Zbornik sudske prakse

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

Predmet C-623/17

Privacy International
protiv
Secretary of State for Foreign and Commonwealth Affairs,
Secretary of State for the Home Department,
Government Communications Headquarters,
Security Service,
Secret Intelligence Service

(zahtjev za prethodnu odluku koji je uputio Investigatory Powers Tribunal (Sud za istražne ovlasti, Ujedinjena Kraljevina))

„Zahtjev za prethodnu odluku – Obrada osobnih podataka i zaštita privatnog života u području elektroničkih komunikacija – Direktiva 2002/58/EZ – Područje primjene – Članak 1. stavak 3. – Članak 15. stavak 3. – Povelja Europske unije o temeljnim pravima – Članci 7., 8. i 51. te članak 52. stavak 1. – Članak 4. stavak 2. UEU-a – Opći i neselektivni prijenos podataka o vezi korisnikâ usluge elektroničkih komunikacija sigurnosnim službama”

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.

– 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 koje smatraju nužnima za zaštitu nacionalne sigurnosti i borbu protiv 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.

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

5. Upućujem na odgovarajuću točku svojeg mišljenja u predmetima C-511/18 i C-512/18.

B. Nacionalno pravo (koje se primjenjuje na ovaj spor)

1. Telecommunications Act 1984 [11]

6. U skladu s člankom 94., ministar operatoru javne elektroničke komunikacijske mreže može dati opće ili posebne smjernice koje smatra nužnim u interesu nacionalne sigurnosti ili odnosa s vladom neke zemlje ili državnog područja izvan Ujedinjene Kraljevine.

2. Data Retention and Investigatory Powers Act 2014 [12]

7. Člankom 1. utvrđuje se:

„(1) Ministar može na temelju akta kojim se određuje zadržavanje zahtijevati od javnog telekomunikacijskog operatora da zadrži relevantne podatke o komunikacijama ako ocijeni da je to nužno i proporcionalno za ispunjavanje jednog ili više ciljeva iz točaka (a) do (h) članka 22. stavka 2. Regulation of Investigatory Powers Acta 2000 (Zakon iz 2000. o istražnim ovlastima; u daljnjem tekstu: RIPA).

(2) Akt kojim se određuje zadržavanje može:

(a) se odnositi na određenog operatora ili bilo koju kategoriju operatora;

7 Osim ovog predmeta, riječ je o predmetima C-511/18 i C-512/18, La Quadrature du Net i dr., 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

11 Zakon iz 1984. o telekomunikacijama; u daljnjem tekstu: Zakon iz 1984.

12 Zakon iz 2014. o zadržavanju podataka i istražnim ovlastima; u daljnjem tekstu: DRIPA

(b) odrediti zadržavanje svih podataka ili bilo koje kategorije podataka;

(c) odrediti razdoblje ili razdoblja tijekom kojih podaci moraju biti zadržani,

(d) sadržavati druge zahtjeve ili ograničenja u odnosu na zadržavanje podataka;

(e) propisati različite odredbe u različite svrhe;

(f) se odnositi na podatke, neovisno o tome postoje li na dan kad je akt kojim se određuje zadržavanje donesen ili stupa na snagu.

(3) Ministar može uredbama propisati daljnja pravila koja se odnose na zadržavanje relevantnih podataka o komunikacijama.

