Zbornik sudske prakse

MIŠLJENJE NEZAVISNOG ODVJETNIKA
HENRIKA SAUGMANDSGAARDA ØEA
od 3. svibnja 2018.[1]

Predmet C-207/16

Ministerio Fiscal

(zahtjev za prethodnu odluku koji je uputio Audiencia Provincial de Tarragona (Provincijski sud u Tarragoni, Španjolska))

„Zahtjev za prethodnu odluku – Elektroničke komunikacije – Obrada osobnih podataka – Pravo na privatnost i pravo na zaštitu takvih podataka – Direktiva 2002/58/EZ – Članak 1. i članak 15. stavak 1. – Povelja Europske unije o temeljnim pravima – Članci 7. i 8. i članak 52. stavak 1. – Podaci prikupljeni u okviru pružanja usluga elektroničkih komunikacija – Zahtjev policijskog tijela za pristup u svrhu kaznene istrage – Načelo proporcionalnosti – Pojam ‚teško kazneno djelo' kojim se može opravdati zadiranje u temeljna prava – Kriteriji ozbiljnosti – Izrečena kazna – Najmanji prag"

I. Uvod

1. Ovaj se zahtjev za prethodnu odluku u biti odnosi na tumačenje pojma „teška kaznena djela"[2] u smislu sudske prakse Suda koja proizlazi iz presude Digital Rights Ireland i dr.[3] (u daljnjem tekstu: presuda Digital Rights) te potom iz presude Tele2 Sverige i Watson i dr.[4] (u daljnjem tekstu: presuda Tele2), u kojoj se taj pojam upotrebljavao kao kriterij za ocjenu zakonitosti i proporcionalnosti zadiranja u prava propisana člancima 7. i 8. Poveljom Europske unije o temeljnim pravima (u daljnjem tekstu: Povelja), odnosno, redom pravo na poštovanje privatnog i obiteljskog života, kao i prava na zaštitu osobnih podataka.

2. Ovaj je zahtjev za prethodnu odluku upućen u okviru pravnog sredstva podnesenog protiv sudske odluke kojom je odbijena mogućnost da se policijskim tijelima dostave određeni podaci o bračnom stanju koje zadržavaju operatori mobilne telefonije, radi identifikacije pojedinaca u svrhu kaznene istrage. Pobijana odluka bila je, među ostalim, obrazložena razmatranjem da činjenice iz kojih proizlazi ta istraga nisu činile teško kazneno djelo, suprotno onom što se zahtijevalo primjenjivim španjolskim propisima.

1 Izvorni jezik: francuski

2 Izraz ovdje treba shvatiti kao da se odnosi samo na kaznena djela.

3 Presuda od 8. travnja 2014. (C-293/12 i C-594/12, EU:C:2014:238), u kojoj je Sud proglasio nevaljanom Direktivu 2006/24/EZ 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.) jer je „usvajanjem Direktive 2006/24 zakonodavac Unije prekoračio granice koje nameće poštovanje načela proporcionalnosti s obzirom na članak 7., članak 8. i članak 52. stavak 1. Povelje" (t. 69.).

4 Presuda od 21. prosinca 2016. (C-203/15 i C-698/15, EU:C:2016:970), u kojoj je Sud presudio da se pravu Unije, *s jedne strane*, „protivi nacionalni propis poput onoga u glavnom postupku, koji 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" i, *s druge strane*, da mu se „protivi nacionalni propis kojim se uređuje zaštita i sigurnost podataka o prometu i lokaciji i osobito pristup nadležnih nacionalnih tijela zadržanim podacima kad svrha tog pristupa u okviru borbe protiv kriminaliteta nije ograničena na borbu protiv teških kaznenih djela, kad se navedeni pristup ne podvrgava prethodnom nadzoru suda ili neovisnog upravnog tijela i kad nije propisano da se predmetni podaci zadržavaju na području Unije" (t. 1. i 2. izreke).

3. Sud koji je uputio zahtjev u biti pita Sud o načinu određivanja praga težine kaznenih djela od kojeg se, s obzirom na gore navedenu sudsku praksu, može opravdati povreda temeljnih prava zaštićenih člancima 7. i 8. Povelje prilikom pristupa nadležnih nacionalnih tijela osobnim podacima koje su zadržali pružatelji usluga elektroničkih komunikacija.

4. Nakon što utvrdim da je Sud nadležan za odlučivanje o tom zahtjevu za prethodnu odluku te da je potonji zahtjev dopušten, namjeravam dokazati da pristup osobnim podacima u okolnostima kao što su one u ovom slučaju dovodi do zadiranja u gore navedena temeljna prava koje ne odgovara situacijama u kojima se samo borbom protiv teških kaznenih djela može opravdati povreda navedenih prava, u skladu s gore navedenom sudskom praksom.

5. Budući da smatram da, s obzirom na poseban predmet glavnog postupka, neće biti potrebno da Sud odgovori na izvorni tekst prethodnih pitanja, tek ću podredno iznijeti navode o kriterijima na temelju kojih bi eventualno bilo moguće definirati pojam „teška kaznena djela" u smislu te sudske prakse, osobito s obzirom na kriterij izrečene kazne.

II. Pravni okvir

A. Pravo Unije

6. U preambuli 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)[5], kako je izmijenjena Direktivom 2009/136/EZ[6] (u daljnjem tekstu: Direktiva 2002/58) navodi se:

„(2) Ova Direktiva traži poštovanje temeljnih prava te poštuje načela priznata posebno [Poveljom]. Ova Direktiva posebno traži osiguranje punoga poštovanja prava određenih u člancima 7. i 8. [te Povelje].

[…]

(11) Poput Direktive 95/46/EZ[7], ova Direktiva ne obuhvaća pitanja zaštite temeljnih prava i sloboda koje se odnose na aktivnosti koje nisu uređene pravom Zajednice. Stoga se njome 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 javne sigurnosti, obrane, državne sigurnosti (uključujući gospodarsko blagostanje države kada se aktivnosti odnose na sigurnosna pitanja države) te za provođenje odredaba kaznenog prava. Kao posljedica toga, ova Direktiva ne utječe na sposobnost država članica da provode zakonito presretanje elektroničkih komunikacija, odnosno da poduzimaju druge mjere ako je to nužno u neku od gore navedenih svrha te u skladu s Europskom konvencijom za zaštitu ljudskih prava i temeljnih sloboda [u daljnjem tekstu: EKLJP], na način kako je tumači Europski sud za ljudska prava [u daljnjem tekstu: ESLJP]. Takve mjere moraju biti prikladne, strogo razmjerne svrsi za koju se poduzimaju i neophodne unutar demokratskog društva te trebaju biti podložne prikladnim zaštitnim mehanizmima u skladu s [EKLJP-om][8]."

5 SL 2002., L 201, str. 37. (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 52., str. 111.)

6 Direktiva Europskog parlamenta i Vijeća od 25. studenoga 2009. (SL 2009., L 337, str. 11.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 52., str. 224. i ispravci SL 2017., L 162, str. 56. i SL 2018., L 74, str. 11.)

7 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.)

8 Osobito, u skladu s člankom 8. EKLJP-a, prema kojem:
„1. Svatko ima pravo na poštovanje svoga privatnog i obiteljskog života, doma i dopisivanja.
2. Javna vlast se neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te radi sprječavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih".

7. U skladu s člankom 1. Direktive 2002/58, naslovljenim „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 […].

[…]

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.”

8. Njezin članak 2., naslovljen „Definicije”, glasi kako slijedi:

„Definicije iz Direktive 95/46[…] i Direktive 2002/21/EZ Europskog parlamenta i Vijeća od 7. ožujka 2002. o zajedničkom regulatornom okviru za elektroničke komunikacijske mreže i usluge (Okvirna direktiva)[9] primjenjuju se osim ako nije drukčije određeno.

Sljedeće definicije se također primjenjuju:

(a) ‚korisnik’ znači svaka fizička osoba koja koristi javno dostupnu elektroničku komunikacijsku uslugu, u privatne ili poslovne svrhe, pri čemu nije nužno da se pretplatila na tu uslugu;

(b) ‚podaci o prometu’ znači svi podaci koji se obrađuju u svrhu prijenosa komunikacije na elektroničkoj komunikacijskoj mreži ili za njezino naplaćivanje;

(c) ‚podaci o lokaciji’ znači svi podaci koji se obrađuju u sklopu elektroničke komunikacijske mreže ili u sklopu usluga elektroničkih komunikacija, koji ukazuju na zemljopisnu lokaciju terminalne opreme korisnika javno dostupnih usluga elektroničkih komunikacija;

(d) ‚komunikacija’ znači svaka informacija koja se razmjenjuje ili prenosi između ograničenog broja stranaka putem javno dostupne elektroničke komunikacijske usluge. Ovo ne uključuje informaciju prenesenu kao dio usluge emitiranja za javnost putem elektroničke komunikacijske mreže, osim u onoj mjeri u kojoj se informacija može odnositi na pretplatnika ili na korisnika koji prima informaciju koji se mogu identificirati;

[…]”

9. Člankom 15. Direktive 2002/58, naslovljenim „Primjena određenih odredaba Direktive 95/46[…]”, u njegovu stavku 1., predviđa se da „[d]ržave 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[…]. 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”.

9 SL 2002., L 108, str. 33. (posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 49., str. 25.)

B. Španjolsko pravo

1. Zakon 25/2007

10. Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a la redes públicas de comunicaciones (Zakon 25/2007 o zadržavanju podataka koji se odnose na elektroničke komunikacije i javne komunikacijske mreže) od 18. listopada 2007.[10] (u daljnjem tekstu: Zakon 25/2007) u španjolsko pravo prenosi Direktivu 2006/24[11], koju je Sud u presudi Digital Rights proglasio nevaljanom.

11. U skladu s člankom 1. Zakona 25/2007, u verziji mjerodavnoj za činjenice u glavnom postupku:

„1. Cilj ovog zakona je urediti obvezu operatora da zadržavaju podatke koji su dobiveni ili obrađeni u okviru pružanja elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža, kao i obvezu dostavljanja tih podataka ovlaštenim službenicima svaki put kad se to od njih zatraži putem potrebnog sudskog odobrenja u svrhu otkrivanja, istrage i suđenja za teška kaznena djela predviđena Kaznenim zakonikom ili posebnim kaznenim zakonima.

2. Ovaj se zakon primjenjuje na podatke o prometu i lokaciji kako pravnih tako i fizičkih osoba te na uz to vezane podatke nužne za identificiranje pretplatnika ili registriranog korisnika.

[…]”

12. U članku 3. navedenog zakona nabrajaju se podaci koje su operatori dužni zadržati. Riječ je, među ostalim, na temelju stavka 1. podstavka (a) točke 1. podtočke ii. tog članka, o podacima potrebnim za pronalaženje i identifikaciju izvora komunikacije, kao što su, što se tiče mobilne telefonije, ime i adresa pretplatnika ili registriranog korisnika.

2. Kazneni zakonik

13. Na temelju članka 13. stavka 1. španjolskog Kaznenog zakonika, u verziji mjerodavnoj za činjenice u glavnom postupku, „[t]eška kaznena djela su ona koja se zakonom kažnjavaju teškom kaznom”.

14. Članak 33. navedenog zakonika glasi kako slijedi:

„1. Ovisno o njihovoj naravi i trajanju, kazne se klasificiraju kao teške, manje teške i lakše.

2. Teške kazne su:

(a) kazna doživotnog zatvora s mogućnošću pomilovanja,

(b) zatvorska kazna dulja od pet godina.

[…]”

10 BOE br. 251 od 19. listopada 2007., str. 42517.

11 To proizlazi i iz preambule navedenog zakona i iz njegovih ključnih odredbi, čiji je tekst sličan onom odgovarajućih odredbi Direktive 2006/24.

3. Zakonik o kaznenom postupku

15. Španjolski Zakonik o kaznenom postupku izmijenjen je s Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (Organski zakon 13/2015 o izmjeni Zakonika o kaznenom postupku u svrhu jačanja postupovnih jamstava i reguliranja mjera tehnološke istrage) od 5. listopada 2015.[12] (u daljnjem tekstu: Organski zakon 13/2015).

16. Tim se zakonom, koji je stupio na snagu 6. prosinca 2015., u Zakonik o kaznenom postupku uvodi područje pristupa podacima o telefonskoj i telematskoj komunikaciji koje su zadržali pružatelji usluga elektroničkih komunikacija.

