obveza iz iste direktive [39].

76. Kao što je to Sud istaknuo u presudi Tele2 Sverige i Watson, „područje primjene Direktive 2002/58 mora [se] ocjenjivati vodeći računa osobito o njezinoj općoj strukturi" [40]. S tog gledišta, tumačenje članka 1. stavka 3. i članka 15. stavka 1. Direktive 2002/58, koje im daje smisao a da pritom ne izgube svoju učinkovitost, jest tumačenje koje, u prvoj od te dvije odredbe, utvrđuje materijalno isključenje koje se odnosi na *aktivnosti* koje obavljaju države članice u području nacionalne sigurnosti (i istovjetnim područjima) i, u drugoj odredbi, ovlaštenje za donošenje *zakonskih mjera* (odnosno općih pravila) koje, u svrhu nacionalne sigurnosti, utječu na aktivnosti pojedinaca koji podliježu vlasti država članica, pri čemu se tim mjerama ograničavaju prava zajamčena Direktivom 2002/58.

4. Isključenje nacionalne sigurnosti u Direktivi 2002/58

77. Nacionalna sigurnost (ili njezin istoznačan izraz „državna sigurnost", kao što se ističe u članku 15. stavku 1.) u Direktivi 2002/58 razmatra se na dvojak način. S jedne strane, ona je razlog za *isključenje* (iz primjene te direktive) svih aktivnosti država članica koje osobito „imaju za cilj" tu nacionalnu sigurnost. S druge strane, ona je razlog za *ograničenje*, koje se provodi zakonom, prava i obveza utvrđenih Direktivom 2002/58, odnosno u pogledu aktivnosti privatne ili trgovačke prirode koje nisu povezane s područjem regalnih aktivnosti [41].

78. Na koje se aktivnosti odnosi članak 1. stavak 3. Direktive 2002/58? Prema mojem mišljenju, sam Conseil d'État (Državno vijeće, Francuska) pruža dobar primjer kad navodi članke L. 851-5 i L. 851-6 Zakonika o unutarnjoj sigurnosti, pri čemu upućuje na „tehnike prikupljanja informacija koje država izravno primjenjuje, ali kojima se ne uređuju aktivnosti pružatelja elektroničkih komunikacijskih usluga na način da im se propisuju posebne obveze" [42].

79. Smatram da je to ključno za utvrđivanje opsega isključenja iz članka 1. stavka 3. Direktive 2002/58. Njezinim sustavom nisu obuhvaćene *aktivnosti* koje, s ciljem zaštite nacionalne sigurnosti, samostalno obavljaju tijela javne vlasti, a da pritom od pojedinaca ne zahtijevaju suradnju te im stoga ne nalažu obveze u upravljanju njihovim poslovanjem.

39 Naime, teško bi bilo tvrditi da se člankom 15. stavkom 1. Direktive 2002/58 omogućuje ograničavanje utvrđenih prava i obveza koje propisuje u području, kao što je nacionalna sigurnost, koje bi u načelu bilo izvan njezina područja primjene, na temelju članka 1. stavka 3. same Direktive. Kao što je to Sud potvrdio u točki 73. presude Tele2 Sverige i Watson, članak 15. stavak 1. Direktive 2002/58 „nužno pretpostavlja da nacionalne mjere koje su [njime] predviđene […] spadaju u područje primjene spomenute direktive jer potonja izričito ovlašćuje države članice da ih donesu samo uz poštovanje uvjeta koje predviđa".

40 Presuda Tele2 Sverige i Watson, t. 67.

41 Kao što je to podredno istaknuo nezavisni odvjetnik H. Saugmandsgaard Øe u svojem mišljenju u predmetu Ministerio Fiscal (C-207/16, EU:C:2018:300, t. 47.), „ne treba miješati, s jedne strane, osobne podatke koji se *izravno* obrađuju u okviru suverenih aktivnosti države, u području koje je obuhvaćeno kaznenim pravom i, s druge strane, osobne podatke koji se obrađuju u okviru poslovnih aktivnosti pružatelja usluga elektroničkih komunikacija koje *potom* upotrebljavaju nadležna državna tijela".

42 Točke 18. i 21. odluke kojom se upućuje zahtjev za prethodnu odluku u predmetu C-511/18

80. Međutim, popis aktivnosti tijela javne vlasti koje se isključuju iz općeg sustava obrade osobnih podataka treba tumačiti restriktivno. Konkretno, pojam *nacionalne sigurnosti*, za koju su odgovorne isključivo države članice u skladu s člankom 4. stavkom 2. UEU-a, ne može se proširiti na druge sektore koji su više ili manje bliski javnom životu.

81. Budući da se ova prethodna pitanja odnose na uključenost pojedinaca (odnosno osoba koje korisnicima pružaju elektroničke komunikacijske usluge), a ne na puku intervenciju državnih tijela, nije nužno detaljnije utvrditi okvire nacionalne sigurnosti *stricto sensu*.

82. Smatram međutim da kao smjernica može poslužiti kriterij iz Okvirne odluke 2006/960/PUP [43], u čijem se članku 2. točki (a) razlikuju tijela zadužena za izvršavanje zakona u širem smislu, koja obuhvaćaju, s jedne strane, „nacionalno policijsko, carinsko ili drugo tijelo koje je ovlašteno na temelju nacionalnog zakonodavstva otkrivati, sprečavati i provoditi istrage o kaznenim djelima ili kriminalnim aktivnostima, te izvršavati ovlaštenja i provoditi prisilne mjere u okviru takvih radnji" i, s druge strane, „[a]gencije ili službe zadužene posebno za pitanja nacionalne sigurnosti" [44].

83. U uvodnoj izjavi 11. Direktive 2002/58 utvrđuje se da „poput Direktive 95/46 […], ova Direktiva ne obuhvaća pitanja zaštite temeljnih prava i sloboda koje se odnose na aktivnosti koje nisu uređene pravom [Unije]". Stoga se Direktivom 2002/58 „ne mijenja postojeća ravnoteža između prava na privatnost pojedinca i mogućnosti država članica da poduzmu mjere iz članka 15. stavka 1. ove Direktive, koje su nužne za zaštitu […] državne sigurnosti […]".

84. Postoji naime kontinuitet između Direktive 95/46 i Direktive 2002/58 u pogledu nadležnosti država članica za nacionalnu sigurnost. Predmet nijedne od tih dviju direktiva nije zaštita temeljnih prava u tom posebnom području, u kojem aktivnosti država članica nisu „uređene pravom [Unije]".