(4) Te odredbe mogu se osobito odnositi na:

(a) zahtjeve koji prethode donošenju akta kojim se određuje zadržavanje;

(b) maksimalno trajanje razdoblja tijekom kojeg podaci trebaju biti zadržani na temelju akta kojim se određuje zadržavanje;

(c) sadržaj, donošenje, stupanje na snagu, preispitivanje, izmjenu ili opoziv akta kojim se određuje zadržavanje;

(d) integritet, sigurnost ili zaštitu zadržanih podataka na temelju ovog članka, pristup tim podacima kao i njihovo razotkrivanje ili uništenje;

(e) provedbu relevantnih zahtjeva ili ograničenja ili provjeru usklađenosti s tim zahtjevima ili ograničenjima;

(f) kodeks dobre prakse koji se odnosi na relevantne zahtjeve, ograničenja ili ovlasti;

(g) povrat od strane ministra (pod određenim uvjetima ili bez njih) troškova koje je snosio javni telekomunikacijski operator radi usklađivanja s relevantnim zahtjevima ili ograničenjima;

[…]

(5) Maksimalno trajanje razdoblja određenog na temelju stavka 4. točke (b) ne smije biti dulje od 12 mjeseci počevši od datuma određenog u pogledu podataka na koje se odnose uredbe iz stavka 3.

(6) Javni telekomunikacijski operator koji na temelju ovog članka zadržava relevantne podatke o komunikacijama može otkriti te podatke samo ako:

(a) ih otkriva u skladu s:

(i) poglavljem 2. dijela 1. [RIPA-e] ili

(ii) sudskom odlukom ili bilo kojim drugim sudskim odobrenjem ili nalogom; ili ako

(b) se to predviđa uredbama iz stavka 3.

(7) Ministar može uredbama propisati pravila koja se odnose na bilo koju donesenu odredbu (ili odredbu koja se može donijeti) na temelju stavka 4. točaka (d) do (g) ili stavka 6. u pogledu podataka o komunikacijama koje pružatelji telekomunikacijskih usluga zadržavaju u skladu s kodeksom dobre prakse na temelju članka 102. Anti-terrorism, Crime and Security Acta 2001 (Zakon iz 2001. o borbi protiv terorizma, o kriminalu i sigurnosti)".

3. RIPA

8. Člankom 21. predviđa se:

„[…]

(4) U ovom poglavlju izraz ‚podaci o komunikacijama' znači bilo što od navedenog:

(a) bilo koji podatak o prometu sadržan u komunikaciji ili koji joj je priložen (od pošiljatelja ili na drugi način) u svrhu bilo koje poštanske usluge ili telekomunikacijskog sustava kojim se ti podaci prenose ili se mogu prenositi;

(b) bilo koja informacija koja ne uključuje ništa od sadržaja komunikacije (osim bilo koje informacije iz točke (a)) i koja se odnosi na korištenje bilo koje osobe:

(i) bilo koje poštanske ili telekomunikacijske usluge; ili

(ii) u vezi s pružanjem bilo koje telekomunikacijske usluge bilo kojeg dijela telekomunikacijskog sustava bilo kojoj osobi ili korištenje tom uslugom bilo koje osobe;

(c) bilo koja informacija koja nije obuhvaćena točkama (a) ili (b) koju je zadržala ili dobila u pogledu primatelja usluge osoba koja pruža poštansku ili telekomunikacijsku uslugu.

[…]

(6) U ovom odjeljku, pojam ‚podatak o prometu', u pogledu bilo koje komunikacije odnosi se na:

(a) bilo koji podatak kojim se utvrđuje ili može utvrditi bilo koja osoba, uređaj ili lokacija prema kojoj ili od koje se prenosi ili može prenijeti komunikacija;

(b) bilo koji podatak kojim se utvrđuje ili odabire, ili kojim se može utvrditi ili odabrati oprema s pomoću koje se prenosi ili može prenijeti komunikacija;

(c) bilo koji podatak koji sadržava signale za pokretanje uređaja koji se upotrebljava u komunikacijskom sustavu u svrhu prijenosa bilo kakve komunikacije; i

(d) bilo koji podatak kojim se utvrđuju podaci sadržani u posebnoj komunikaciji ili koji su joj priloženi ili drugi podaci dokle god su sadržani u posebnoj komunikaciji ili su joj priloženi.