17. U skladu s člankom 579. stavkom 1. Zakonika o kaznenom postupku, u verziji koja proizlazi iz navedenog zakona, „[s]ud može odobriti presretanje privatne, poštanske i telegrafske korespondencije, uključujući telefaks, Burofax i međunarodne novčane doznake, koje osumnjičenik šalje ili prima, kao i otvaranje i analizu te korespondencije ako postoje naznake na temelju kojih se može smatrati da bi se time omogućilo otkrivanje ili provjera činjenice ili relevantnog čimbenika u predmetu kada je predmet istrage jedno od sljedećih kaznenih djela:

1. namjerna kaznena djela koja se kažnjavaju najvećom zatvorskom kaznom od najmanje tri godine,

2. kaznena djela počinjena u okviru zločinačke organizacije,

3. kaznena djela terorizma”.

18. U članku 588.ter j istog zakonika, naslovljenom „Podaci dostupni u automatiziranim arhivima pružatelja usluga”, navodi se:

„1. Elektronički podaci koje zadržavaju pružatelji usluga ili osobe koje omogućavaju komunikaciju, u skladu sa zakonodavstvom koje se odnosi na zadržavanje podataka o elektroničkim komunikacijama ili na vlastitu inicijativu iz poslovnih ili drugih razloga, te koji su povezani s komunikacijskim procesom mogu se dostaviti radi uzimanja u obzir u okviru postupka samo uz sudsko odobrenje.

2. Kada se uvid u te podatke pokaže nužnim za istragu, od nadležnog suda valja zatražiti odobrenje pristupa informacijama koje se nalaze u automatiziranim arhivima pružatelja usluga, među ostalim za unakrsno ili napredno pretraživanje podataka, ako se pojasni narav podataka u koje je potrebno steći uvid i razlozi kojima se opravdava njihovo dostavljanje.”

III. Glavni postupak, prethodna pitanja i postupak pred Sudom

19. G. Hernández Sierra policiji je prijavio nasilnu krađu svojeg novčanika i mobilnog telefona, koja se dogodila 16. veljače 2015. i tijekom koje je bio teško ozlijeđen.

12 BOE br. 239 od 6. listopada 2015., str. 90192.

20. Policija je 27. veljače 2015. pred Juzgado de Instrucción nº 3 de Tarragona (Istražni sud br. 3 u Tarragoni, Španjolska, u daljnjem tekstu: Istražni sud) podnijela zahtjev kojim traži da se različitim telefonskim operatorima naloži da dostave, s jedne strane, brojeve telefona koji su između 16. i 27. veljače 2015. aktivirani s brojem IMEI [13] ukradenog mobilnog telefona i, s druge strane, osobne podatke nositelja ili korisnika svih telefonskih brojeva koji odgovaraju SIM karticama aktiviranima s navedenim brojem IMEI [14].

21. Rješenjem od 5. svibnja 2015. Istražni sud odbio je taj zahtjev jer zahtijevana mjera nije bila korisna za identifikaciju počiniteljâ kaznenog djela i jer se, u svakom slučaju, Zakonom 25/2007 dostava podataka koje su zadržali telefonski operatori ograničava na teška kaznena djela, odnosno, u skladu sa španjolskim Kaznenim zakonikom [15], na ona koja se kažnjavaju zakonskom kaznom većom od pet godina, dok predmetne činjenice ne čine teško kazneno djelo.

22. Ministerio Fiscal (Državno odvjetništvo, Španjolska), jedina stranka u postupku, podnio je žalbu protiv tog rješenja pred Audiencia Provincial de Tarragona (Provincijski sud u Tarragoni, Španjolska), tvrdeći da je dostavljanje predmetnih podataka trebalo odobriti zbog naravi činjenica i zbog odluke Tribunal Supremo (Vrhovni sud, Španjolska) u pogledu sličnog slučaja [16].

23. Rješenjem od 9. veljače 2016., navedeni žalbeni sud je kao privremenu mjeru za telefonske operatore naložio produljenje zadržavanja podataka na koje se odnosi sporni zahtjev.

24. U odluci tog suda kojom se upućuje zahtjev za prethodnu odluku navodi se da je nakon donošenja pobijane odluke španjolski zakonodavac uveo, na temelju Organskog zakona 13/2015 [17], dva alternativna kriterija za utvrđivanje stupnja težine kaznenog djela. Prvi je materijalni kriterij, povezan s ponašanjima koja odgovaraju kvalifikacijama kaznenog djela čija je kaznena narav posebna i teška i koja su osobito štetna za pravne interese pojedinaca i kolektiva [18]. Drugi je formalni normativni kriterij, koji se temelji isključivo na kazni predviđenoj za predmetno kazneno djelo. Međutim, prag od tri godine zatvora koji se predviđa potonjim kriterijem može obuhvatiti veliku većinu kvalifikacija kaznenog djela. K tome, sud koji je uputio zahtjev napominje da se interesom države da zaštiti građane i da kazni protupravna postupanja ne može opravdati neproporcionalna povreda temeljnih prava osoba.

25. U tim je okolnostima Audiencia Provincial de Tarragona (Provincijski sud u Tarragoni) odlukom od 6. travnja 2016., koju je Sud zaprimio 14. travnja 2016., odlučio prekinuti postupak i Sudu uputiti sljedeća prethodna pitanja:

„1. Može li se dovoljna težina kaznenog djela kao kriterij koji opravdava zadiranje u temeljna prava iz članaka 7. i 8. [Povelje] utvrditi samo na temelju kazne koju je moguće izreći za kazneno djelo o kojem se vodi istraga ili je usto nužno u kažnjivom ponašanju utvrditi posebne vrste štetnosti za pravne interese pojedinaca ili kolektiva?

13 IMEI je pokrata za izraz „International Mobile Equipment Identity” (međunarodni identifikator mobilnog uređaja). IMEI je jedinstveni identifikacijski broj sastavljen od petnaestak znamenki, koji je općenito upisan unutar odjeljka za bateriju mobilnog telefona, kao i na kutiji i na računu koji se dobivaju prilikom kupnje uređaja.

14 Španjolska vlada navodi da se taj zahtjev odnosio na četiri telefonske kompanije i da se njime pojašnjavalo da bi se, u slučaju da je IMEI koristio telefonsku mrežu jedne od tih kompanija, dok je navedenom mrežom upravljao operator virtualne mobilne mreže, gore navedeni podaci koje bi potonji operator prikupio također morali dostaviti.

15 Vidjeti odredbe preuzete u točkama 13. i 14. ovog mišljenja.

16 Vidjeti presudu Sala de lo Penal (Kazneno vijeće) od 26. srpnja 2010. (br. 745/2010, ES:TS:2010:4200), dostupnu na sljedećoj internetskoj adresi:
http://www.poderjudicial.es/search/contenidos.action?
action=contentpdf&databasematch=TS&reference=5697924&links=&optimize=20100812&publicinterface=true.

17 Vidjeti točku 15. i sljedeće točke ovog mišljenja. Prema mišljenju suda koji je uputio zahtjev, ta je reforma očito relevantna za zahtjev za prethodnu odluku. Na raspravi je španjolska vlada navela da je novi propis primjenjiv u ovom slučaju.

18 Odnosno kaznena djela terorizma i ona počinjena u okviru zločinačke organizacije.

2. Ako je u skladu s temeljnim načelima prava Unije koja je Sud kao standard strogog nadzora Direktive [koja je presudom Digital Rights proglašena nevaljanom] koristio u svojoj presudi [Digital Rights] to da se težina kaznenog djela treba utvrditi samo na temelju kazne koju je moguće izreći, kolika bi trebala biti ta najmanja kazna? Bi li u skladu s time bila opća odredba o najmanje tri godine zatvora?"

26. Postupak pred Sudom prekinut je odlukom predsjednika od 23. svibnja 2016., u očekivanju objave presude Suda u spojenim predmetima Tele2 Sverige i Watson i dr., C-203/15 i C-698/15.

27. Na upit Suda nakon objave te presude od 21. prosinca 2016.[19], sud koji je uputio zahtjev naveo je da namjerava ustrajati na svojem zahtjevu za prethodnu odluku. Tvrdio je da su prethodna pitanja koja je postavio i dalje relevantna jer se u navedenoj presudi zaista navode primjeri teških kaznenih djela[20], ali se nedovoljno jasno definira materijalni sadržaj pojma težine kaznenog djela koji može služiti kao kriterij ocjene opravdanosti mjere zadiranja. Međutim, taj pojam dovodi do opasnosti da uvjeti zadržavanja podataka i pristup njima na nacionalnoj razini budu vrlo široko utvrđeni, čime se ne bi poštovala temeljna prava iz presude Tele2. Stoga je prilikom donošenja Organskog zakona 13/2015 španjolski zakonodavac, unatoč kriterijima navedenim u presudi Digital Rights[21], znatno snizio, u odnosu na prethodna pravila iz Zakona 25/2007, prag težine kaznenih djela za koje se odobrava zadržavanje i dostavljanje osobnih podataka.

28. Nakon tog odgovora, postupak pred Sudom ponovno je pokrenut 16. veljače 2017. Pisana očitovanja zatim su podnijele španjolska, češka, estonska, irska, francuska, latvijska, mađarska i austrijska vlada, vlada Ujedinjene Kraljevine i Europska komisija.

29. Za potrebe rasprave Sud je postavio pitanja za pisani odgovor španjolskoj vladi, na koja je ona odgovorila 9. siječnja 2018., te pitanja za usmeni odgovor svim zainteresiranim osobama iz članka 23. Statuta Suda Europske unije.

30. Na raspravi održanoj 29. siječnja 2018. španjolsko Državno odvjetništvo, španjolska, češka, danska, estonska, irska, francuska, latvijska i poljska vlada, vlada Ujedinjene Kraljevine i Komisija podnijeli su svoja usmena očitovanja.

IV. Analiza

A. Uvodne napomene

31. Prije temeljitog ispitivanja pitanja postavljenih u ovom zahtjevu za prethodnu odluku, smatram potrebnim iznijeti nekoliko napomena o posebnom predmetu tog zahtjeva.

32. *Kao prvo*, s obzirom na navode iz odluke kojom se upućuje zahtjev za prethodnu odluku i dodatnih informacija koje je dostavila španjolska vlada, ističem da je *glavni postupak* obilježen znatnim posebnostima koje ga razlikuju osobito od konteksta predmetâ u kojima su donesene presude Digital Rights i Tele2[22].

19 Vidjeti bilješku 4. ovog mišljenja.

20 Vidjeti točku 103. presude Tele2 u kojoj se navode „organizirani kriminal i terorizam". Napominjem da je isti dvostruki primjer bio naveden u točkama 24. i 51. presude Digital Rights, koji je očito povezan s tekstom uvodnih izjava 7. do 10. Direktive 2006/24, koja je proglašena nevaljanom u toj presudi.

21 Sud koji je uputio zahtjev osobito navodi točku 60. presude Digital Rights, u kojoj je Sud istaknuo da „Direktiva 2006/24 ne predviđa nikakav objektivni kriterij koji bi omogućio ograničenje pristupa nadležnih nacionalnih tijela podacima i njihove naknadne uporabe u svrhu sprečavanja, otkrivanja ili kaznenih progona koji se odnose na kaznena djela koja se mogu, s obzirom na širinu i ozbiljnost zadiranja u temeljna prava iz članaka 7. i 8. Povelje, smatrati dovoljno teškima za opravdanje takvog zadiranja. Suprotno tome, Direktiva se u članku 1. stavku 1. ograničava na općenito upućivanje na teška kaznena djela koja svaka država članica definira u svojem unutarnjem pravu".

22 U tom pogledu, vidjeti među ostalim bilješke 3. i 4. ovog mišljenja.

33. Naime, zahtjevom policijskih tijela o kojem je ovdje riječ nastoje se dobiti *isključivo* podaci koji omogućuju identifikaciju nositeljâ ili korisnikâ telefonskih brojeva povezanih sa SIM karticama koje su umetnute u ukradeni mobilni telefon [23]. K tome, nesporno je da se taj zahtjev odnosi na jasno određeno i ograničeno razdoblje, odnosno na dvanaestak dana [24].

34. U takvim okolnostima, broj osoba na koje se može odnositi sporna mjera nije neograničen, nego ograničen. K tome, te osobe nisu bilo koji imatelj SIM kartice, nego pojedinci specifičnog profila, s obzirom na to da je riječ o onima koji su upotrebljavali ukradeni telefon nakon što su ga otuđili, ili čak koji ga još uvijek posjeduju i za koje se stoga legitimno može smatrati da su sami počinitelji kaznenog djela ili da su s njima u odnosu.