85. „Ravnoteža" na koju se odnosi ta uvodna izjava proizlazi iz potrebe da se poštuju nadležnosti država članica u području nacionalne sigurnosti kad ih izvršavaju *izravno i vlastitim sredstvima*. Suprotno tomu, kad se, uključujući zbog istih razloga nacionalne sigurnosti, zahtijeva sudjelovanje pojedinaca, kojima se nalažu određene obveze, tom se okolnošću određuje ulazak u neko područje (zaštita privatnosti koju zahtijevaju ti privatni sudionici) uređeno pravom Unije.

86. Direktivom 95/46 i Direktivom 2002/58 nastoji se postići ta ravnoteža na način da se njima dopušta da se prava pojedinaca ograniče na temelju regulatornih mjera koje su donijele države članice u skladu s, redom, njezinim člankom 13. stavkom 1. i člankom 15. stavkom 1. U tom pogledu nema nikakve razlike između dviju direktiva.

87. Što se tiče Uredbe br. 2016/679, kojom se uspostavlja (novi) opći okvir za zaštitu osobnih podataka, njezinim se člankom 2. stavkom 2. isključuje „obrada osobnih podataka" kad države članice „obavljaju aktivnosti koje su obuhvaćene područjem primjene glave V. poglavlja 2. UEU-a".

43 Okvirna odluka Vijeća od 18. prosinca 2016. o pojednostavljenju razmjene informacija i obavještajnih podataka između tijela zaduženih za izvršavanje zakona u državama članicama Europske unije (SL 2006., L 386, str. 89.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 19., svezak 8., str. 140.)

44 U istom se smislu člankom 1. stavkom 4. Okvirne odluke Vijeća 2008/977/PUP od 27. studenoga 2008. o zaštiti osobnih podataka obrađenih u okviru policijske i pravosudne suradnje u kaznenim stvarima (SL 2008., L 350, str. 60.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 16., svezak 2., str. 118.) predviđalo da ta odluka „ne dovodi u pitanje osnovne interese nacionalne sigurnosti i specifičnih obavještajnih aktivnosti u području nacionalne sigurnosti".

88. Kao što se u Direktivi 95/46 obrada osobnih podataka kvalificirala samo s obzirom na svoju svrhu, neovisno o subjektu koji je obavlja, u Uredbi br. 2016/679 isključeni postupci obrade utvrđuju se s obzirom na svoju svrhu i osobe koje je obavljaju: isključuju se obrade koje obavljaju države članice tijekom *djelatnosti* koja nije obuhvaćena opsegom prava Unije (članak 2. stavak 2. točke (a) i (b)) i koje obavljaju tijela *u svrhu sprečavanja kaznenih djela i u svrhu zaštite* od prijetnji javnoj sigurnosti [45].

89. Utvrđivanje tih aktivnosti tijela javne vlasti treba nužno biti restriktivno, kako se propisi Unije u području zaštite privatnosti ne bi lišili učinkovitosti. Člankom 23. Uredbe br. 2016/679, u vezi s člankom 15. stavkom 1. Direktive 2002/58, predviđa se ograničavanje, *zakonskom mjerom*, njome utvrđenih prava i obveza, kad je potrebna zaštita, među ostalim ciljevima, nacionalne sigurnosti, obrane ili javne sigurnosti. Ponavljam, ako je zaštita tih ciljeva dovoljna kako bi se utvrdilo isključenje iz područja primjene Uredbe br. 2016/679, pozivanje na nacionalnu sigurnost kao opravdanje za ograničavanje, zakonskom mjerom, prava utvrđenih tom uredbom bilo bi suvišno.

90. Kao što je to slučaj s Direktivom 2002/58, ne bi bilo logično da zakonske mjere predviđene člankom 23. Uredbe br. 2016/679 (kojim se, ponavljam, odobravaju državna ograničenja pravâ na privatnost građana zbog razloga nacionalne sigurnosti) ulaze u njezino područje primjene i, istodobno, da zbog obuhvaćenosti nacionalne sigurnosti sama Uredba jednostavno postane neprimjenjiva, što bi značilo nepostojanje bilo kakvog priznavanja subjektivnog prava.

B. Potvrda i mogućnosti razvoja sudske prakse uspostavljene presudom Tele2 Sverige i Watson

91. U svojem mišljenju u predmetu C-520/18 provodim detaljnu analizu [46] sudske prakse Suda u tom području, na temelju koje istodobno predlažem njezino potvrđivanje i određeni oblik tumačenja za preciziranje njezina sadržaja.

92. Upućujem na tu analizu za koju smatram da je ovdje nije nužno prenijeti zbog puke jezične ekonomije. Razmatranja koja ću u nastavku iznijeti u pogledu prethodnih pitanja koja je uputio Conseil d'État (Državno vijeće) stoga treba tumačiti uzimajući u obzir odgovarajuće odlomke iz mišljenja u predmetu C-520/18.

C. Odgovor na prethodna pitanja

1. Obveza zadržavanja podataka (prvo prethodno pitanje u predmetima C-511/18 i C-512/18 te drugo prethodno pitanje u predmetu C-512/18)

93. Što se tiče obveze zadržavanja podataka koja se nalaže pružateljima elektroničkih komunikacijskih usluga, sud koji je uputio zahtjeve želi konkretno znati sljedeće:

– Čini li ta obveza, čije se ispunjavanje zahtijeva u skladu s člankom 15. stavkom 1. Direktive 2002/58, zadiranje koje je opravdano „pravom na sigurnost" zajamčenim člankom 6. Povelje i zahtjevima nacionalne sigurnosti (prvo pitanje u predmetima C-511/18 i C-512/18, kao i treće pitanje u predmetu C-511/18).

– Odobrava li se Direktivom 2000/31 zadržavanje podataka koji omogućuju identifikaciju bilo koje osobe koja je doprinijela stvaranju sadržaja dostupnih javnosti na internetu (drugo pitanje u predmetu C-512/18).

45 Naime, Uredbom br. 2016/679 isključuje se obrada podataka koju obavljaju države članice tijekom *djelatnosti* koja nije obuhvaćena opsegom prava Unije, uz obradu koju obavljaju tijela *u svrhu zaštite* javne sigurnosti.

46 Točke 27. do 68.

a) Uvodna razmatranja

94. Conseil d'État (Državno vijeće) poziva se na temeljna prava priznata člancima 7. (poštovanje privatnog i obiteljskog života), 8. (zaštita osobnih podataka) i 11. (sloboda izražavanja i informiranja) Povelje. Naime, to su prava u koja bi se, prema mišljenju Suda, moglo zadirati obvezom zadržavanja podataka o prometu koju nacionalna tijela nalažu pružateljima elektroničkih komunikacijskih usluga [47].