[…]"

9. Člankom 22. propisuje se:

„(1) Taj članak primjenjuje se na slučaj kad osoba odgovorna u svrhu ovog poglavlja ocijeni da je zbog razloga navedenih u stavku 2. ovog članka potrebno dobiti sve podatke o komunikaciji.

(2) Zbog razloga iznesenih u ovom stavku treba dobiti podatke o komunikacijama ako su potrebni:

(a) u interesu nacionalne sigurnosti;

(b) u svrhu sprečavanja ili otkrivanja kaznenih djela ili sprečavanja nereda;

(c) radi gospodarskih interesa Ujedinjene Kraljevine pod uvjetom da su ti interesi jednako relevantni za interese nacionalne sigurnosti;

(d) u interesu javne sigurnosti;

(e) u svrhu zaštite javnog zdravlja;

(f) u svrhu utvrđivanja porezne osnovice ili ubiranja bilo kojeg poreza, pristojbe, naknade ili drugog nameta, doprinosa ili troška koji treba platiti javnoj upravi;

(g) u svrhu sprečavanja, u hitnom slučaju, smrti, ozljeda ili bilo kakve štete za tjelesno ili duševno zdravlje fizičke osobe ili ublažavanja bilo kakve ozljede ili štete za tjelesno ili duševno zdravlje fizičke osobe;

(h) u bilo koju drugu svrhu (koja nije obuhvaćena točkama (a) do (g)) određenu u nalogu ministra na temelju članka 22. stavka 2. točke (h) [DRIPA-e].

(4) Ako u stavku 5. nije drukčije uređeno, odgovorna osoba, kad joj se čini da telekomunikacijski ili poštanski operator raspolaže, može raspolagati ili bi mogao raspolagati podacima, može od njega zahtijevati da:

(a) dobije podatke, ako već njima ne raspolaže i

(b) otkrije, u svakom slučaju, sve podatke kojima raspolaže ili koje je naknadno dobio.

(5) Odgovorna osoba ne smije dati odobrenje u skladu sa stavkom 3. ili podnijeti zahtjev na temelju stavka 4. osim ako smatra da je dobivanje predmetnih podataka, koje se temelji na ponašanju koje je odobreno ili se zahtijeva na temelju odobrenja ili zahtjeva, proporcionalno cilju dobivanja podataka."

10. U skladu s člankom 65., pred Investigatory Powers Tribunalom (Sud za istražne ovlasti) treba pokrenuti postupak ako postoje razlozi na temelju kojih se može smatrati da su podaci dobiveni na neprimjeren način.

II. Činjenice i prethodna pitanja

11. Prema tvrdnjama suda koji je uputio zahtjev, glavni postupak odnosi se na masovne komunikacijske podatke koje prikupljaju i upotrebljavaju United Kingdom Security and Intelligence Agencies (sigurnosne i obavještajne agencije Ujedinjene Kraljevine; u daljnjem tekstu: SIA).

12. Ti podaci uključuju „tko, kada, gdje, kako i s kime" koristi telefon i internet. Uključuju i položaj pokretnih i nepokretnih telefonskih linija za odlazne i dolazne pozive, te položaj računala korištenih za pristup internetu. Ne uključuju sadržaj komunikacija, koji se može pribaviti samo sudskim nalogom.

13. Tužitelj u glavnom postupku (Privacy International, nevladina organizacija za zaštitu ljudskih prava) podnio je tužbu sudu koji je uputio zahtjev jer je smatrao da SIA-ino prikupljanje i uporaba navedenih podataka povređuje pravo na poštovanje privatnog života iz članka 8. Europske konvencije o ljudskim pravima (u daljnjem tekstu: EKLJP) te je protivno pravu Unije.

14. Tužena tijela [13] tvrde da je njihova uporaba takvih ovlasti zakonita i bitna, među ostalim, za zaštitu nacionalne sigurnosti.