35. Štoviše, ti podaci ne odgovaraju bilo kojoj vrsti „osobnih podataka" [25] koje zadržavaju pružatelji usluga elektroničkih komunikacija, nego samo onima koji se odnose na osobni identitet gore navedenih pojedinaca, odnosno njihovu imenu i, eventualno, njihovoj adresi [26], podacima koji se također mogu nazvati podacima „za kontakt". Druge informacije o tim pojedincima koje se odnose na te pojedince, a koje se mogu pronaći u arhivima navedenih pružatelja [27], prema mojem su mišljenju isključene iz glavnog postupka.

36. Nadalje, cilj koji se želi postići nije, prema mojem mišljenju, prikupljanje podataka koji se odnose na lokaciju ili komunikaciju kao takve [28], nego na fizičke osobe koje se traži jer su mogle koristiti elektroničku komunikacijsku uslugu s pomoću ukradenog telefona, čak i ako te osobe nisu izvršile konkretan telefonski poziv. Naime, iz objašnjenja koje je Sudu pružilo španjolsko Državno odvjetništvo proizlazi da se zatraženi osobni podaci, koji se dobivaju iz odnosa između određene SIM kartice i broja IMEI ukradenog uređaja, tehnički mogu dobiti zahvaljujući jednostavnoj vezi potonjeg uređaja s pristupnom točkom mobilnoj telefoniji, čak i ako imatelj kartice nije uputio nijedan poziv s predmetnog telefona, stoga neovisno o bilo kakvoj stvarnoj komunikaciji [29]. Na sudu koji je uputio zahtjev je da provjeri tu tvrdnju činjenične naravi, koja mi se ipak čini dovoljno vjerodostojnom da bi bilo razumno smatrati je istinitom.

37. S obzirom na sve te elemente, najprije ističem da se glavni postupak odnosi na osobne podatke čije prosljeđivanje nije zatraženo na opći i neselektivan način, nego ciljano u pogledu osoba i ograničeno u pogledu razdoblja. K tome, zatraženi podaci nisu na prvi pogled osobito osjetljive naravi, iako se na temeljna prava zajamčena člancima 7. i 8. Povelje ipak može utjecati pristupom podacima te vrste [30].

23 Prema mojem mišljenju, „nositelji ili korisnici" iz tog zahtjeva nužno su osobe koje su pretplaćene, registrirane ili koje se barem mogu identificirati (vidjeti također bilješku 25. ovog mišljenja), a ne pojedinci koji su kupili SIM karticu bez ostavljanja traga.

24 Vidjeti točku 20. ovog mišljenja.

25 U skladu s definicijom iz članka 2. točke (a) Direktive 95/46, na koji upućuje članak 2. Direktive 2002/58, pojam „osobni podaci" znači „bilo koji podaci koji se odnose na utvrđenu fizičku osobu ili fizičku osobu koju se može utvrditi", pri čemu je pojašnjeno da je „osoba koja se može utvrditi […] osoba čiji je identitet moguće utvrditi, izravno ili neizravno, a posebno navođenjem identifikacijskog broja ili jednog ili više činitelja značajnih za njegov fizički, fiziološki, mentalni, gospodarski, kulturni ili socijalni identitet". Sud je već istaknuo da se „pravo na poštovanje privatnog života s obzirom na obradu osobnih podataka odnosi na svaku informaciju [koja odgovara toj definiciji]" (vidjeti osobito presudu od 17. listopada 2013., Schwarz, C-291/12, EU:C:2013:670, t. 26.) i da je njezin doseg vrlo širok (vidjeti osobito presudu od 20. prosinca 2017., Nowak, C-434/16, EU:C:2017:994, t. 33.).

26 Prema mišljenju španjolske vlade, adresa zainteresiranih osoba nije bila izričito zatražena.

27 Informacije kao što su, na primjer, bračno stanje pojedinca, broj njegove nacionalne osobne iskaznice, njegovi bankovni podaci ili njegova eventualna telefonska pretplata.

28 Podaci koji se mogu odnositi na brojeve povezane s dolaznim ili odlaznim pozivima, ili pak na datum, trajanje ili učestalost komunikacija, ili čak na njihov sadržaj. Španjolska vlada pojašnjava da je, u ovom slučaju, policija izričito navela da se njihov zahtjev ne odnosi na dobivanje podataka zaštićenih povjerljivošću komuniciranja.

29 Drugim riječima, ti se podaci mogu dobiti jednostavnom aktivacijom predmetnog mobilnog uređaja, bez obzira na to je li ga kasnije njegov nositelj ili imatelj upotrebljavao za određenu međusobnu komunikaciju.

30 Vidjeti točku 74. i sljedeće točke ovog mišljenja.

38. *Kao drugo*, napominjem da iz obrazloženja odluke kojom se upućuje zahtjev za prethodnu odluku proizlazi da su prethodna pitanja postavljena u ovom predmetu specifična po tome da se ne odnose na uvjete *zadržavanja* osobnih podataka u sektoru elektroničkih komunikacija, nego na načine *pristupa* nacionalnih tijela takvim podacima koje su zadržali pružatelji usluga koji djeluju u tom sektoru [31].

39. Sud koji je uputio zahtjev navodi, među ostalim, da se, na temelju članka 588.ter j Zakonika o kaznenom postupku, sudsko odobrenje se zahtijeva za prosljeđivanje elektroničkih podataka koje arhiviraju pružatelji usluga nadležnim tijelima kako bi ih se uzelo u obzir u okviru postupka. Stavkom 1. navedenog članka pojašnjava se da zadržavanje takvih podataka mogu izvršavati pružatelji u skladu s relevantnim zakonodavstvom ili na vlastitu inicijativu, iz poslovnih ili drugih razloga.

40. U ovom slučaju, osobne podatke u pogledu kojih policijska tijela zahtijevaju pristup u svrhu istrage operatori mobilne telefonije mogli su arhivirati u skladu s obvezom koja proizlazi iz španjolskog zakona [32]. Sud koji je uputio zahtjev nije pružio pojašnjenja o tom pitanju, pri čemu se podsjeća da je njegov zahtjev za prethodnu odluku usredotočen na eventualni pristup podacima koji su već zadržani i da je poznato da usklađenost pohranjivanja podataka sa zahtjevima prava Unije nije dovedena u pitanje u glavnom postupku [33]. Stoga se, prema mojem mišljenju, valja osloniti na pretpostavku prema kojoj su podaci o kojima je riječ u glavnom predmetu zadržani u skladu s nacionalnim zakonodavstvom i u skladu s uvjetima utvrđenima u članku 15. stavku 1. Direktive 2002/58, što je isključivo na sudu koji je uputio zahtjev da provjeri [34].

41. U razmatranjima koja slijede vratit ću se na pravne posljedice utvrđenja koja su ovdje uvodno iznesena [35].

B. Postupovni prigovori koje je istaknula španjolska vlada

42. Španjolska vlada istaknula je dvije kategorije postupovnih prigovora od kojih se jedna odnosi na nadležnost Suda, a druga na dopuštenost zahtjeva za prethodnu odluku, na koje će Sud morati odgovoriti prije nego što, ovisno o slučaju, odluči o meritumu.

31 Pojašnjavam da pristup osobnim podacima, u apsolutnom smislu, prema mojem mišljenju ne predstavlja manju opasnost za temeljna prava zajamčena člancima 7. i 8. Povelje od zadržavanja takvih podataka. Opasnost se čak može smatrati većom jer se pristupom zadržanim podacima konkretizira potencijalno štetno korištenje za koje ih se može upotrijebiti.

32 Španjolska vlada navodi da se u Španjolskoj mogu zakonito zadržati ime, prezime i, eventualno, adresa nositelja SIM kartice. Naime, čini mi se da iz članka 1. i članka 3. stavka 1. podstavka (a) točke 1. podtočke ii. Zakona 25/2007 (vidjeti točku 10. i sljedeće točke ovog mišljenja) proizlazi da su operatori mobilne telefonije dužni zadržati podatke koji su dobiveni ili obrađeni u okviru njihova pružanja usluga, osobito ime i adresu pretplatnika ili registriranog korisnika, s obzirom na to da ti podaci mogu biti potrebni kako bi se pronašao i utvrdio izvor komunikacije. Podsjećam da su ekvivalentni zahtjevi navedeni u članku 3. i članku 5. stavku 1. podstavku (a) točki 1. podtočki ii. Direktive 2006/24, koja je prenesena navedeni zakonom.

33 Okolnost koju je i Sud istaknuo u presudi od 29. siječnja 2008., Promusicae (C-275/06, EU:C:2008:54, t. 45. *in fine*).

34 U tom smislu presuda od 19. travnja 2012., Bonnier Audio i dr. (C-461/10, EU:C:2012:219, t. 37.)

35 Osobito, što se tiče nadležnosti Suda i odgovora na prvo prethodno pitanje, vidjeti točku 43. i sljedeće točke odnosno točku 70. i sljedeće točke ovog mišljenja.

1. Nadležnost Suda s obzirom na područje primjene prava Unije

43. Najprije, podsjećam da iz ustaljene sudske prakse proizlazi da se temeljna prava koja se jamče u pravnom sustavu Unije, a osobito ona koja su utvrđena u člancima 7. i 8. Povelje, primjenjuju samo ako je predmetna situacija uređena pravom Unije [36]. K tome, člankom 51. stavkom 1. Povelje predviđa se da se njezine odredbe odnose na države članice samo „kada provode pravo Unije", u smislu sudske prakse Suda koja se odnosi na taj pojam [37]. Prema tome, kada pravna situacija ne ulazi u područje primjene prava Unije, Sud nije nadležan o njoj odlučivati, a odredbe Povelje na koje se eventualno poziva ne mogu same po sebi biti temelj te nadležnosti [38].

44. U ovom slučaju, pitanja koja je postavio sud koji je uputio zahtjev odnose se isključivo na članke 7. i 8. Povelje, kao i na „temeljna načela prava Unije koja je Sud primijenio u svojoj presudi [Digital Rights]". Međutim, taj sud smatra da direktive primjenjive u području zaštite osobnih podataka, kao što su Direktiva 95/46 i Direktiva 2002/58, čine poveznicu koja se na temelju članka 51. stavka 1. Povelje zahtijeva između glavnog predmeta i prava Unije.

45. U tom pogledu, napominjem, *kao prvo*, da španjolska vlada najprije tvrdi da Sud nema potrebnu nadležnost za odlučivanje o ovom zahtjevu za prethodnu odluku jer se potonji zahtjev ne odnosi na primjenu prava Unije. Tvrdi, među ostalim, da je glavni postupak *isključen iz područja primjene prava Unije* jer se odnosi na pristup policije podacima koji u okviru istrage podliježu sudskoj odluci, što je aktivnost države u kaznenim stvarima [39] te je stoga obuhvaćeno izuzećima predviđenim u članku 1. stavku 3. Direktive 2002/58, kao i u članku 3. stavku 2. prvoj alineji Direktive 95/46 [40]. Na raspravi je vlada Ujedinjene Kraljevine navela da se slaže s tim stajalištem španjolske vlade.

46. Međutim, smatram da je Direktiva 2002/58 primjenjiva na nacionalne mjere kao što su one o kojima je riječ u glavnom postupku. Naime, Sud je u presudi Tele2 već presudio da su nacionalna zakonodavstva koja se odnose na zadržavanje podataka u svrhu borbe protiv kriminaliteta obuhvaćena područjem primjene te direktive, ne samo u dijelu u kojem se njima utvrđuju obveze koje u tom smislu imaju pružatelji usluga elektroničkih komunikacija, nego i u dijelu u kojem se njima uređuje pristupa nacionalnih tijela podacima zadržanim u tom okviru [41]. Kao i Komisija, smatram da se razmatranja navedena u toj presudi mogu prenijeti na nacionalna pravila koja su primjenjiva na ovaj slučaj, odnosno ona koja proizlaze iz Zakona 25/2007 u vezi sa španjolskim Zakonikom o kaznenom postupku kako je izmijenjen Organskim zakonom 13/2015 [42], te se stoga mogu prenijeti na predmet glavnog postupka.

47. Dodajem da ne treba miješati, s jedne strane, osobne podatke koji se *izravno* obrađuju u okviru suverenih [43] aktivnosti države, u području koje je obuhvaćeno kaznenim pravom [44] i, s druge strane, osobne podatke koji se obrađuju u okviru poslovnih aktivnosti pružatelja usluga elektroničkih komunikacija koje *potom* upotrebljavaju nadležna državna tijela [45]. Nadalje, napominjem da je Sudu

36 Vidjeti osobito presudu od 16. svibnja 2017., Berlioz Investment Fund (C-682/15, EU:C:2017:373, t. 49. i navedenu sudsku praksu).