95. Sud koji je uputio zahtjeve upućuje i na pravo na sigurnost koje se štiti člankom 6. Povelje. Na njega se ne poziva toliko kao na pravo koje bi moglo biti ugroženo, koliko kao na čimbenik kojim bi se moglo opravdati nalaganje te obveze.

96. Slažem se s Komisijom u pogledu toga da pozivanje na članak 6. u tim uvjetima može biti dvosmisleno. Kao i Komisija, smatram da tu odredbu ne treba tumačiti na način da se njome „Uniji [može] naložiti pozitivna obveza donošenja mjera za zaštitu pojedinaca od kaznenih djela" [48].

97. Sigurnost zajamčena tim člankom Povelje ne izjednačava se s javnom sigurnosti. Odnosno, drugim riječima, povezana je s potonjom javnom sigurnosti kao i svako drugo temeljno pravo, s obzirom na to da je javna sigurnost neophodan uvjet za ostvarivanje temeljnih prava i sloboda.

98. Kao što podsjeća Komisija, članak 6. Povelje odgovara članku 5. Europske konvencije o ljudskim pravima (u daljnjem tekstu: EKLJP), kao što se to navodi u popratnim objašnjenjima. Iz teksta članka 5. EKLJP-a proizlazi da je „sigurnost", koja se tim člankom štiti, osobna sigurnost u užem smislu, koja se shvaća kao jamstvo prava na fizičku slobodu u odnosu na proizvoljno uhićenje ili pritvaranje. U konačnici, riječ je o sigurnosti da se nitko ne smije lišiti slobode, osim u slučajevima, uvjetima i postupku propisanim zakonom.

99. Stoga je riječ o *osobnoj sigurnosti*, koja se odnosi na uvjete u kojima se može ograničiti fizička sloboda osoba [49], a ne o *javnoj sigurnosti* koja je svojstvena postojanju države, što je u razvijenom društvu neophodna pretpostavka za usklađivanje izvršavanja javnih ovlasti s ostvarivanjem prava pojedinaca.

100. Međutim, neke vlade traže da se više uzme u obzir pravo na sigurnost u drugonavedenom smislu. Naime, Sud nije zanemario tu sigurnost, štoviše, izričito ju je naveo u svojim presudama [50] i mišljenjima [51]. Nikad nije osporio važnost ciljeva u općem interesu koji se odnose na zaštitu nacionalne sigurnost i javnog poretka [52], borbu protiv međunarodnog terorizma radi održavanja međunarodnog mira i sigurnosti i borbu protiv teških kaznenih djela radi osiguranja javne sigurnost [53], koju je pravilno kvalificirao kao „primarnu" [54]. Kao što je svojedobno istaknuo, „zaštita javne sigurnosti pridonosi i zaštiti prava i sloboda drugih osoba" [55].

101. Prilika koju pružaju predmetni zahtjevi za prethodnu odluku mogla bi se iskoristiti za jasnije predlaganje uspostavljanja ravnoteže između, s jedne strane, prava na sigurnost i, s druge strane, prava na privatnost i prava na zaštitu osobnih podataka. Tako bi se izbjegli prigovori da se drugonavedenim pravima daje prednost u odnosu na prvonavedeno pravo.

47 U tom pogledu, presuda Tele2 Sverige i Watson, t. 92., uz upućivanje, po analogiji, na presudu Digital Rights, t. 25. i 70.

48 Točka 37. Komisijinih pisanih očitovanja

49 Tako to tumači ESLJP. U pogledu toga vidjeti presudu od 5. srpnja 2016., Buzadji protiv Republike Moldove, ECHR:2016:0705JUD002375507, u čijoj se točki 84. tvrdi da je glavni cilj prava priznatog člankom 5. EKLJP-a spriječiti proizvoljno ili neopravdano oduzimanje slobode pojedincu.

50 Presuda Digital Rights, t. 42.

51 Mišljenje 1/15 (Sporazum PNR EU-Kanada) od 26. srpnja 2017. (u daljnjem tekstu: Mišljenje 1/15, EU:C:2017:592, t. 149. i navedena sudska praksa)

52 Presuda od 15. veljače 2016., N. (C-601/15 PPU, EU:C:2016:84, t. 53.)

53 Presuda Digital Rights, t. 42. i navedena sudska praksa.

54 *Ibidem*, t. 51.

55 Mišljenje 1/15, t. 149.

102. Smatram da se na tu ravnotežu upućuje u uvodnoj izjavi 11. i u članku 15. stavku 1. Direktive 2002/58, u dijelu u kojem se odnose na zahtjeve nužnosti i razmjernosti mjera *unutar demokratskog društva*. Ponavljam, pravo na sigurnost svojstveno je samom postojanju i održivosti demokracije, čime se opravdava njegovo potpuno uzimanje u obzir u kontekstu ocjene te proporcionalnosti. Drugim riječima, iako je zaštita načela povjerljivosti podataka primarna u demokratskom društvu, ne treba podcijeniti ni važnost njegove sigurnosti.

103. Stoga kontekst koji uključuje ozbiljne i kontinuirane prijetnje nacionalnoj sigurnosti i osobito rizik terorističkih napada treba uzeti u obzir u skladu s navedenim u zadnjoj rečenici točke 119. presude Tele2 Sverige i Watson. Nacionalni sustav može odgovoriti na način koji je proporcionalan prirodi i ozbiljnosti prijetnji s kojima se suočava, a da pritom taj odgovor ne mora nužno biti istovjetan onome u drugim državama članicama.

104. U konačnici, moram dodati da prethodna razmatranja nisu prepreka tomu da se nacionalnim zakonodavstvom, u *iznimnim* situacijama u pravom smislu riječi, koje uključuju neposrednu prijetnju ili izvanredni rizik kojima se opravdava službeno proglašenje krizne situacije u državi članici, na ograničeno vrijeme predvidi mogućnost propisivanja toliko široke i opće obveze zadržavanja podataka koliko se to smatra nužnim [56].