15. Prema podacima iz odluke kojom se upućuje zahtjev za prethodnu odluku, u skladu sa smjernicama koje izdaje ministar na temelju članka 94. Zakona iz 1984., SIA-e primaju masovne komunikacijske podatke posredstvom operatora javnih elektroničkih komunikacijskih mreža.

16. Navedeni podaci uključuju podatke o prometu i položaju te pružaju informacije o društvenim, trgovačkim, financijskim, komunikacijskim i putnim aktivnostima korisnikâ. SIA te podatke, nakon što ih pribavi, zadržava na siguran način, pri čemu upotrebljava opće tehnike (na primjer, filtriranje i agregaciju), odnosno tehnike koje nisu usmjerene na posebne i poznate mete.

17. Sud koji je uputio zahtjev smatra dokazanim da su te tehnike bitne za SIA-in rad u borbi protiv ozbiljnih prijetnji javnoj sigurnosti, uključujući područja borbe protiv terorizma, protuobavještajnih aktivnosti i suzbijanja širenja nuklearnog oružja. SIA-ine sposobnosti prikupljanja i uporabe podataka bitne su za zaštitu nacionalne sigurnosti Ujedinjene Kraljevine.

18. Prema mišljenju suda koji je uputio zahtjev, sporne su mjere u skladu s nacionalnim pravom i člankom 8. EKLJP-a. Međutim, dvoji o njihovoj usklađenosti s pravom Unije, s obzirom na presudu Tele2 Sverige i Watson.

19. U tim okolnostima, navedeni sud upućuje Sudu sljedeća prethodna pitanja:

„1. Uzimajući u obzir članak 4. UEU-a i članak 1. stavak 3. Direktive 2002/58 […], obuhvaća li opseg prava Unije i Direktive [2002/58] zahtjev propisan smjernicom Secretary of Statea (ministar) kojim se pružatelju elektroničke komunikacijske mreže nalaže da Security and Intelligence Agenciesima (sigurnosne i obavještajne agencije; SIA) pruža masovne komunikacijske podatke?

2. Ako je odgovor na prvo pitanje potvrdan, primjenjuju li se na takvu smjernicu ministra neki od zahtjeva Watson[[14] odnosno i neki drugi zahtjevi uz one koji su propisani EKLJP-om? Ako je tome tako, na koji se način i u kojoj mjeri ti zahtjevi primjenjuju, uzimajući u obzir bitnu SIA-inu potrebu da za zaštitu nacionalne sigurnosti koristi masovno prikupljanje i tehnike automatske obrade, te u kojoj mjeri propisivanje takvih zahtjeva može kritično onemogućiti takve sposobnosti, ako su one u drugim pogledima usklađene s EKLJP-om?”

20. Sud koji je uputio zahtjev svoja pitanja postavlja na sljedeći način:

„(a) sposobnosti SIA-a da koriste [masovne komunikacijske podatke], koji im se dostavljaju, bitne su za zaštitu nacionalne sigurnosti Ujedinjene Kraljevine, uključujući područja borbe protiv terorizma, protuobavještajnih aktivnosti i suzbijanja širenja nuklearnog oružja;

(b) temeljno obilježje SIA-ine uporabe [tih podataka] jest otkrivanje prethodno nepoznatih prijetnji za nacionalnu sigurnost uporabom neciljanih masovnih tehnika koje se temelje na objedinjavanju [tih podataka] na jednom mjestu. Glavna korist jest brzo utvrđivanje i praćenje mete, kao i pružanje osnove za akciju u situaciji neposredne prijetnje;

13 Secretary of State for Foreign and Commonwealth Affairs (ministar vanjskih poslova i poslova Commonwealtha, Ujedinjena Kraljevina), Secretary of State for the Home Department (ministar unutarnjih poslova, Ujedinjena Kraljevina) i tri SIA-e Ujedinjene Kraljevine, odnosno Government Communications Headquarters (Vladin komunikacijski stožer (GCHQ), Ujedinjena Kraljevina), Security Service (Sigurnosna služba (MI5), Ujedinjena Kraljevina) i Secret Intelligence Service (Tajna obavještajna služba (MI6), Ujedinjena Kraljevina)