37 Vidjeti osobito presudu od 6. listopada 2016., Paoletti i dr. (C-218/15, EU:C:2016:748, t. 14. i sljedeće točke).

38 Vidjeti osobito presudu od 1. prosinca 2016., Daouidi (C-395/15, EU:C:2016:917, t. 63.).

39 Prema mišljenju španjolske vlade, riječ je o izvršenju prava kažnjavanja (*ius puniendi*) koje imaju državna tijela. U tom pogledu, vidjeti mišljenje nezavisnog odvjetnika M. Camposa Sánchez-Bordone u predmetu Breyer (C-582/14, EU:C:2016:339, t. 86. do 92.).

40 Načela navedena u tim odredbama također se spominju u uvodnoj izjavi 11. Direktive 2002/58, u kojoj se upućuje na njezin članak 15. stavak 1. (vidjeti točke 6. i 7. ovog mišljenja).

41 Vidjeti točke 72. do 81. presude Tele2. U tom pogledu, vidjeti također moje mišljenje u spojenim predmetima Tele2 Sverige i dr. (C-203/15 i C-698/15, EU:C:2016:572, t. 88. do 97. i t. 124.).

42 Vidjeti osobito članak 1. stavak 1. Zakona 25/2007 i članak 579. stavak 1. Zakonika o kaznenom postupku, navedene u točkama 11. i 17. ovog mišljenja, kao i, u pogledu zakonske obveze navedenih pružatelja, točku 40. ovog mišljenja.

43 Budući da je pojašnjeno da se takozvane „suverene" aktivnosti države odnose na funkcije namijenjene državi ili njezinim tijelima, ne može ih se povjeriti privatnim subjektima, osobito one koje su povezane s pravosuđem, policijom i vojskom.

44 Kao što su podaci koje obrađuju policijska ili pravosudna tijela s ciljem potrage za počiniteljima kaznenih djela (na primjer, podaci koji se prikupljaju i analiziraju prilikom presretanja telefonskih razgovora koje provode policijski službenici na zahtjev istražnog suca).

45 Kao što su podaci za kontakt korisnikâ telefonskih usluga koji se upotrebljavaju prilikom kaznene istrage, kao u glavnom postupku.

nedavno upućen zahtjev za prethodnu odluku koji se osobito odnosi na tumačenje članka 1. stavka 3. Direktive 2002/58 u kontekstu u kojem službe za sigurnost i informiranje države članice upotrebljavaju podatke koje im takvi pružatelji trebaju skupno dostavljati [46], što je problematika o kojoj, prema mojem mišljenju, ne treba odlučivati u ovom predmetu [47].

48. *Kao drugo*, napominjem da su druga pitanja bila postavljena u pogledu *područja primjene Direktive 2002/58*, o kojoj ovisi nadležnost Suda u ovom predmetu, s obzirom na *vrstu podataka o kojoj je riječ u glavnom postupku*.

49. Kao što sam već naveo [48], iz elemenata uloženih u spis proizlazi da se spornim zahtjevom za pristup nastoje dobiti informacije o identitetu nositeljâ ili korisnikâ brojeva telefona koji odgovaraju SIM karticama koje su aktivirane s pomoću ukradenog mobilnog telefona radi pronalaženja osoba koje su zadržale taj uređaj, a ne podaci o pozivima koji su eventualno obavljeni s tog uređaja.

50. Drugim riječima, čak i ako je širi raspon osobnih podataka eventualno mogao biti obuhvaćen s obzirom na španjolski propis [49], ovaj se glavni postupak odnosi na podatke povezane isključivo s identitetom „korisnikâ" u smislu članka 2. drugog podstavka točke (a) Direktive 2002/58, a ne s bilo kojom „lokacijom" [50] u smislu navedenog članka 2. drugog stavka točke (c), ni sa samim „komunikacijama" u smislu tog istog članka 2. drugog stavka točke (d) [51].

51. Prema mišljenju španjolskog Državnog odvjetništva, španjolske, danske, irske i latvijske vlade, vlade Ujedinjene Kraljevine i Komisije, informacije kao što su one o kojima je ovdje riječ, pod uvjetom da se uzmu u obzir zasebno, odnosno neovisno o eventualno obavljenim komunikacijama, u načelu ne trebaju biti obuhvaćene ni pojmom „podaci o prometu" u smislu navedenog članka 2. drugog stavka točke (b), kojim se potonji podaci definiraju kao „svi podaci koji se obrađuju u svrhu prijenosa komunikacije na elektroničkoj komunikacijskoj mreži ili za njezino naplaćivanje" [52].

52. Točno je da se čini da se identifikacijski podaci koje ovdje zahtijevaju policijska tijela ne odnose na „promet" komunikacija u pravom smislu riječi, s obzirom na to da se ti podaci mogu dobiti unatoč eventualnoj potpunoj odsutnosti poziva obavljenih s pomoću ukradenog uređaja te stoga čak i ako operator mobilne telefonije tijekom ciljanog razdoblja nije prenio nikakvu međusobnu komunikaciju [53].

46 Vidjeti odluku kojom se upućuje zahtjev za prethodnu odluku u predmetu u tijeku Privacy International (C-623/17) u kojoj se, među ostalim, navode presude od 30. svibnja 2006., Parlament/Vijeće i Komisija (C-317/04 i C-318/04, EU:C:2006:346, t. 56. do 59.), kao i od 10. veljače 2009., Irska/Parlament i Vijeće (C-301/06, EU:C:2009:68, t. 88. i 91.), iz kojih proizlazi da se obrada podataka o putnicima u zračnom prometu koji su predmet te prve presude ne zahtijeva radi pružanja usluga, nego radi zaštite javne sigurnosti, te je stoga isključena iz područja primjene Direktive 95/46.

47 Budući da se, s jedne strane, glavni postupak ovdje ne odnosi na skupno, nego na ciljano praćenje podataka te da se, s druge strane, razmatranja Suda u presudi Tele2 prema mojem mišljenju mogu prenijeti na ovaj slučaj, kao što sam naveo u točki 46. ovog mišljenja.

48 Vidjeti točku 33. i sljedeće točke ovog mišljenja.

49 Vidjeti osobito članak 1. stavak 2. Zakona 25/2007 i članak 579. stavak 1. Zakonika o kaznenom postupku.

50 Naime, zahtjevom policijskih tijela ne nastoji se otkriti zemljopisni položaj ukradenog uređaja ili osoba koje su ga zadržale, nego samo identitet potonjih osoba.

51 Odredbe navedenog članka 2. koje su preuzete u točki 8. ovog mišljenja.

52 Podaci o prometu koji su uređeni člankom 6. Direktive 2002/58.

53 Vidjeti točku 36. ovog mišljenja.

53. Međutim, smatram da je spor kao što je onaj u glavnom predmetu obuhvaćen područjem primjene Direktive 2002/58 jer je obrada informacija povezanih sa SIM karticama i njihovim nositeljima o kojima je riječ u ovom slučaju s poslovnog stajališta nužna za pružanje usluga elektroničkih komunikacija [54], barem za naplaćivanje usluge koja je pružena [55], bez obzira na to jesu li pozivi izvršeni u okviru tog pružanja.

54. Naime, s obzirom na članak 1. stavak 1. i članak 3. Direktive 2002/58 [56], slažem se s mišljenjem koje je osobito iznijela Komisija, prema kojem je cilj te direktive općenito uređivanje obrade osobnih podataka koja se provodi u okviru pružanja usluga elektroničkih komunikacija, tako da njezino područje primjene uključuje podatke koji se odnose na identitet korisnika takvih usluga, kao što su oni o kojima je ovdje riječ, a ne samo one koji su povezani s određenom komunikacijom. Uzimajući u obzir i ciljeve zaštite iz navedene direktive, koji se prvenstveno sastoje od zaštite temeljnih prava zajamčenih Poveljom [57], smatram dakle da pojam „komunikacija" u smislu tog instrumenta treba široko tumačiti i da je u ovom slučaju itekako riječ o načelu povjerljivosti komunikacija predviđenom tim instrumentom [58].

55. Također smatram da je to tumačenje potkrijepljeno ranijom presudom Suda, u kojoj je već priznao da područje primjene Direktive 2002/58 obuhvaća spor koji se odnosi na prosljeđivanje imena i adresa korisnika usluge elektroničke komunikacije [59]. Dodajem da se članak 12. navedene direktive, koji se odnosi na telefonske imenike pretplatnika, prema mojem mišljenju zasigurno odnosi na podatke te naravi [60] i da je njezina uvodna izjava 15. također odraz fleksibilnog razumijevanja pojma „komunikacija", koji uključuje, među ostalim, „adres[u] koj[u] pruža pošiljatelj komunikacije" [61].

56. K tome, takav je pristup u skladu sa sudskom praksom ESLJP-a u tom području [62], s obzirom na to da se u preambuli Direktive 2002/58 ističe da se njome nastoji zajamčiti povjerljivost komunikacija i pravo korisnika na privatnost u skladu s EKLJP-om kako ga tumači navedeni sud [63], čak i ako potonji instrument nije formalno integriran u pravni poredak Unije [64].

57. Prema tome, smatram da je spor kao što je onaj u glavnom predmetu obuhvaćen materijalnim područjem primjene Direktive 2002/58 i da prigovor nenadležnosti koji je istaknula španjolska vlada stoga treba odbiti.

58. Radi cjelovitosti, pojašnjavam međutim da, pod pretpostavkom da se Direktiva 2002/58 ne priznaje kao primjenjiva u takvom slučaju, Direktiva 95/46, koju navodi sud koji je uputio zahtjev kao i španjolska vlada, ne može biti temelj nadležnosti Suda za odlučivanje u ovom predmetu.

54 Elektronička komunikacijska usluga u članku 2. točki (c) Direktive 2002/21 (kojom se utvrđuje zajednički regulatorni okvir u tom području) definira se kao „usluga koja se uobičajeno pruža uz naknadu i sastoji se u cijelosti, ili većim dijelom, od prijenosa signala u elektroničkim komunikacijskim mrežama […]".

55 Činjenica da obrada podataka može biti potrebna za naplaćivanje usluge, osobito kada je riječ o pretplatnicima, navedena je u nekoliko odredbi Direktive 2002/58 (među ostalim, u uvodnim izjavama 26., 27. i 29., članku 2. drugom stavku točki (g), kao i članku 6. stavcima 2. i 5.). U tom pogledu, vidjeti i točku 86. presude Tele2 i navedenu sudsku praksu.

56 Odredbe koje se općenito odnose na „obrad[u] osobnih podataka u području elektroničkih komunikacija" odnosno „obradu osobnih podataka u vezi s pružanjem […] elektroničkih komunikacijskih usluga".

57 Vidjeti uvodne izjave 2., 7. i 11., članak 1. stavak 1. i članak 15. stavak 3. Direktive 2002/58.

58 Vidjeti uvodnu izjavu 21., članak 1. stavak 1. i članak 5. Direktive 2002/58, kojim se posebno uređuje povjerljivost komunikacija.

59 Vidjeti presudu od 29. siječnja 2008., Promusicae (C-275/06, EU:C:2008:54, t. 29. do 31. i 45.).

60 U pogledu tumačenja tog članka 12. vidjeti osobito presudu od 15. ožujka 2017., Tele2 (Netherlands) i dr. (C-536/15, EU:C:2017:214, t. 33. i sljedeće točke, kao i navedena sudska praksa).

61 U skladu s navedenom uvodnom izjavom 15, „[k]omunikacija može uključiti informacije o imenu, broju ili adresi koje pruža pošiljatelj komunikacije odnosno korisnik veze s ciljem prijenosa komunikacije […]".

62 Pojam podataka koji se odnose na privatnost pojedinca u smislu članka 8. EKLJP-a (naveden u bilješci 8. ovog mišljenja) ESLJP je tumačio široko (vidjeti osobito presudu ESLJP-a od 13. veljače 2018. Ivašenko protiv Rusije, CE:ECHR:2018:0213JUD006106410, t. 63. i sljedeće točke), kao što je već istaknuto (vidjeti presudu od 9. studenoga 2010., Volker und Markus Schecke i Eifert, C-92/09 i C-93/09, EU:C:2010:662, t. 59. kao i navedena sudska praksa ESLJP-a).

63 Vidjeti uvodne izjave 3., 11. i 24. Direktive 2002/58.

64 Vidjeti osobito presudu Tele2 (točka 120. u kojoj je napravljena usporedba sa sudskom praksom ESLJP-a, kao i točka 126. i sljedeće točke, u kojima se podsjeća na položaj Unije u odnosu na EKLJP).