105. Stoga bi prvo pitanje iz obaju zahtjeva za prethodnu odluku trebalo preoblikovati na način da se više usmjeri na mogućnost da se zadiranje opravda razlozima nacionalne sigurnosti. Stoga bi se dvojba odnosila na to je li obveza koja se nalaže pružateljima elektroničkih komunikacijskih usluga u skladu s člankom 15. stavkom 1. Direktive 2002/58.

b) Ocjena

1) Određivanje nacionalnih pravila, kako su navedena u obama zahtjevima za prethodnu odluku, s obzirom na sudsku praksu Suda

106. Uzimajući u obzir odluke kojima se upućuju zahtjevi za prethodnu odluku, spornim propisom u glavnim postupcima propisuje se obveza zadržavanja podataka:

– operatorima elektroničkih komunikacija i osobito osobama koje nude pristup javnim internetskim komunikacijskim uslugama; i

– fizičkim ili pravnim osobama koje, čak i besplatno, za stavljanje na raspolaganje javnosti na internetu, osiguravaju pohranu bilo koje vrste signala, pisanog teksta, slika, zvukova ili poruka, a koji su dobiveni od primatelja tih usluga [57].

107. Operatori tijekom jedne godine od dana njihova zapisa trebaju zadržati podatke na temelju kojih se može identificirati korisnik, podatke o korištenoj komunikacijskoj terminalnoj opremi, tehničke značajke, datum, vrijeme i trajanje svakog poziva, podatke o zatraženim ili upotrijebljenim dodatnim uslugama i njihovim pružateljima, kao i podatke koji omogućuju identifikaciju primatelja komunikacije i, u slučaju djelatnosti telefonije, podatke koji omogućuju utvrđivanje izvora i lokacije komunikacije [58].

56 Vidjeti točke 105. do 107. mojega mišljenja u predmetu C-520/18.

57 Tako proizlazi iz članka L. 851-1 Zakonika o unutarnjoj sigurnosti, u kojem se upućuje na članak L. 34-1 Zakonika o pošti i elektroničkim komunikacijama i članak 6. zakona br. 2004-575 za promicanje povjerenja u digitalnu ekonomiju.

58 Tako je navedeno u članku R. 10-13 Zakonika o pošti i elektroničkim komunikacijama.

108. Kad je osobito riječ o uslugama pristupa internetu i uslugama pohrane, čini se da se nacionalnim propisom zahtijeva zadržavanje IP adresa [59], lozinki i, ako je sklopljen ugovor ili izrađen račun za plaćanje, podataka o načinu izvršenog plaćanja, kao i referentnog broja plaćanja, iznosa, datuma i vremena transakcije [60].

109. Ta se obveza zadržavanja zahtijeva u svrhu istrage, otkrivanja i progona kaznenih djela [61]. Drugim riječima, za razliku od, kao što će se to pokazati, obveze *prikupljanja* podataka o prometu i lokaciji, cilj obveze njihova *zadržavanja* nije isključivo sprečavanje terorizma [62].

110. Što se tiče uvjeta *pristupa* zadržanim podacima, iz informacija pruženih u odlukama kojima se upućuju zahtjevi za prethodnu odluku proizlazi da se predviđaju za zajednički sustav (intervencija sudskog tijela) ili da je taj pristup ograničen na pojedinačno imenovane i ovlaštene službenike, nakon odobrenja premijera donesenog na temelju neobvezujućeg mišljenja neovisnog upravnog tijela [63].

111. Nije teško primijetiti da, kao što je to istaknula Komisija [64], podaci čije se zadržavanje zahtijeva nacionalnim pravilima u biti odgovaraju podacima koje je Sud ispitivao u presudama Digital Rights i Tele2 Sverige i Watson [65]. Kao i tada, ti su podaci predmet „obvez[e] općeg i neselektivnog zadržavanja podataka", kao što to potpuno otvoreno ističe Conseil d'État (Državno vijeće) na početku svojih prethodnih pitanja.

112. Ako je to slučaj, što u konačnici treba ocijeniti sud koji je uputio zahtjeve, može se samo zaključiti da predmetni propis podrazumijeva „[m]iješanje […] u temeljna prava utvrđena člancima 7. i 8. Povelje [koje je] širokog dosega i treba ga smatrati osobito ozbiljnim" [66].

113. Nijedna od zainteresiranih stranaka nije dovela u pitanje to da takav propis podrazumijeva zadiranje u navedena prava. Sada se nije potrebno zadržavati na tom pitanju, čak niti kako bi se podsjetilo da povreda tih prava neizbježno ugrožava same temelje nekog društva koje nastoji poštovati, među ostalim vrijednostima, osobnu privatnost zajamčenu Poveljom.

114. Primjena sudske prakse uspostavljene presudom Tele2 Sverige i Watson i potvrđene presudom Ministerio Fiscal svakako navodi na zaključak da sporni propis „prelazi […] granice strogo nužnog i ne može se smatrati opravdanim u demokratskom društvu, kao što to zahtijeva članak 15. stavak 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. i člankom 52. stavkom 1. Povelje" [67].

115. Naime, kao i propis koji se analizira u presudi Tele2 Sverige i Watson, propis o kojem je ovdje riječ također „na općenit način obuhvaća sve pretplatnike i registrirane korisnike te se odnosi na sva sredstva elektroničke komunikacije kao i na sve podatke o prometu, ne predviđa nikakvo razlikovanje, ograničenje ili iznimku s obzirom na cilj koji se želi postići" [68]. Posljedično, on se „primjenjuje i na

59 Na sudu je koji je uputio zahtjeve da provjeri to pitanje, u pogledu kojeg su na raspravi iznesena suprotstavljena stajališta.

60 Članak 1. Uredbe br. 2011-219

61 Članak R. 10-13 Zakonika o pošti i elektroničkim komunikacijama

62 La Quadrature du Net i Fédération des founisseurs d'accès á Internet associatifs ističu opseg svrha kojima služi zadržavanje, ovlast diskrecijske ocjene dodijeljene tijelima, nepostojanje objektivnih kriterija u njezinu definiranju i važnost oblika kaznenih djela koja se ne mogu kvalificirati kao teška.

63 Commission nationale de contrôle des techniques de renseignement (Nacionalna komisija za nadzor nad tehnikama prikupljanja podataka, Francuska). Vidjeti u tom pogledu točke 145. i 148. pisanih očitovanja francuske vlade.

64 Točka 60. Komisijinih pisanih očitovanja

65 U tim se presudama zapravo ide korak dalje, s obzirom na to da se u njima također razmatra, u slučaju usluga pristupa internetu, zadržavanje IP adrese ili lozinki.

66 Presuda Tele2 Sverige i Watson, t. 100.

67 *Ibidem*, t. 107.