14 *Id est*, sudska praksa uspostavljena presudom Tele2 Sverige i Watson

(c) pružatelj elektroničke komunikacijske mreže nije naknadno obvezan zadržati navedene podatke (dulje od razdoblja koje zahtijeva njegovo uobičajeno poslovanje), a koje zatim zadržava samo država (SIA);

(d) nacionalni sud je utvrdio (ovisno o određenim pitanjima o kojima još nije odlučeno) da su zaštitne mjere u vezi sa SIA-inom uporabom [tih podataka] dosljedne zahtjevima EKLJP-a; te

(e) nacionalni sud je utvrdio da bi nalaganje zahtjeva navedenih u presudi [Tele2 Sverige i Watson], ako je primjenjivo, onemogućilo SIA-ine mjere poduzete radi zaštite nacionalne sigurnosti i stoga dovelo u opasnost nacionalnu sigurnost Ujedinjene Kraljevine".

III. Postupak pred Sudom

21. Tajništvo Suda zaprimilo je zahtjev za prethodnu odluku 31. listopada 2017.

22. Pisana očitovanja podnijeli su belgijska, britanska, ciparska, češka, estonska, francuska, irska, latvijska, mađarska, nizozemska, norveška, njemačka, poljska, portugalska, španjolska i švedska vlada te Komisija.

23. Na raspravi održanoj 9. rujna 2019., koja je održana i za predmete C-511/18, C-512/18 i C-520/18, sudjelovale su stranke četiriju prethodnih postupaka, prethodno navedene vlade, Komisija i Europski nadzornik za zaštitu osobnih podataka.

IV. Analiza

A. Područje primjene Direktive 2002/58 i isključenje nacionalne sigurnosti (prvo prethodno pitanje)

24. U mišljenju od istog datuma koje iznosim u predmetima C-511/18 i C-512/18, objašnjavam razloge zbog kojih se, prema mojem mišljenju, 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" [15].

25. Prilikom iznošenja svojih argumenata razmatram utjecaj presuda Suda od 30. svibnja 2006., Parlament/Vijeće i Komisija [16] i Tele2 Sverige i Watson, pri čemu zagovaram kompromisno tumačenje obiju presuda [17].

26. U istom mišljenju, nakon utvrđivanja primjenjivosti Direktive 2002/58, ispitujem isključenje nacionalne sigurnosti koje se navodi u toj direktivi i utjecaj članka 4. stavka 2. UEU-a [18].

27. Ne dovodeći u pitanje ono što ću iznijeti u nastavku, upućujem na već izneseno u navedenom mišljenju i mišljenju u predmetu C-520/18.

15 Mišljenje u predmetima C-511/18 i C-512/18, t. 42.

16 Predmeti C-317/04 i C-318/04, EU:C:2006:346

17 Mišljenje u predmetima C-511/18 i C-512/18, t. 44. do 76.

18 *Ibidem*, t. 77. do 90.

1. Primjena Direktive 2002/58 u ovom predmetu

28. Na temelju spornih pravila u ovom sporu, na pružatelje elektroničkih komunikacijskih usluga odnosi se obveza koja podrazumijeva, osim zadržavanja podataka, obradu podataka koje posjeduju zbog usluge koju pružaju korisnicima javnih komunikacijskih mreža u Uniji [19].

29. Naime, navedeni operatori obvezni su prenositi te podatke SIA-i. Ovdje se postavlja pitanje dopušta li se člankom 15. stavkom 1. Direktive 2002/58 da se taj prijenos zbog svojeg cilja jednostavno isključi iz prava Unije.