59. Naime, kao što navodi Komisija, točno je da je Direktiva 95/46 instrument općeg dosega u području obrade osobnih podataka [65], ali pitanja koja je postavio sud koji je uputio zahtjev prema mojem mišljenju nisu relevantna ako se ispituju samo s tog stajališta, s obzirom na to da im je cilj utvrditi prag od kojeg se kaznena djela mogu kvalificirati kao „teška" u smislu sudske prakse koja proizlazi iz presuda Digital Rights i Tele2, koje se ne odnose na tumačenje navedene direktive [66].

2. Dopuštenost zahtjeva za prethodnu odluku

60. Španjolska vlada podredno tvrdi, u slučaju da Sud presudi da je nadležan za odgovaranje na postavljena pitanja, da zahtjev za prethodnu odluku treba proglasiti nedopuštenim, i to iz dva razloga.

61. *Kao prvo*, ta vlada tvrdi da sud koji je uputio zahtjev *nije jasno utvrdio normativni okvir Unije* o kojem Sud treba odlučiti.

62. U tom pogledu podsjeća na ustaljenu sudsku praksu prema kojoj, u okviru suradnje uspostavljene člankom 267. UFEU-a, Sud može odbiti odlučiti o prethodnim pitanjima, koja uživaju presumpciju relevantnosti, samo ako je očito da zatraženo tumačenje ili ocjena valjanosti pravila Unije nema nikakve veze s činjeničnim stanjem ili predmetom spora u glavnom postupku, ako je problem hipotetski ili ako Sud ne raspolaže činjeničnim i pravnim elementima potrebnima da bi se mogao dati koristan odgovor na upućena pitanja [67].

63. Međutim, smatram da u ovom slučaju prigovor koji je istaknula španjolska vlada nije osnovan. Naime, s obzirom na navode suda koji je uputio zahtjev, smatram da je taj sud dostatno utvrdio odredbe prava Unije koje su prema njegovu mišljenju relevantne. Podsjećam, s jedne strane, da se postavljena pitanja osobito odnose na članke 7. i 8. Povelje, s druge strane, da taj sud navodi da su direktive 95/46 i 2002/58 potrebna poveznica između nacionalnog zakonodavstva primjenjivog u glavnom predmetu i prava Unije [68] te, konačno, da Direktiva 2002/58 posebno traži, kao što je navedeno u njezinoj uvodnoj izjavi 2., osiguranje punoga poštovanja prava određenih u člancima 7. i 8. Povelje [69].

64. Dodajem da nije važno to što je cilj jednog od elemenata španjolskih propisa navedenih u odluci kojom se upućuje zahtjev za prethodnu odluku, odnosno Zakona 25/2007, prenošenje Direktive 2006/24, koja je stavljena izvan snage nakon što je u presudi Digital Rights proglašena nevaljanom [70]. Kao što pravilno navodi sud koji je uputio zahtjev, nije točno smatrati da prethodna pitanja koja se ovdje upućuju Sudu nisu relevantna zbog navedenog proglašenja nevaljanosti. U tom pogledu, dovoljno je utvrditi da je područje na koje se odnose ta pitanja, odnosno zaštita osobnih podataka, obuhvaćeno područjem nadležnosti Unije i da je glavni postupak obuhvaćen područjem primjene akta prava Unije, odnosno Direktive 2002/58 [71], koja je trebala biti izmijenjena Direktivom 2006/24 koja je proglašena nevaljanom.

65 Dok se Direktivom 2002/58 uređuje konkretan sektor elektroničkih komunikacija (vidjeti osobito njezine uvodne izjave 4. i 10. te članak 1. stavke 1. i 2.).

66 Podsjećam da je pojam „teška kaznena djela" kao ograničavajući kriterij djelovanja država članica uveden Direktivom 2006/24 o zadržavanju podataka, koja je presudom Digital Rights proglašena nevaljanom, te ga je Sud potom upotrijebio u presudi Tele2 za tumačenje odredbi Direktive 2002/58 u kontekstu nacionalnih propisa o zadržavanju podataka i pristupu tim podacima (vidjeti također bilješke 3. i 4. ovog mišljenja). Iz toga, prema mojem mišljenju, proizlazi da, ako se Direktivu 2002/58 proglasi neprimjenjivom na ovaj slučaj, neće biti potrebno tumačenje navedenog pojma, koje je zatražio sud koji je uputio zahtjev.

67 Vidjeti osobito presude od 16. lipnja 2015., Gauweiler i dr. (C-62/14, EU:C:2015:400, t. 24. i 25.), kao i od 22. veljače 2018., Porras Guisado (C-103/16, EU:C:2018:99, t. 34.).

68 Vidjeti i točku 44. ovog mišljenja.

69 Vidjeti također presudu Tele2 (t. 82.).

70 Vidjeti i točku 10. ovog mišljenja. Napominjem da je situacija bila slična u jednom od predmeta u kojima je donesena presuda Tele2 (vidjeti točke 15. i 63.).

71 U tom potonjem pogledu, vidjeti točku 45. i sljedeće točke ovog mišljenja.

65. Uostalom, može se primijetiti da velika većina stranaka koje su podnijele očitovanja Sudu polaze od načela da ovaj zahtjev za prethodnu odluku valja ispitati s obzirom na članak 15. stavak 1. Direktive 2002/58 u vezi s člancima 7. i 8. Povelje, kao i na temelju zaključaka koji proizlaze iz presuda Digital Rights i Tele2. To je i moje mišljenje, s obzirom na to da je pojašnjeno da se izraz „kaznena djela", a ne „teška kaznena djela" u Direktivi 2002/58 navodi isključivo u navedenom članku 15. stavku 1.[72].

66. *Kao drugo*, španjolska vlada tvrdi da *članak 7. Povelje*, koji je ključan element ovog zahtjeva za prethodnu odluku, *nije relevantan* jer se istražna mjera zatražena u glavnom predmetu ne odnosi na presretanje komunikacija te stoga ne može utjecati na povjerljivost komunikacija, tako da su postavljena pitanja hipotetska.

67. Ja pak smatram da je članak 7. Povelje itekako relevantan u ovom predmetu i da zahtjev za prethodnu odluku stoga nije hipotetske naravi. Iako je točno da u ovom slučaju ne postoji opasnost od povrede prava na povjerljivost komunikacija, s obzirom na predmet mjere o kojoj je riječ u glavnom postupku[73], ipak ostaje činjenica da se mjerom te vrste može povrijediti pravo na poštovanje privatnog života koje je zajamčeno navedenom odredbom, čak i ako je ta povreda, prema mojem mišljenju, malih razmjera[74].

68. Naime, kao što je Sud već ranije ustaljeno presuđivao, 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, osobito od strane pružatelja usluga elektroničkih komunikacija, te za pristup tim podacima kako bi se njima koristila javna tijela[75].

69. Prema tome, smatram da prigovor nedopuštenosti koji je istaknula španjolska vlada treba odbiti te da stoga valja odlučiti o meritumu zahtjeva za prethodnu odluku.

C. Elementi potrebni za utvrđivanje dovoljne težine kaznenog djela kojom se opravdava zadiranje u navedena temeljna prava (prvo pitanje)

70. Svojim prvim prethodnim pitanjem, sud koji je uputio zahtjev u biti pita Sud o elementima koje treba uzeti u obzir prilikom utvrđivanja jesu li kaznena djela dovoljno teška kako bi se opravdalo ograničenjetemeljnih prava zajamčenih člancima 7. i 8. Povelje u okviru zadržavanja osobnih podataka i pristupa njima, u skladu sa sudskom praksom koja proizlazi iz presude Digital Rights te potom iz presude Tele2.

72 Vidjeti i točku 71. ovog mišljenja.

73 Vidjeti točke 36. i 52. ovog mišljenja

74 U pogledu nepostojanja ozbiljnosti zadiranja u ovom slučaju, vidjeti točku 74. i sljedeće točke ovog mišljenja.

75 Vidjeti osobito presudu Digital Rights (t. 26. i sljedeće točke) kao i mišljenje 1/15 (Sporazum o PNR-u između EU-a i Kanade) od 26. srpnja 2017. (EU:C:2017:592, t. 124. i navedena sudska praksa).

71. U tom pogledu, podsjećam da je pojam „teška kaznena djela" Sud upotrijebio u presudi Digital Rights [76], katkad zajedno s pojmom „teški kriminal" [77], kao kriterij provjere svrhe i proporcionalnosti zadiranja u gore navedena temeljna prava koje proizlazi iz odredbi prava Unije o osobnim podacima, odnosno odredaba Direktive 2006/24. Pojašnjavam da je taj pojam, koji se ne navodi u Direktivi 2002/58 [78], bio upotrijebljen u Direktivi 2006/24 [79], čija je nevaljanost bila predmet navedene presude. Sud je potom ta dva pojma upotrijebio u presudi Tele2 [80] kao isti kriterij ocjene, ali se taj put odnosio na usklađenost odredbi koje su donijele države članice s pravom Unije [81].

72. Konkretnije, prvim se prethodnim pitanjem Sud poziva da odluči treba li, u svrhu ocjene postojanja „teškog kaznenog djela" kojim se može opravdati zadiranje u temeljna prava zajamčena člancima 7. i 8. Povelje u pogledu osobnih podataka, uzeti u obzir isključivo kaznu izrečenu za sporno kazneno djelo ili, štoviše, osobito štetnu narav protupravnog postupanja u pogledu pravnih interesa pojedinaca i kolektiva.

73. Međutim, kao i Komisija, smatram da prije odlučivanja o tom pitanju valja ispitati predstavlja li zadiranje o kojem je riječ u sporu kao što je onaj u glavnom postupku dovoljno visok stupanj ozbiljnosti da bi se na temelju prava Unije zahtijevalo da to zadiranje bude opravdano borbom protiv teškog kaznenog djela kako bi ga se moglo prihvatiti. Naime, smatram da, ako to nije slučaj, Sud mora tumačiti relevantne odredbe prava Unije ne na način da se pridržava tumačenja koje je zatražio sud koji je uputio zahtjev, nego nakon što preoblikuje prvo postavljeno pitanje [82] koliko je potrebno s obzirom na okolnosti glavnog postupka [83].

1. Uzimanje u obzir nepostojanja ozbiljnosti spornog zadiranja

74. *Najprije* valja utvrditi da se postupcima kao što su oni o kojima je riječ u glavnom postupku itekako mogu povrijediti temeljna prava zajamčena člancima 7. i 8. Povelje te stoga mogu *činiti zadiranje* u ta prava u smislu sudske prakse koja proizlazi iz presuda Digital Rights i Tele2.

75. Točno je da je, kao što su španjolska i danska vlada navele u svojem izlaganju [84] i kao što sam već napomenuo [85], narav podataka kojima tijela zadužena za predmetnu kaznenu istragu žele imati pristup izgleda manje osjetljiva nego u slučaju određenih drugih kategorija osobnih podataka [86], uzimajući u obzir da se predmetni zahtjev odnosi samo na ime, prezime i, eventualno, adresu pojedinaca na koje je ta istraga usmjerena, kao korisnika brojeva telefona koji su aktivirani s ukradenog mobilnog telefona koji je predmet te istrage.

76 Vidjeti točke 24., 41., 49. i 57. do 61. presude Digital Rights.

77 Vidjeti točke 41., 42., 51. i 59. presude Digital Rights.

78 Budući da se u Direktivi 2002/58 navodi samo izraz „kaznena djela", u njezinoj prvoj rečenici članka 15. stavka 1.

79 U biti, u uvodnoj izjavi 9. Direktive 2006/24, kao i, doslovno, u uvodnoj izjavi 21. i u članku 1. stavku 1. te direktive.

80 Vidjeti, što se tiče pojma „teška kaznena djela", točke 105., 106. i 119. te, što se tiče pojma „teški kriminal", točke 102., 103., 108., 110., 111., 114., 115., 118., 125. i 134. presude Tele2.

81 Odnosno, članak 15. stavak 1. Direktive 2002/58, na temelju kojeg države članice mogu donijeti mjeru kojom se odstupa od načela povjerljivosti komunikacija i s njima povezanih podataka o prometu kad ona predstavlja nužnu, prikladnu i razmjernu mjeru unutar demokratskog društva s obzirom na ciljeve utvrđene tom odredbom.

82 Budući da se drugo prethodno pitanje postavlja tek podredno.

83 Iz ustaljene sudske prakse proizlazi da radi pružanja korisnog odgovora sudu koji je uputio zahtjev, koji će mu omogućiti da riješi spor koji se pred njim vodi, Sud mora, ako je potrebno, preoblikovati postavljena pitanja (vidjeti osobito presudu od 22. veljače 2018., SAKSA, C-185/17, EU:C:2018:108, t. 28.).