68 *Ibidem*, t. 105.

osobe za koje ne postoji nikakva naznaka koja bi navela na mišljenje da njihovo ponašanje može imati vezu, čak i posrednu ili daleku, s teškim kaznenim djelima" i to na način da se njime ne predviđa nikakva iznimka „pa se primjenjuje i na osobe čije su komunikacije prema pravilima nacionalnog prava podvrgnute profesionalnoj tajni"[69].

116. Tako se spornim propisom također „ne zahtijeva nikakav odnos između podataka čije je zadržavanje propisano i prijetnje javnoj sigurnosti. Posebice, on nije ograničen na zadržavanje podataka iz jednog privremenog razdoblja i/ili jednog određenog zemljopisnog područja i/ili jednog kruga osoba koje mogu na bilo koji način biti umiješane u teško kazneno djelo ili na osobe koje, ako se zadrže njihovi podaci, mogu zbog drugih razloga doprinijeti borbi protiv kriminaliteta"[70].

117. Iz prethodno navedenog proizlazi da taj propis „prelazi […] granice strogo nužnog i ne može se smatrati opravdanim u demokratskom društvu, kao što to zahtijeva članak 15. stavak 1. Direktive 2002/58, u vezi s člancima 7., 8. i 11. i člankom 52. stavkom 1. Povelje"[71].

118. Prethodno navedeno bilo je dovoljno da Sud zaključi da istovjetna nacionalna pravila nisu u skladu s člankom 15. stavkom 1. Direktive 2002/58 jer se njima „u cilju borbe protiv kriminaliteta određuje opće i neselektivno zadržavanje svih podataka o prometu i lokaciji svih pretplatnika i registriranih korisnika u pogledu svih sredstava elektroničke komunikacije"[72].

119. Sada se pak postavlja pitanje može li se sudska praksa Suda u području zadržavanja osobnih podataka, ako ne izmijeniti, barem prilagoditi ako je cilj koji se nastoji postići tim „općim i neselektivnim" zadržavanjem borba protiv terorizma. Prvo pitanje u predmetu C-511/18 upravo je sastavljeno „u kontekstu koji uključuje ozbiljne i kontinuirane prijetnje nacionalnoj sigurnosti, i osobito rizik terorističkih napada".

120. Međutim, iako je to *činjenični okvir* u kojem se propisuje obveza zadržavanja podataka, točno je da se *pravni okvir* tog pravila ne odnosi isključivo na terorizam. U sustavu zadržavanja podataka i pristupa podacima o kojem se raspravlja u postupku pred Conseil d'État (Državno vijeće) ta se obveza općenito uvjetuje svrhom istrage, otkrivanja i progona kaznenih djela.

121. U svakom slučaju, podsjećam da borba protiv terorizma nije izostavljena iz argumentacije u presudi Tele2 Sverige i Watson, pri čemu Sud tada nije smatrao da je za taj oblik kaznenog djela potreban neki otklon u njegovoj sudskoj praksi[73].

122. Stoga, i u načelu, smatram da na pitanje suda koji je uputio zahtjeve, a koje se usredotočuje na posebnost terorističke prijetnje, treba odgovoriti na isti način kao što je Sud odlučio u presudi Tele2 Sverige i Watson.

123. Kao što sam to tvrdio u mišljenju u predmetu Stichting Brein, „[i]zvjesnost u primjeni prava možda ne nalaže pravosudnim tijelima primjenu *stare decisis* u apsolutnom smislu, ali od njih svakako zahtijeva da budu razboriti i da se pridržavaju odluka koje su, nakon zrelog razmišljanja o konkretnom pravnom problemu, sama donijela"[74].

69 *Loc. ult. cit.*

70 Presuda Tele2 Sverige i Watson, t. 106.

71 *Ibidem*, t. 107.

72 *Ibidem*, t. 112.

73 *Ibidem*, t. 103.

74 Predmet C-527/15, EU:C:2016:938, t. 41.

2) Ograničeno zadržavanje podataka zbog prijetnji nacionalnoj sigurnosti, uključujući terorističku prijetnju

124. Međutim, je li moguće prilagoditi ili nadopuniti tu sudsku praksu, s obzirom na njezine posljedice za borbu protiv terorizma ili za zaštitu države od drugih sličnih prijetnji nacionalnoj sigurnosti?

125. Već sam istaknuo da samo zadržavanje osobnih podataka podrazumijeva zadiranje u prava zajamčena člancima 7., 8. i 11. Povelje[75]. Neovisno o tome što se njime, u konačnici, nastoji omogućiti retrospektivni ili istodobni *pristup* podacima u određenom trenutku[76], samo zadržavanje podataka kojima se prekoračuje ono što je nužno za prijenos komunikacije ili naplatu usluga koje pruža pružatelj pretpostavlja povredu granica predviđenih u člancima 5. i 6. Direktive 2002/58.

126. Korisnici tih usluga (zapravo, gotovo svi građani u najrazvijenijim društvima) imaju ili trebaju imati legitimno očekivanje u smislu da se njihovi podaci, ako ne daju svoj pristanak, više neće zadržavati, osim onih pohranjenih u skladu s tim odredbama. Iznimke iz članka 15. stavka 1. Direktive 2002/58 trebaju se tumačiti s obzirom na tu pretpostavku.

127. Kao što sam to već objasnio, Sud je u presudi Tele2 Sverige i Watson, također u pogledu borbe protiv terorizma, odbio mogućnost općeg i neselektivnog zadržavanja osobnih podataka[77].

128. S obzirom na dobivene kritike, ne smatram da se sudskom praksom uspostavljenom tom presudom podcjenjuje teroristička prijetnja, kao osobito težak oblik kriminaliteta koji podrazumijeva izričitu namjeru osporavanja autoriteta države i destabilizacije ili uništavanja njezinih institucija. Borba protiv terorizma doslovno je ključna za državu i njezin uspjeh, što je cilj u općem interesu kojeg se ne može odreći država koja se temelji na vladavini prava.

129. Gotovo su sve zainteresirane vlade u postupku, osim Komisije, istaknule da bi se, ne uzimajući u obzir njegove tehničke poteškoće, djelomičnim i ciljanim zadržavanjem osobnih podataka nacionalne obavještajne službe lišile mogućnosti pristupa informacijama koje su nužne za identificiranje prijetnji javnoj sigurnosti i obrani države, kao i za kazneni progon počinitelja terorističkih napada[78].