30. Prema mojem mišljenju, ne dopušta se. Zadržavanje navedenih podataka koje uslijedi nakon njihova daljnjeg prijenosa može se kvalificirati kao obrada osobnih podataka koju provode pružatelji elektroničkih telekomunikacijskih usluga zbog čega su svakako obuhvaćeni područjem primjene Direktive 2002/58.

31. Razlozi nacionalne sigurnosti ne mogu biti važniji od tog utvrđenja, kao što to predlaže sud koji je uputio zahtjev, što ima za posljedicu da sporna obveza ne bi bila obuhvaćena područjem primjene prava Unije. Prema mojem mišljenju, ponavljam, pružateljima se nalaže obrada podataka u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga u javnim komunikacijskim mrežama u Uniji, što je upravo područje primjene Direktive 2002/58, kako se propisuje njezinim člankom 3. stavkom 1.

32. Slijedom te pretpostavke, spor se više ne odnosi na SIA-ine aktivnosti (na koje bi se, kao što sam to ranije napomenuo, moglo ne primjenjivati pravo Unije kad se ne bi odnosile na operatore elektroničkih komunikacija), nego na zadržavanje i daljnji prijenos podataka koje posjeduju navedeni operatori. S tog stajališta, u obzir se uzimaju temeljna prava koja jamči Unija.

33. Ponavljam, ključni čimbenik za rješavanje ovog spora jest obveza općeg i neselektivnog zadržavanja podataka kojima mogu pristupiti tijela javne vlasti.

2. Pozivanje na nacionalnu sigurnost

34. Budući da sud koji je uputio zahtjev u ovom predmetu posebno ističe SIA-ine aktivnosti koje utječu na nacionalnu sigurnost, upućujem na neke od točaka iz svojeg mišljenja od istog datuma u predmetima C-511/18 i C-512/18, koje se odnose na isto pitanje:

„77. Nacionalna sigurnost […] se u Direktivi 2002/58 razmatra 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.

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'. […]

19 Na temelju članka 2. Direktive 2002/58, za potrebe primjene te direktive, upotrebljavaju se definicije iz Direktive 95/46. U skladu člankom 2. točkom (b) potonje direktive „obrada osobnih podataka" znači „bilo koji postupak ili skup postupaka koji se provode nad osobnim podacima, bilo automatskim putem ili ne, kao što je prikupljanje, snimanje, organiziranje, pohrana, prilagođavanje ili mijenjanje, vraćanje, obavljanje uvida, uporaba, *otkrivanje prijenosom* i širenjem ili *stavljanje na raspolaganje drugim načinom*, poravnavanje ili kombiniranje, blokiranje, brisanje ili uništavanje" (moje isticanje).

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.

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.

[…]

82. Smatram […] da kao smjernica može poslužiti kriterij iz Okvirne odluke 2006/960/PUP, […] 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'. […]

[…]

84. Postoji […] 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 uvodna izjava [11. Direktive 2002/58] 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, njihovim člankom 13. stavkom 1. odnosno člankom 15. stavkom 1. U tom pogledu nema nikakve razlike između dviju direktiva.

[…]

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."

3. Posljedice primjene presude Tele2 Sverige i Watson u ovom predmetu

35. Sud koji je uputio zahtjev usredotočio se na tumačenje Suda u presudi Tele2 Sverige i Watson, pri čemu je naveo poteškoće koje bi, prema njegovu mišljenju, nastale primjenom te presude na ovaj predmet.

36. Naime, u presudi Tele2 Sverige i Watson navedeni su uvjeti koje treba ispuniti nacionalni propis kojim se uspostavlja obveza zadržavanja podataka o prometu i lokaciji kako bi im tijela javne vlasti naknado mogla pristupiti.

37. Kao i u predmetima C-511/18 i C-512/18, i zbog sličnih razloga, smatram da nacionalna pravila na koja se odnosi predmetni zahtjev za prethodnu odluku nisu u skladu s uvjetima utvrđenim u presudi Tele2 Sverige i Watson jer podrazumijevaju opće i neselektivno zadržavanje osobnih podataka koje omogućuje detaljan uvid u život dotičnih osoba tijekom duljeg razdoblja.