84 Španjolska vlada naglasila je da podaci koju su predmet spora u glavnom postupku ne omogućuju utvrđivanje, na primjer, profila dotične osobe.

85 Vidjeti točke 35. do 37. ovog mišljenja.

86 Podsjećam da se člankom 8. Direktive 95/46 predviđaju posebna pravila za obradu „osobnih podataka kojima se otkriva rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, članstvo u sindikatu i obradu podataka u vezi sa zdravljem ili spolnim životom". U pogledu pojma osjetljivih podataka i njihove obrade, vidjeti *Priručnik o europskom zakonodavstvu o zaštiti podataka*, koji su priredili Agencija Europske unije za temeljna prava i Vijeće Europe, 2014., ažurirana verzija dostupna na sljedećoj internetskoj adresi: https://www.coe.int/fr/web/data-protection/home, str. 46. i sljedeće stranice te str. 94. i sljedeće stranice.

76. Međutim, smatram da za utvrđivanje trebaju li osobni podaci biti obuhvaćeni zaštitom predviđenom u pravu Unije te osobito Direktivom 2002/58[87] nije važno jesu li informacije na koje se odnosi zahtjev za zadržavanje ili komunikaciju osobito osjetljive. Naime, kao što je istaknuto u okviru prvih zakonodavnih akata u tom području, „u skladu sa svrhom njihove uporabe, svi podaci o osobi, čak i oni koji se čine da nisu štetni, mogu biti osjetljive naravi (kao što je, na primjer, obična poštanska adresa)"[88]. Štoviše, Sud je već presudio da radi utvrđivanja *postojanja zadiranja* u temeljno pravo zajamčeno člankom 7. Povelje, „nevažno [je] imaju li dotične informacije o privatnom životu osjetljiv karakter, odnosno jesu li zainteresirane osobe zbog tog zadiranja pretrpjele eventualne neugodnosti"[89].

77. Nadalje, podsjećam da je dostavljanje osobnih podataka trećoj osobi, čak i javnom tijelu kao što je služba policije, zadiranje u temeljno pravo zajamčeno člankom 7. Povelje[90], uključujući ako se te informacije proslijeđuju radi kaznene istrage, što je situacija koja je uostalom izričito navedena u članku 15. stavku 1. Direktive 2002/58[91]. Dodajem da se takvim postupkom također može povrijediti temeljno pravo na zaštitu osobnih podataka zajamčeno u članku 8. Povelje s obzirom na to da predviđa obradu osobnih podataka[92].

78. Stoga, smatram da treba utvrditi da mjera kao što je ona o kojoj je riječ u glavnom postupku čini zadiranje u temeljna prava zajamčena člancima 7. i 8. Povelje.

79. *Međutim*, smatram da u predmetnim okolnostima nedostaje ključni element koji je Sud primijenio kako bi se u fazi opravdavanja takvog zadiranja zahtijevalo postojanje „teškog kaznenog djela", pojam čiju je definiciju zatražio sud koji je uputio zahtjev, kako bi se moglo odstupiti od načela povjerljivosti elektroničkih komunikacija. Element koji u ovom slučaju, prema mojem mišljenju, *nedostaje* kako bi se odgovorilo na prvo prethodno pitanje riječima koje je upotrijebio taj sud jest *ozbiljnost spornog zadiranja*, čimbenik koji bi, da je prisutan, doveo do potrebe za obrazloženijim opravdanjem.

80. U tom pogledu, ističem da je Sud u presudi Digital Rights naglasio široku i osobito tešku narav zadiranja koje proizlazi iz predmetnog propisa time što je osobito istaknuo da „Direktiva 2006/24 na općenit način obuhvaća svaku osobu i sva sredstva elektroničke komunikacije kao i sve podatke o prometu bez ikakvog razlikovanja, ograničenja ili iznimke s obzirom na cilj borbe protiv teških kaznenih djela"[93].

81. Na sličan način, Sud je u presudi Tele2 odlučio da se „član[ku] 15. stav[ku] 1. Direktive 2002/58 […] protivi nacionalni propis poput onoga u glavnom postupku, koji 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"[94]. U toj je presudi također

87 Osjetljiv karakter određenih podataka navodi se samo u uvodnoj izjavi 25. Direktive 2002/58, a da se iz njega ne može zaključiti da je riječ o općem zahtjevu.

88 Vidjeti Komunikaciju Komisije od 13. rujna 1990. o zaštiti osoba u pogledu obrade osobnih podataka u Zajednici i o sigurnosti informacijskih sustava [COM(90) 314 *final*, str. 20.].

89 Vidjeti mišljenje 1/15 (Sporazum o PNR-u između EU-a i Kanade) od 26. srpnja 2017. (EU:C:2017:592, t. 124. i navedena sudska praksa). ESLJP je također odlučio u tom smislu (vidjeti presudu ESLJP-a od 16. veljače 2000. Amann protiv Švicarske, CE:ECHR:2000:0216JUD002779895, t. 68. do 70.).

90 Vidjeti točku 68. ovog mišljenja. Vidjeti također presudu ESLJP-a od 8. veljače 2018. Ben Faiza protiv Francuske, (CE:ECHR:2018:0208JUD003144612, t. 66. do 68.), u pogledu sudskog zahtjeva koji se odnosi na dostavljanje informacija o uporabi telefona.

91 Na sljedeći način: „s ciljem sprečavanja, istrage, otkrivanja i progona kaznenih djela".

92 Vidjeti u tom smislu mišljenje 1/15 (Sporazum o PNR-u između EU-a i Kanade) od 26. srpnja 2017. (EU:C:2017:592, t. 126. i navedena sudska praksa).

93 Točka 57. presude Digital Rights. U pogledu osobite ozbiljnosti predmetnog zadiranja vidjeti također točke 37., 39., 47., 48., 60. i 65. te presude.

94 Točka 1. izreke presude Tele2

uspostavljena veza između, s jedne strane, osobite „ozbiljnosti zadiranja" koja je tako utvrđena i, s druge strane, potrebe da se opravda ograničenje temeljnih prava takvog dosega zajamčenih člancima 7. i 8. Povelje, koje se temelji na razlogu od općeg interesa koji je jednako važan kao i „borba protiv teških kaznenih djela" [95].

82. Takva veza između ozbiljnosti utvrđenog zadiranja i ozbiljnosti razloga kojim se omogućuje njegovo opravdavanje uspostavljena je u skladu s načelom proporcionalnosti [96]. Štoviše, smatram da je ESLJP u svojoj sudskoj praksi koja se odnosi na članak 8. EKLJP-a [97] utvrdio vezu koja je ekvivalentna onoj koja, prema mojem mišljenju, proizlazi iz presuda Digital Rights i Tele2.

83. Međutim, kao što sam prethodno naveo [98] i kao što su, konkretnije, istaknule francuska vlada, vlada Ujedinjene Kraljevine i Komisija, narav zadiranja o kojoj je riječ u ovom glavnom postupku je, s više stajališta, različita od onih koje je Sud predvidio u tim dvjema prethodnim presudama. Stoga treba drukčije ispitati usklađenost s pravom Unije mjere kao što je ona o kojoj je ovdje riječ.

84. U ovom slučaju nije riječ o mjeri koja se odnosi na obvezu općeg i neselektivnog zadržavanja podataka o prometu i lokaciji svih pretplatnika ili registriranih korisnika u pogledu svih sredstava elektroničke komunikacije. Riječ je o ciljanoj mjeri kojom se nadležnim tijelima u svrhu kaznene istrage nastoji omogućiti pristup podacima koje su pružatelji usluga zadržali iz poslovnih razloga i koji se odnose isključivo na identitet (ime, prezime i eventualno adresu) ograničene kategorije pretplatnika ili korisnika konkretnog komunikacijskog sredstva, odnosno onih čiji je broj telefona bio aktiviran s mobilnog telefona čija je krađa predmet istrage, i to tijekom ograničenog razdoblja, odnosno tijekom dvanaestak dana [99].

85. Dodajem da su potencijalno štetni učinci za osobe na koje se odnosi predmetni zahtjev za pristup istovremeno umjereni i ograničeni. Naime, budući da se upotrebljavaju u jedinstvenom okviru istražne mjere, zatraženi podaci nisu namijenjeni otkrivanju široj javnosti [100]. Štoviše, na mogućnost pristupa koja se nudi policijskim tijelima odnose se postupovna jamstva na temelju španjolskog prava, s obzirom na to da iz nje proizlazi sudski nadzor koji je uostalom doveo do odbijanja zahtjeva policije u glavnom postupku.

95 U skladu s točkom 102. presude Tele2, *„[s] obzirom na ozbiljnost zadiranja* u predmetna temeljna prava utvrđenog nacionalnim propisom, koji u svrhu borbe protiv kriminaliteta određuje zadržavanje podataka o prometu i lokaciji, *samo borba protiv teških kaznenih djela može opravdati takvu mjeru* (vidjeti analogijom, u pogledu Direktive 2006/24, presudu Digital Rights, t. 60. [u kojoj se navodi izraz *‚s obzirom na širinu i ozbiljnost zadiranja'*])" (moje isticanje). U točki 115. presude Tele2 preuzima se to rasuđivanje u pogledu *pristupa* takvim podacima. U pogledu osobite ozbiljnosti predmetnog zadiranja vidjeti također točke 97. i 100. te presude.

96 Stoga, u točki 115. presude Tele2 ističe se da, *„budući da cilj [nacionalnog propisa kojim se odstupa od načela povjerljivosti elektroničkih komunikacija] mora biti u vezi s ozbiljnošću zadiranja* u temeljna prava koje uzrokuje taj pristup, slijedi da u području sprečavanja, istrage, otkrivanja i progona kaznenih djela *samo borba protiv teških kaznenih djela može opravdati takav pristup* zadržanim podacima" (moje isticanje).

97 Naime, taj je sud u više navrata istaknuo potrebu za *odvagivanjem*, s jedne strane, interesa države da zaštiti svoju *nacionalnu sigurnost* mjerama koje utječu na osobne podatke i, s druge strane, *ozbiljnosti povrede* prava pojedinca u pogledu njegove privatnosti, što su dva čimbenika o kojima ovisi margina prosudbe države, osobito kada potonja država nastoji spriječiti ili progoniti *teška kaznena djela* (vidjeti presudu ESLJP-a od 26. ožujka 1987. Leander protiv Švedske, CE:ECHR:1987:0326JUD000924881, t. 59.; presudu ESLJP-a od 26. lipnja 2006. Weber i Saravia protiv Njemačke, CE:ECHR:2006:0629DEC005493400, t. 106., 125. i 126., kao i presudu ESLJP-a od 4. prosinca 2015. Roman Zakharov protiv Rusije, CE:ECHR:2015:1204JUD004714306, t. 232. i 244.).

98 Vidjeti točku 32. i sljedeće točke ovog mišljenja.

99 Napominjem da je u mišljenju 1/15 (Sporazum o PNR-u između EU-a i Kanade) od 26. srpnja 2017. (EU:C:2017:592, osobito točke 194. i 207. do 209.) Sud također ocijenio nužnost zadiranja koje sadržava predviđeni sporazum time što je ispitao načine uporabe i zadržavanja podataka koji su u tom sporazumu predviđeni, osobito sa stajališta konkretnog konteksta tih mjera, njihovih specifičnosti i njihova trajanja.

100 Kao što to na primjer može biti u slučaju identiteta osoba koji se objavljuje u novinskom članku ili na internetskoj stranici.

86. Zadiranje u gore navedena temeljna prava do kojeg dolazi dostavljanjem tih podataka o osobnom identitetu, prema mojem mišljenju, nije osobito ozbiljno [101] jer podaci takve naravi i tako ograničenog dosega sami po sebi ne omogućuju dobivanje različitih i/ili preciznih podataka o dotičnim osobama [102] te stoga ne utječu izravno i izrazito na intimnost njihova privatnog života u tim osobitim okolnostima [103].

87. *Prema tome*, kao i Komisija, smatram da, kako bi se sudu koji je uputio zahtjev pružilo relevantne naznake za odlučivanje o sporu koji je pred njim pokrenut, valja *preoblikovati* prvo prethodno pitanje tako da se odgovor koji Sud treba pružiti odnosi na tumačenje članka 15. stavka 1. Direktive 2002/58 s obzirom na okolnosti kao što su one u ovom slučaju, odnosno uz postojanje zadiranja u gore navedena temeljna prava, koje nije osobito ozbiljno i koje se temelji na borbi protiv vrste kaznenih djela čija se težina dovodi u pitanje.