130. Kad je riječ o toj ocjeni, čini mi se važnim istaknuti da borbu protiv terorizma ne treba razmatrati samo u odnosu na njezinu učinkovitost. Otuda proizlaze poteškoće u pogledu borbe protiv terorizma, ali i njezin uspjeh kad se ta borba odvija sredstvima i metodama koje su u skladu sa zahtjevima vladavine prava, a to je prije svega zahtjev da vlast i moć podliježu granicama prava i, osobito, pravnom poretku čiji su razlog i svrha postojanja zaštita temeljnih prava.

75 Kao što je Sud podsjetio u točki 124. Mišljenja 1/15, „dostavljanje osobnih podataka trećoj osobi, primjerice javnom tijelu, predstavlja zadiranje u temeljno pravo predviđeno člankom 7. Povelje, neovisno o kasnijem korištenju dostavljenim informacijama. Isto vrijedi i za čuvanje osobnih podataka te za pristup tim podacima kako bi se njima koristila javna tijela. U tom je pogledu nevažno imaju li dotične informacije o privatnom životu osjetljiv karakter, odnosno jesu li zainteresirane osobe zbog tog zadiranja pretrpjele eventualne neugodnosti”.

76 Kao što je nezavisni odvjetnik P. Cruz Villalón istaknuo u mišljenju u predmetu Digital Rights, C-293/12 i C-594/12 (EU:C:2013:845, t. 72.), „prikupljanje i osobito zadržavanje u golemim bazama podataka brojnih podataka koji su dobiveni ili obrađeni u okviru najvećeg djela tekućih elektroničkih komunikacija građana Unije predstavlja ozbiljno miješanje u njihov privatan život, čak i kada samo stvaraju moguće uvjete za retrospektivan nadzor njihovih kako osobnih tako i profesionalnih djelovanja. Prikupljanje tih podataka stvara uvjete za nadzor koji, da se i izvršava samo retrospektivno prilikom njihovog iskorištavanja, ipak predstavlja stalnu prijetnju tijekom cijelog trajanja razdoblja njihovog zadržavanja pravu građana Unije na tajnost njihovog privatnog života. Rasprostranjeni osjećaj nastalog nadzora postavlja posebno akutno pitanje o trajanju zadržavanja podataka.”

77 Presuda Tele2 Sverige i Watson, t. 103.: „ne može […] opravdati da se nacionalni propis koji određuje opće i neselektivno zadržavanje svih podataka o prometu i lokaciji smatra nužnim u svrhu navedene borbe”.

78 Tako to tumači, na primjer, francuska vlada koja tu tvrdnju potkrepljuje konkretnim primjerima korisnosti općeg zadržavanja podataka koje je državi omogućilo da reagira na ozbiljne terorističke napade koji su se dogodili u Francuskoj posljednjih godina (točka 107. i točke 122. do 126. pisanih očitovanja francuske vlade).

131. Ako se, kad je riječ o terorizmu, za opravdanje njegovih sredstava u obzir uzima samo kriterij potpune (i maksimalne) učinkovitosti protiv njegovih napada na utvrđeni poredak, onda se, kad je riječ o vladavini prava, učinkovitost mjeri u uvjetima u kojima se, radi njezine obrane, ne dopušta zaobilaženje postupaka i jamstava na temelju kojih se kvalificira kao zakonit poredak. Jednostavnim ustupanjem pukoj učinkovitosti, vladavina prava izgubila bi sebi svojstveno obilježje te bi se, u izvanrednim slučajevima, mogla pretvoriti u prijetnju za građane. Ne postoji nikakvo jamstvo da, kad bi tijela javne vlasti raspolagala prekomjernim instrumentima za progon kaznenih djela, s pomoću kojih bi mogla zanemariti ili povrijediti temeljna prava, njihovo nekontrolirano i potpuno slobodno postupanje u konačnici ne bi ugrozilo slobodu svih osoba.

132. Ponavljam, učinkovitost tijela javne vlasti nailazi na nepremostivu prepreku u vidu temeljnih prava građana, čija se ograničenja, kao što se to propisuje člankom 52. stavkom 1. Povelje, mogu provesti samo zakonom i u skladu s njihovim bitnim sadržajem „ako su potrebna i ako zaista odgovaraju ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba”[79].

133. Na uvjete u kojima se, u skladu s presudom Tele2 Sverige i Watson, dopušta *ciljano* zadržavanje podataka upućujem u svojem mišljenju u predmetu C-520/18[80].

134. Okolnosti u kojima, na temelju informacija kojima raspolažu obavještajne službe, postoji osnovana sumnja u pogledu pripreme terorističkog napada mogu biti legitiman slučaj u kojem se propisuje obveza zadržavanja određenih podataka. Taj slučaj tim više može biti stvarno počinjenje napada. Iako, u potonjem slučaju, počinjenje kaznenog djela samo po sebi može biti opravdavajući kriterij za donošenje te mjere, u slučaju puke sumnje u moguće počinjenje napada, okolnosti na kojima se temelji ta sumnja trebale bi ispunjavati minimalni stupanj vjerodostojnosti koji je neophodan za objektivno odvagivanje indicija kojima se ona može opravdati.

135. Iako je teško, nije nemoguće detaljno i u skladu s objektivnim kriterijima utvrditi kategorije podataka, čije se zadržavanje smatra nužnim, kao i krug dotičnih osoba. Točno je da bi *najpraktičnije* i *najučinkovitije* bilo opće i neselektivno zadržavanje svih podataka koje pružatelji elektroničkih komunikacijskih usluga mogu prikupiti, ali već sam istaknuo da se pitanje ne može riješiti s obzirom na *praktičnu* nego na *pravnu učinkovitost*, i u kontekstu vladavine prava.

136. Taj je zadatak utvrđivanja u pravilu zakonodavni, u okviru granica utvrđenih sudskom praksom Suda. Ponovno upućujem na razmatranja koja u tom pogledu iznosim u svojem mišljenju u predmetu C-520/18[81].

79 Presuda od 15. veljače 2016., N. (C-601/15 PPU, EU:C:2016:84, t. 50.) Stoga je riječ o osjetljivoj ravnoteži između javnog poretka i slobode na koju sam već uputio i koja se u načelu nastoji uspostaviti svim propisima Unije. Kao primjer može poslužiti Direktiva (EU) 2017/541 Europskog parlamenta i Vijeća od 15. ožujka 2017. o suzbijanju terorizma i zamjeni Okvirne odluke Vijeća 2002/475/PUP i o izmjeni Odluke Vijeća 2005/671/PUP (SL 2017., L 88, str. 6. i ispravak SL 2018., L 119, str. 41.). Dok se u njezinu članku 20. stavku 1. navodi da države članice trebaju osigurati da „djelotvorni istražni instrumenti […] budu dostupni” osobama koje su odgovorne za istragu ili kazneni progon kaznenih djela terorizma, njezinom se uvodnom izjavom 21. propisuje da bi se takvim instrumentima trebalo koristiti „ciljano i uzimajući u obzir načelo proporcionalnosti te prirodu i ozbiljnost kaznenih djela koja se istražuju, te bi se tim korištenjem trebalo poštovati pravo na zaštitu osobnih podataka”.