38. U mišljenju u tim dvama predmetima postavljam pitanje je li moguće prilagoditi ili nadopuniti sudsku praksu uspostavljenu tom presudom, s obzirom na njezine posljedice za borbu protiv terorizma ili za zaštitu države od drugih sličnih prijetnji nacionalnoj sigurnosti.

39. U nastavku ću također navesti neke od točaka iz tog mišljenja u kojem zapravo tvrdim da, s obzirom na to da se navedena sudska praksa može prilagoditi, treba je u bitnome potvrditi:

„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 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. […]

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. […], 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.

138. Stoga se i u ovom slučaju nacionalnim propisom moraju predvidjeti materijalni i postupovni uvjeti kojima se uređuje pristup nadležnih tijela zadržanim podacima. […] 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. […]

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. […] 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."

B. Drugo prethodno pitanje

40. Sud koji je uputio zahtjev postavlja drugo pitanje u slučaju potvrdnog odgovora na prvo pitanje. U tom bi slučaju želio znati koje „drug[e] zahtjev[e] uz one koji su propisani EKLJP-om" ili koji proizlaze iz presude Tele2 Sverige i Watson treba zahtijevati.

41. U tom smislu tvrdi da bi nalaganje uvjeta iz presude Tele2 Sverige i Watson „onemogućilo SIA-ine mjere poduzete radi zaštite nacionalne sigurnosti".

42. Budući da na prvo pitanje predlažem niječan odgovor, nije potrebno razmatrati drugo pitanje. Potonje pitanje, kao što to sam sud koji je uputio zahtjev ističe, uvjetovano je time da se u skladu s pravom Unije proglase „masovno prikupljanje i tehnike automatske obrade" osobnih podataka svih korisnika u Ujedinjenoj Kraljevini, koje operatori elektroničkih komunikacijskih usluga trebaju prenijeti SIA-i.

43. Ako Sud bude smatrao nužnim odgovoriti na drugo pitanje, smatram da navedene uvjete iz presude Tele2 Sverige i Watson treba potkrijepiti u odnosu na:

– zabranu općeg pristupa podacima;

– nužnost prethodnog odobrenja suda ili neovisnog tijela kako bi taj pristup bio zakonit;

– obvezu obavješćivanja dotičnih osoba, osim ako bi se time ugrozila učinkovitost mjere;

– zadržavanje podataka u Uniji.

44. Ponavljam, dovoljno je potvrditi te uvjete obvezne primjene, zbog razloga koje sam naveo u mišljenju u predmetima C-511/18 i C-512/18 te C-520/18, a da pritom nije potrebno uvoditi „druge" dodatne uvjete, u smislu u kojem to navodi sud koji je uputio zahtjev.

V. Zaključak

45. S obzirom na sve prethodno navedeno, predlažem Sudu da Investigatory Powers Tribunalu (Sud za istražne ovlasti, Ujedinjena Kraljevina) odgovori na sljedeći način:

„Članak 4. UEU-a i članak 1. stavak 3. 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) treba tumačiti na način da im se protivi nacionalni propis kojim se pružatelju elektroničke komunikacijske mreže nalaže obveza da sigurnosnim i obavještajnim agencijama države članice pruža ‚masovne komunikacijske podatke' za koje se podrazumijeva da su prethodno prikupljeni na opći i neselektivan način."

Podredno:

„Pristup sigurnosnih i obavještajnih agencija države članice podacima koje prenose pružatelji elektroničke komunikacijske mreže treba biti u skladu s uvjetima utvrđenim u presudi od 21. prosinca 2016., Tele2 Sverige i Watson (C-203/15 i C-698/15, EU:C:2016:970)."