88. U tom pogledu, podsjećam da, s obzirom na to da su ciljevi kojima se može opravdati nacionalno zakonodavstvo kojim se odstupa od načela povjerljivosti elektroničkih komunikacija taksativno nabrojani u članku 15. stavku 1. Direktive 2002/58, pristup zadržanim podacima treba stvarno i strogo odgovarati jednom od navedenih ciljeva [104]. Među potonjim ciljevima naveden je cilj od općeg interesa „sprečavanja, istrage, otkrivanja i progona *kaznenih djela*” [105], bez dodatnog pojašnjenja u pogledu njihove naravi.

89. Iz tako upotrijebljene terminologije proizlazi da nije nužno da se kaznena djela kojima se opravdava predmetna mjera ograničavanja na temelju navedenog članka 15. stavka 1. mogu kvalificirati kao „teška” u smislu sudske prakse koja proizlazi iz presuda Digital Rights i Tele2. Prema mojem mišljenju, isključivo ako je pretrpljeno zadiranje osobito ozbiljno, kao u predmetima u kojima su donesene navedene presude, tada sama kaznena djela kojima se može opravdati takvo zadiranje trebaju biti osobito teška. Suprotno tomu, u slučaju u kojem zadiranje nije ozbiljno valja ponovno primijeniti temeljno načelo koje proizlazi iz teksta te odredbe, odnosno da se svakom vrstom „kaznenih djela” može opravdati takvo zadiranje.

90. Prema mojem mišljenju, treba osigurati da se ne tumače preširoko zahtjevi koje je Sud utvrdio u tim dvjema presudama, kako se ne bi spriječila, barem ne pretjerano, mogućnost država članica da odstupaju od sustava uspostavljenog Direktivom 2002/58, koja im je dodijeljena člankom 15. stavkom 1. te direktive, u slučajevima u kojima zadiranja u predmetnu privatnost istovremeno imaju legitimnu svrhu i ograničen doseg, kao što su ona koja u ovom slučaju mogu proizlaziti iz zahtjeva službe policije. Konkretnije, smatram da se pravu Unije ne protivi mogućnost nadležnih tijela da pristupe identifikacijskim podacima koje zadržavaju pružatelji usluga elektroničkih komunikacija i koji omogućavaju pronalaženje navodnih počinitelja kaznenog djela koje nije teško.

91. Prema tome, predlažem Sudu da *na prethodno pitanje, kako je preoblikovano, odgovori* da članak 15. stavak 1. Direktive 2002/58, u vezi s člancima 7. i 8. te člankom 52. stavkom 1. Povelje, treba tumačiti na način da mjera kojom se nadležnim nacionalnim tijelima omogućuje da, u svrhu borbe protiv kaznenih djela, imaju pristup identifikacijskim podacima korisnika telefonskih brojeva

101 U tom smislu vidjeti Konvenciju o kiberkriminalitetu sklopljenu pod okriljem Vijeća Europe u Budimpešti 23. studenoga 2001. koju su potpisale sve države članice Unije (dostupno na sljedećoj internetskoj adresi: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?_coeconventions_WAR_coeconventionsportlet_languageId=fr_FR), u čijem se članku 18. nalaže donošenje zakonodavnih mjera kojima će se nadležnim tijelima omogućiti da pružatelju usluga nalože da im dostavi podatke koji se odnose na pretplatnike, kao što su „identitet, adresa […] i broj telefona”, a koje on posjeduje.

102 Kao što je danska vlada pravilno istaknula, kada policija dobije, kao u ovom slučaju, podatke o imenu i adresi vlasnika SIM kartice koja je upotrijebljena u okviru kaznenog djela, to nije bitno drukčije od, na primjer, dobivanja informacija koje se odnose na vlasnika vozila upotrijebljenog za počinjenje kaznenog djela.

103 Za razliku od informacija koje su osobito invazivne, među ostalim u pogledu praćenja komunikacija i profila dotičnih osoba, o kojima je bila riječ u predmetima u kojima su donesene presude Digital Rights (vidjeti točke 26. do 29. i 37.) i Tele2 (vidjeti točke 97. do 100.).

104 Vidjeti osobito točke 90. i 115. presude Tele2.

105 Moje isticanje

aktiviranih s određenog mobilnog telefona i tijekom ograničenog razdoblja, u okolnostima kao što su one u glavnom postupku, dovodi do zadiranja u temeljna prava zajamčena navedenom direktivom i Poveljom, koje nije dovoljno ozbiljno da bi takav pristup trebalo ograničiti na slučajeve u kojima je predmetno kazneno djelo teško.

92. S obzirom na tako predložen odgovor, sva ću sljedeća razmatranja, radi cjelovitosti, iznijeti samo *podredno*.

2. Eventualno određivanje kriterija relevantnih za utvrđivanje dovoljne težine kaznenog djela

93. U slučaju da Sud presudi, suprotno onome što predlažem, da bez obzira na izrazito posebne okolnosti ovog glavnog postupka u ovom predmetu valja utvrditi što treba smatrati „teškim kaznenim djelom" u smislu sudske prakse koja proizlazi iz presuda Digital Rights i Tele2[106], potrebno je još postaviti pitanje, *kao prvo*, o tome je li ta kvalifikacija *autonoman pojam* prava Unije, čije bi definiranje onda bilo na Sudu. Međutim, u skladu s odgovorom koji je najprije predložila francuska vlada, ne slažem se s tim stajalištem iz sljedećih razloga.

94. Najprije, napominjem da Direktiva 2006/24, iz koje proizlazi uporaba pojma „teško kazneno djelo"[107], nije sadržavala definiciju tog pojma, nego je o tom pitanju upućivala na pravne poretke država članica[108]. Dodajem da se relevantna razmatranja koja se navode u presudama Digital Rights i Tele2 ne trebaju shvaćati, prema mojem mišljenju, kao da se njima nastoje uskladiti pravna pravila na snazi u državama članicama koja se odnose na sadržaj tog pojma.

95. U tom pogledu, podsjećam da su kazneno zakonodavstvo i pravila o kaznenom postupku obuhvaćeni nadležnošću država članica, čak i ako na pravni poredak potonjih država ipak mogu utjecati odredbe prava Unije koje su donesene u tom području[109]. U skladu s člankom 83. stavkom 2. UFEU-a, samo ako se pokaže da je za osiguranje učinkovite provedbe politike Unije u području koje podliježe mjerama usklađivanja nužno usklađivanje kaznenog prava država članica, Unija može donijeti direktive kojima je cilj utvrditi minimalna pravila za definiranje kaznenih djela i sankcija u dotičnom području. Međutim, u trenutačnom stanju prava Unije ne postoji odredba općeg dosega kojom bi se usklađeno definirao pojam „teško kazneno djelo"[110].

96. Smatram da je ovlast za utvrđivanje onoga što čini „teško kazneno djelo", u načelu, na nadležnim tijelima država članica. Neovisno o tome, Sud je dužan, zahvaljujući zahtjevima za prethodnu odluku koje mu sudovi država članica mogu uputiti, osigurati poštovanje svih zahtjeva koji proizlaze iz prava Unije te, među ostalim, osigurati dosljednu primjenu zaštite koja se nudi odredbama Povelje.

97. Ističem da ne samo da se predmetna pravna kvalifikacija može razlikovati ovisno o državi članici, u skladu s običajima i prioritetima koje je svaka od njih utvrdila, nego se također s vremenom može mijenjati, u skladu sa smjernicama koje se donose u kaznenoj politici, u više ili manje stroge, kako bi se uzeo u obzir razvoj kriminala,[111] kao i, općenitije, promjene društva i potrebe koje postoje na nacionalnoj razini, osobito u smislu kaznenog progona.

106 Odnosno u slučaju da Sud smatra da je zadiranje o kojem je riječ u glavnom postupku dovoljno ozbiljno da se na prvo pitanje odgovori kako ga je postavio sud koji je uputio zahtjev ili da u tom pogledu nije važno što navedeno zadiranje nije ozbiljno.

107 Vidjeti točku 71. ovog mišljenja.

108 U članku 1. stavku 1. Direktive 2006/24 navodi se da je njezin cilj „uskladiti odredbe država članica koje se odnose na obveze pružatelja […] elektroničkih komunikacijskih usluga […], kako bi se osiguralo da ti podaci budu dostupni u svrhu istrage, otkrivanja i progona *teških kaznenih djela, kako su određena nacionalnim zakonodavstvom svake države članice*" (moje isticanje). Vidjeti također uvodnu izjavu 21. te direktive.

109 Vidjeti osobito presude od 15. rujna 2011., Dickinger i Ömer (C-347/09, EU:C:2011:582, t. 31.), kao i od 6. prosinca 2011., Achughbabian (C-329/11, EU:C:2011:807, t. 33.).

110 U tom pogledu, vidjeti također točku 112. ovog mišljenja.

111 U pogledu dinamičnosti teških kaznenih djela, vidjeti također moje mišljenje u spojenim predmetima Tele2 Sverige i dr. (C-203/15 i C-698/15, EU:C:2016:572, t. 214.).

98. K tome ističem da, s obzirom na to da postoje velike razlike u rasponima kazni koje se uobičajeno primjenjuju u različitim državama članicama [112], težina kaznenog djela nije povezana samo s povezanom težinom kazne. Pitanje je li kazneno djelo teško vrlo je relativno u smislu da ovisi o rasponu kazni koje se općenito primjenjuju u predmetnoj državi članici. Stoga, činjenicom da država članica predviđa nisku zatvorsku kaznu, ili čak kaznu kojom se zamjenjuje zatvorska kazna, ne dovodi se stoga u pitanje stvarna težina predmetne vrste kaznenog djela [113].

99. Prema mojem mišljenju, valja poštovati osobitosti sustava kaznenog prava svake države članice ako se pravom Unije za njih ne utvrđuju stroge obveze, po analogiji s onime što je Sud presudio u pogledu zaštite javne sigurnosti [114], pojma koji je prema mojem mišljenju sličan pojmu borbe protiv teškog kriminala, osobito s obzirom na tekst prve rečenice članka 15. stavka 1. Direktive 2002/58.

100. Prema tome, podredno smatram da pojam „teško kazneno djelo" u smislu sudske prakse Suda koja proizlazi iz presuda Digital Rights i Tele2 nije autonoman pojam prava Unije čiji sadržaj treba definirati Sud, čak ni ako je činjenica da odstupanje predviđeno člankom 15. stavkom 1. Direktive 2002/58 trebaju provesti države članice u skladu s obvezama koje proizlaze iz prava Unije, osobito iz temeljnih prava zajamčenih Poveljom i to pod nadzorom Suda.

101. U tom potonjem pogledu iz sudske prakse Suda proizlazi, među ostalim, da navedeni članak 15. stavak 1., u dijelu u kojem omogućuje državama članicama da ograniče doseg određenih prava i obveza predviđenih tom direktivom, treba tumačiti usko te da stoga ne može dovesti do toga da odstupanje od tih prava i načelnih obveza postane pravilo [115]. Prema tome, doseg navedenog pojma „teško kazneno djelo" države članice ne smiju preširoko tumačiti.

102. *Kao drugo* i krajnje podredno, *u slučaju da Sud smatra da je navedeni pojam autonoman*, tada treba odgovoriti na pitanje kako ga je postavio sud koji je uputio zahtjev te, prema tome, odlučiti o utvrđivanju kriterija koji omogućuje ocjenu na razini prava Unije je li kazneno djelo dovoljno teško kako bi se opravdala povreda temeljnih prava zajamčenih člancima 7. i 8. Povelje.

103. Konkretnije, Sud treba odrediti je li za utvrđivanje postojanja „teškog kaznenog djela" u smislu navedene sudske prakse dovoljno osloniti se na kaznu predviđenu za navodno kazneno djelo ili je potrebno, k tome, da je protupravno postupanje bilo osobito štetno za pravne interese pojedinaca i kolektiva. U tom pogledu, prema mojem mišljenju, kao i prema mišljenju danske, španjolske, francuske, mađarske, austrijske i poljske vlade te vlade Ujedinjene Kraljevine, u biti se valja odlučiti za drugi dio te alternative, a ne za njezin prvi dio, odabirom definicije koja se temelji na *nizu kriterija ocjene* [116].

112 Na primjer, u području borbe protiv organiziranog kriminala, u Izvješću Komisije od 7. srpnja 2016. navodi da se kazne koje predviđaju države članice međusobno znatno razlikuju (od tri mjeseca do 17 godina zatvora) za teško kazneno djelo koje čini sudjelovanje u zločinačkoj organizaciji (vidjeti Izvješće Europskom parlamentu i Vijeću na temelju članka 10. Okvirne odluke Vijeća 2008/841/PUP od 24. listopada 2008. o borbi protiv organiziranog kriminala, COM(2016) 448 *final*, str. 7., t. 2.1.4.1.).