80 Točke 87. do 95.

81 Točke 100. do 107.

3) Pristup zadržanim podacima

137. Polazeći od pretpostavke da su operatori prikupili podatke u skladu s odredbama Direktive 2002/58 i da su zadržani u skladu s člankom 15. stavkom 1.[82], pristup nadležnih tijela tim informacijama treba provesti pod uvjetima koje je Sud zahtijevao i koje analiziram u mišljenju u predmetu C-520/18 na koje upućujem[83].

138. Stoga se i u ovom slučaju nacionalnim propisom moraju predvidjeti materijalni i postupovni uvjeti kojima se uređuje pristup nadležnih tijela zadržanim podacima[84]. U okviru predmetnih zahtjeva za prethodnu odluku, tim bi se uvjetima odobrio pristup podacima o osobama za koje postoji sumnja da namjeravaju počiniti, da će počiniti ili su počinile teroristički čin ili da su sudjelovale u tom činu[85].

139. Međutim, bitno je da pristup predmetnim podacima, osim u valjano opravdanim hitnim slučajevima, bude podvrgnut prethodnom nadzoru suda ili neovisnog upravnog tijela i da odluka tog suda ili tijela bude donesena nakon obrazloženog zahtjeva nadležnih tijela[86]. Na taj način, u slučajevima u kojima nije moguće donijeti odluku na temelju apstraktnog zakona, jamči se odluka *in concreto* tog neovisnog tijela, koje je jednako obvezano jamstvom nacionalne sigurnosti i zaštitom temeljnih prava građana.

4) Obveza zadržavanja podataka koji omogućuju identifikaciju autorâ sadržaja, s obzirom na Direktivu 2000/31 (drugo prethodno pitanje u predmetu C-512/18)

140. Sud koji je uputio zahtjeve upućuje na Direktivu 2000/31 kao polazišnu točku za utvrđivanje mogu li se određene osobe[87] i operatori koji pružaju javne komunikacijske usluge obvezati na to da zadrže podatke „koji omogućuju identifikaciju bilo koje osobe koja je doprinijela stvaranju sadržaja ili jednog od sadržaja usluga koje pružaju, kako bi sudsko tijelo moglo, po potrebi, zatražiti da mu se taj sadržaj dostavi u svrhu osiguravanja poštovanja pravila vezanih uz građansku ili kaznenu odgovornost”.

141. Slažem se s Komisijom da nije prikladno ispitivati usklađenost te obveze s Direktivom 2000/31[88], s obzirom na to da se člankom 1. stavkom 5. točkom (b) potonje direktive iz njezina područja primjene isključuju „pitanja vezana uz usluge informacijskog društva koje pokriva direktiva 95/46/EZ i 97/66/EZ”, odnosno pravila koja sad odgovaraju Uredbi br. 2006/679 i Direktivi 2002/58[89], čiji odnosni članak 23. stavak 1. i članak 15. stavak 1. treba tumačiti, prema mojem mišljenju, na ranije naveden način.

82 Pod uvjetom da se poštuju uvjeti navedeni u točki 122. presude Tele2 Sverige i Watson: Sud je podsjetio da se člankom 15. stavkom 1. Direktive 2002/58 ne omogućuje odstupanje od članka 4. stavka 1. kao ni od članka 4. stavka 1.a, kojima se od pružatelja zahtijeva da poduzmu mjere koje osiguravaju zaštitu zadržanih podataka od rizika zlouporabe i nezakonitog pristupa. U tom je smislu presudio da, „[k]ad je riječ o količini zadržanih podataka, njihovu osjetljivom karakteru i riziku od nezakonitog pristupa tim podacima, pružatelji elektroničkih komunikacijskih usluga moraju prikladnim tehničkim i organizacijskim mjerama, u svrhu osiguranja punog integriteta i povjerljivosti navedenih podataka, jamčiti osobito visoku razinu zaštite i sigurnosti. Nacionalni propis mora osobito propisati zadržavanje na području Unije kao i nepovratno uništenje podataka nakon isteka razdoblja njihova zadržavanja”.

83 Točke 52. do 60.

84 Presuda Tele2 Sverige i Watson, t. 118.

85 *Ibidem*, t. 119.

86 *Ibidem*, t. 120.

87 Osobe koje „[…] za stavljanje na raspolaganje javnosti putem javnih internetskih komunikacijskih usluga, osiguravaju pohranu bilo koje vrste signala, pisanog teksta, slika, zvukova ili poruka, a koji su dobiveni od primatelja tih usluga […]”.

88 Sud koji je uputio zahtjeve općenito i bez upućivanja na bilo koju odredbu navodi tu direktivu u drugom pitanju u predmetu C-512/18.

89 Točke 112. i 113. Komisijinih pisanih očitovanja

2. Obveza prikupljanja u stvarnom vremenu podataka o prometu i podataka o lokaciji (drugo prethodno pitanje u predmetu C-511/18)

142. Prema mišljenju suda koji je uputio zahtjeve, člankom L. 851-2 Zakonika o unutarnjoj sigurnosti odobrava se, isključivo u svrhe sprečavanja terorizma, prikupljanje u stvarnom vremenu podataka o unaprijed određenim pojedincima za koje se sumnja da su povezani s terorističkom prijetnjom. Na isti se način člankom L. 851-4 tog zakonika odobrava da operatori u stvarnom vremenu prenose samo tehničke podatke u pogledu lokacije terminalne opreme.

143. Prema mišljenju suda koji je uputio zahtjeve, tim se tehnikama pružateljima usluga ne nalaže dodatna obveza zadržavanja u odnosu na ono što je nužno za naplaćivanje i stavljanje na tržište njihovih usluga.

144. Osim toga, na temelju članka L. 851-3 Zakonika o unutarnjoj sigurnosti, operatorima elektroničkih komunikacija i pružateljima tehničkih usluga može se propisati obveza da „na svojim mrežama uspostave automatizirane obrade podataka namijenjene, u uvjetima određenim u odobrenju, utvrđivanju veza koje mogu upućivati na terorističku prijetnju”. Ta tehnika ne podrazumijeva opće i neselektivno zadržavanje podataka te je njezin cilj prikupljanje, tijekom ograničenog razdoblja, onih podataka o vezi koji mogu biti povezani s kaznenim djelom terorizma.

145. Prema mojem mišljenju, uvjeti koji se zahtijevaju za pristup zadržanim osobnim podacima trebaju se primjenjivati i na pristup u stvarnom vremenu podacima dobivenim u okviru elektroničkih komunikacija. Stoga upućujem na razmatranja o tom pitanju. Nije važno je li riječ o zadržanim podacima ili podacima dobivenim u stvarnom vremenu jer u oba slučaja dolazi do upoznavanja s osobnim podacima, neovisno o tome jesu li oni stari ili novi.

146. Konkretno, ako je pristup u stvarnom vremenu posljedica veza utvrđenih automatiziranom obradom, kao što je to navedeno u članku L. 851-3 Zakonika o unutarnjoj sigurnosti, nalaže se da unaprijed definirani modeli i kriteriji za tu obradu budu posebni, pouzdani i nediskriminirajući tako da omogućuju identifikaciju pojedinaca za koje se opravdano sumnja da sudjeluju u aktivnostima terorističke skupine [90].

3. Obveza obavješćivanja dotičnih osoba (treće prethodno pitanje u predmetu C-511/18)

147. Sud je utvrdio da tijela kojima je odobren pristup podacima o tome moraju obavijestiti dotične osobe, pod uvjetom da se time ne ugrožavaju istrage u tijeku. Ta se obveza temelji na tome da je navedena informacija nužna kako bi te osobe mogle ostvariti pravo na djelotvoran pravni lijek, koji je izričito naveden u članku 15. stavku 2. Direktive 2002/58, u slučaju povrede njihovih prava [91].

148. Svojim trećim pitanjem u predmetu C-511/18 Conseil d'État (Državno vijeće) želi znati je li taj zahtjev za pružanje informacija u svakom slučaju neophodan ili ih se može zahtijevati kad su predviđena druga jamstva, poput onih opisanih u njegovoj odluci kojom se upućuje zahtjev za prethodnu odluku.

149. U skladu s razmatranjima suda koji je uputio zahtjeve [92], navedena se jamstva odražavaju u mogućnosti da se osobe, koje žele provjeriti je li neka tehnika prikupljanja podataka primijenjena nezakonito, obrate samom Conseil d'État (Državno vijeće). To bi tijelo, po potrebi, moglo poništiti odobrenje mjere i naložiti uništavanje prikupljenih podataka, u okviru postupka kojim se ne predviđa načelo uobičajene kontradiktornosti sudskih postupaka.

90 Presuda Digital Rights, t. 59.

91 Presuda Tele2 Sverige i Watson, t. 121.

92 Točke 8. do 11. odluke kojom se upućuje zahtjev za prethodnu odluku

150. Sud koji je uputio zahtjeve smatra da se tim propisom ne povređuje pravo na djelotvoran pravni lijek. Međutim, smatram da bi se to u teoriji moglo prihvatiti za osobe koje odluče provjeriti jesu li predmet obavještajne operacije. Suprotno tomu, to se pravo ne poštuje ako se osobe koje jesu ili su bile predmet te operacije o tome ne obavijeste te stoga ne mogu niti razmatrati jesu li njihova prava povrijeđena.

151. Čini se da su pravosudna jamstva na koja upućuje sud koji je uputio zahtjev uvjetovana inicijativom osobe koja sumnja u to da se o njoj prikupljaju podaci. Međutim, pristup sudu radi obrane svojih prava treba biti djelotvoran za sve, što podrazumijeva da osoba čiji se osobni podaci obrađuju mora imati mogućnost osporavati zakonitost navedene obrade u sudskom postupku te je se stoga o tome treba obavijestiti.

152. Točno je da se, kao što to proizlazi iz pruženih informacija, sudski postupak može pokrenuti po službenoj dužnosti ili na temelju upravne tužbe, ali dotičnoj osobi u svakom slučaju treba omogućiti da sama pokrene taj postupak, zbog čega je nužno da joj se otkrije činjenica da su njezini osobni podaci predmet određene obrade. Obrana njezinih prava ne može se prepustiti okolnosti da će ta osoba saznati za tu obradu od trećih osoba ili samostalno.

153. Stoga, ako se ne ugrožava tijek istraga za koje je odobren pristup zadržanim podacima, dotičnu osobu treba obavijestiti o tom pristupu.

154. Druga je stvar to je li, nakon što dotična osoba pokrene sudski postupak jer je obaviještena o pristupu svojim podacima, sudski postupak koji uslijedi u skladu za zahtjevima povjerljivosti i tajnosti svojstvenim ispitivanju postupanja tijela javne vlasti u osjetljivim područjima kao što su područje sigurnosti i obrane države. Međutim, to pitanje nije povezano s predmetnim zahtjevima za prethodnu odluku, pa smatram da Sud ne mora odlučivati u tom pogledu.

V. Zaključak

155. S obzirom na prethodno navedeno, predlažem Sudu da Conseil d'État (Državno vijeće, Francuska) odgovori na sljedeći način:

„Članak 15. stavak 1. Direktive 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), u vezi s člancima 7., 8., 11. i člankom 52. stavkom 1. Povelje Europske unije o temeljnim pravima, treba tumačiti na način da:

1. mu se protivi nacionalni propis kojim se, u kontekstu koji uključuje ozbiljne i kontinuirane prijetnje nacionalnoj sigurnosti, i osobito rizik terorističkih napada, operatorima i pružateljima elektroničkih komunikacijskih usluga propisuje obveza općeg i neselektivnog zadržavanja podataka o prometu i lokaciji svih pretplatnika, kao i podataka koji omogućuju identifikaciju stvaratelja sadržaja koje nude pružatelji navedenih usluga.

2. mu se protivi nacionalni propis kojim se ne propisuje obveza obavješćivanja dotičnih osoba o obradi njihovih osobnih podataka koju obavljaju nadležna tijela, osim ako se tim obavješćivanjem ugrožava djelovanje navedenih tijela.

3. mu se ne protivi se nacionalni propis kojim se omogućuje prikupljanje u stvarnom vremenu podataka o prometu i lokaciji pojedinačnih osoba, pod uvjetom da se te aktivnosti obavljaju u skladu s postupcima utvrđenim za pristup osobnim podacima koji su zakonito zadržani i s istim jamstvima."