113 Kao što je navela danska vlada, u Danskoj se primjenjuju lakše kazne u odnosu na druge države članice, a da to ne znači da se smatra da kazneno djelo nije osobito teško. Na primjer, kazna predviđena za posjedovanje materijala s dječjom pornografijom iznosi godinu dana zatvora, dok u drugim državama članicama može iznositi i do deset godina zatvora za ista djela, ali time se ne dovodi u pitanje utvrđenje da je to kazneno djelo osobito teške naravi.

114 Vidjeti osobito presudu od 22. svibnja 2012., I (C-348/09, EU:C:2012:300, t. 21. do 23.) u skladu s kojom se „pravom Unije ne nalaže […] državama članicama ujednačeni sustav vrijednosti u pogledu ocjene ponašanja koja se mogu smatrati protivnima javnoj sigurnosti" i „države članice ostaju slobodne odrediti, u skladu sa svojim nacionalnim potrebama koje se mogu razlikovati od jedne države članice do druge i od jednog razdoblja do drugog, zahtjeve javnog poretka i javne sigurnosti, osobito kao opravdanje za odstupanje od temeljnog načela slobodnog kretanja osoba", ali „ti zahtjevi moraju, međutim, biti strogo shvaćeni tako da njihov doseg ne može jednostrano odrediti svaka država članica bez nadzora institucija Europske unije".

115 Vidjeti u tom smislu točku 89. i sljedeće točke presude Tele2 u pogledu načelne obveze osiguravanja povjerljivosti komunikacija i s njima povezanih podataka o prometu.

116 Napominjem da češka i estonska vlada predlažu da se, u biti, odgovori da je moguće utvrditi dovoljnu težinu kaznenih djela, kao kriterij kojim se opravdava ograničenje temeljnih prava koja se priznaju u člancima 7. i 8. Povelje, oslanjajući se isključivo na izrečenu kaznu, ali da te vlade ipak smatraju da svaka država članica treba imati slobodu primijeniti i druge objektivne kriterije koji odražavaju posebnost njezina pravnog poretka, ako to smatra potrebnim.

104. Što se tiče težine kaznenog djela kojom se može opravdati pristup podacima, prema mojem je mišljenju, s obzirom na načelo proporcionalnosti, nemoguće utvrditi težinu spornih činjenica uzimajući u obzir samo kaznu koju je moguće izreći. Naime, s obzirom na znatne razlike koje još postoje među sustavima kaznenog progona u državama članicama, smatram da se za izrečenu kaznu ne može smatrati da sama po sebi može odražavati, s kvalitativnog stajališta vrste kazne i/ili s kvantitativnog stajališta visine kazne, osobitu težinu kaznenog djela.

105. Iako kazna ima znatnu važnost, drugi se objektivni čimbenici u tom pogledu jednako trebaju uzimati u obzir, u svakom slučaju zasebno. Riječ je, konkretnije, s jedne strane, o kontekstu navodnog kaznenog djela – je li protupravno postupanje počinjeno namjerno, u otegotnim okolnostima i/ili u slučaju ponavljanja kaznenog djela –, s druge strane, o važnosti interesa društva koje je počinitelj kaznenog djela mogao ugroziti, kao i o naravi i/ili razmjerima štete koju je žrtva mogla pretrpjeti u okviru tog kaznenog djela [117] te, konačno, o rasponu kazni koje se općenito primjenjuju u predmetnoj državi članici [118]. Na temelju tog niza alternativnih i netaksativnih kriterija treba, prema mojem mišljenju, eventualno kvalificirati kazneno djelo kao „teško" u smislu sudske prakse Suda o kojoj je riječ.

106. Dodajem da je tako predloženo tumačenje u skladu s pristupom koji je ESLJP primijenio u svojoj sudskoj praksi koja se odnosi na „sprječavanje kaznenih djela" kao cilj koji omogućuje opravdavanje zadiranja u pravo na privatnost zajamčeno člankom 8. EKLJP-a ako su ispunjeni i ostali uvjeti [119]. Prema mojem mišljenju, iz te sudske prakse proizlazi da se na borbu protiv određenih kategorija kaznenih djela u tom okviru valjano mogu pozivati države potpisnice EKLJP-a [120], ne samo s obzirom na izrečenu kaznu, nego i na različite čimbenike procjene među kojima se s pravom nalaze narav predmetnih kaznenih djela, kao i javni te privatni interesi koji su njima ugroženi [121].

107. Prema tome, ako bi Sud pojam „teško kazneno djelo" u smislu sudske prakse koja proizlazi iz presuda Digital Rights i Tele2 smatrao autonomnim pojmom prava Unije, smatram da bi ga trebalo tumačiti na način da težina kaznenog djela kojom se može opravdati pristup nadležnih nacionalnih tijela osobnim podacima na temelju članka 15. stavka 1. Direktive 2002/58 treba utvrditi ne samo uzimajući u obzir kaznu koja se može izreći, nego i niz drugih objektivnih kriterija ocjene, kao što su oni koji su gore navedeni.

D. Podredna definicija najmanje visine kazne potrebne za utvrđivanje dovoljne težine kaznenog djela kojom se opravdava zadiranje u navedena temeljna prava (drugo pitanje)

108. Svojim drugim pitanjem sud koji je uputio zahtjev u biti poziva Sud, s jedne strane, da utvrdi najmanju visinu izrečene kazne potrebnu kako bi se kazneno djelo moglo kvalificirati kao „teško" u smislu sudske prakse koja proizlazi iz presuda Digital Rights i Tele2 te, s druge strane, da odluči je li prag zatvorske kazne od tri godine, kako je predviđen španjolskim Zakonikom o kaznenom postupku, nakon reforme iz 2015. [122], u skladu sa zahtjevima prava Unije.

117 Slažem se sa stajalištem francuske vlade prema kojem se podrazumijeva da su povrede temeljnih interesa naroda, institucija ili cjelovitosti državnog područja po svojoj naravi obuhvaćena područjem „teškog kriminala", ali da njime trebaju biti obuhvaćeni i druge vrste kaznenih djela, kao što su napadi na život, fizički ili psihički integritet i dostojanstvo osoba, kao i povrede imovine koje dovode do znatne imovinske štete za žrtvu, ili pak povrede počinjene serijski kojima se nanosi ponovljena šteta javnom poretku. U pogledu potonjeg pitanja, mađarska vlada navodi i mogućnost uzimanja u obzir izrazitog ponavljanja određenih kaznenih djela na nacionalnoj razini.

118 U tom potonjem pogledu, također vidjeti točku 98. ovog mišljenja.

119 U skladu s člankom 8. stavkom 2. EKLJP-a, takvo zadiranje može biti opravdano samo ako je predviđeno zakonom, ako se odnosi na jedan ili više legitimnih ciljeva nabrojanih u tom stavku i ako je to nužno za ispunjenje tog cilja ili više njih u demokratskom društvu.

120 ESLJP je presudio da relevantna kaznena djela građani trebaju moći lako utvrditi, a da zbog tog zahtjeva predvidljivosti nije potrebno da države taksativno nabroje povrede koje mogu dovesti do takve mjere (vidjeti osobito presudu ESLJP-a od 4. prosinca 2015. Roman Zakharov protiv Rusije, CE:ECHR:2015:1204JUD004714306, t. 244.).

121 Vidjeti osobito presudu ESLJP-a od 26. lipnja 2006. Weber i Saravia protiv Njemačke (CE:ECHR:2006:0629DEC005493400, t. 106. i 115.); presudu ESLJP-a od 4. prosinca 2008. Marper protiv Ujedinjene Kraljevine (CE:ECHR:2008:1204JUD003056204, t. 104. i 119.), kao i presudu ESLJP-a od 30. svibnja 2017. Trabajo Rueda protiv Španjolske (CE:ECHR:2017:0530JUD003260012, t. 39. i 40.).

122 Vidjeti točku 15. i sljedeće točke ovog mišljenja.

109. Ta su pitanja postavljena tek podredno, u slučaju da Sud u odgovoru na prvo prethodno pitanje presudi da težinu kaznenog djela, što je čimbenik kojim se može opravdati zadiranje u temeljna prava na temelju navedene sudske prakse, treba utvrditi uzimajući u obzir samo visinu kazne oduzimanja slobode koja se može izreći.

110. S obzirom na odgovor koji predlažem na prvo prethodno pitanje, prema mojem mišljenju, Sud ne treba odlučiti o drugom pitanju. Međutim, radi sveobuhvatnosti iznijet ću razmatranja u tom pogledu.

111. Što se tiče *prvog dijela drugog pitanja*, kao i, među ostalim, češka i estonska vlada, smatram da se *visina izrečene kazne* koja sama po sebi omogućuje da se kazneno djelo kvalificira kao „teško" ne može ujednačeno odrediti za cijelo područje Unije, s obzirom na razmatranja gore navedena u odgovoru na prvo pitanje suda koji je uputio zahtjev [123].

112. Uostalom, u aktima prava Unije također postoje te razlike u definiciji onoga što treba shvaćati „teškim kaznenim djelom" i, konkretnije, u pogledu praga kazne od kojeg bi se ta definicija primjenjivala. Naime, može se utvrditi da se aktima Unije donesenima na temelju članka 83. stavka 1. UFEU-a predviđaju zatvorske kazne utvrđene na različitim visinama za sva kaznena djela koja se, međutim, smatraju „osobito teškim kriminalitetom" [124], kao što proizlazi, na primjer, iz članka 3. Direktive 2011/92/EU [125] i iz članka 15. Direktive (EU) 2017/541 [126], koji su instrumenti suzbijanja seksualnog zlostavljanja djece odnosno suzbijanja terorizma. Stoga sam zakonodavac Unije nije odabrao ujednačenu definiciju pojma „teško kazneno djelo" s obzirom na određenu visinu izrečene kazne.

113. Podsjećam da je sloboda koja je ostavljena državama članicama za odlučivanje o najmanjoj visini kazne koja se zahtijeva kako bi kaznena djela bila „teška" ograničena pravilima koja se navode u odredbama prava Unije u tom području, ali i načelom na temelju kojeg iznimka ne može biti tako širokog opsega da bi postala opće pravilo [127].

114. U ovom slučaju, čak i ako svaka država članica može ocijeniti koji je odgovarajući prag kazne za utvrđivanje teškog kaznenog djela, ipak je dužna da ga ne odredi toliko nisko, s obzirom na uobičajenu visinu kazni koje se primjenjuju u toj državi [128], da iznimke od zabrane pohranjivanja ili uporabe osobnih podataka koje su predviđene člankom 15. stavkom 1. postanu načela, kao što je pravilno napomenula irska vlada.

115. Štoviše, nesporno je da zadiranja u prava zajamčena člancima 7. i 8. Povelje, koja države članice mogu odobriti na temelju članka 15. stavka 1. Direktive 2002/58, k tome, uvijek ostaju podređena poštovanju općih zahtjeva koji proizlaze iz načela proporcionalnosti, kako je navedeno u članku 52. stavku 1. Povelje [129].

123 Vidjeti točku 93. i sljedeće točke ovog mišljenja.

124 Budući da se člankom 83. stavkom 1. UFEU dopušta da se donesu „minimalna pravila o definiranju kaznenih djela i sankcija u području osobito teškog kriminaliteta s prekograničnim elementima", nabrojana u toj odredbi.

125 Direktiva Europskog parlamenta i Vijeća od 13. prosinca 2011. o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije, te o zamjeni Okvirne odluke Vijeća 2004/68/PUP (SL 2011., L 335, str. 1.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 19., svezak 16., str. 261.), u čijem se članku 3. predviđaju kazne u rasponu od najmanje godine dana do najmanje deset godina zatvora za različite oblike „kaznenih djela seksualnog zlostavljanja" iz tog članka.

126 Direktiva 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.), u čijem se članku 15. stavku 3. predviđaju kazne zatvora koje ne smiju biti kraće od osam ili petnaest godina, ovisno o različitim vrstama „kaznenih djela povezanih s terorističkom skupinom" iz članka 4. te iste direktive.

127 Vidjeti i točku 101. ovog mišljenja.

128 U tom pogledu vidjeti točku 98. ovog mišljenja.

129 Vidjeti osobito uvodnu izjavu 11. i članak 15. stavak 1. Direktive 2002/58, kao i točke 94. do 96. i 116. presude Tele2.

116. Što se tiče *posljednjeg dijela drugog pitanja*, estonska vlada i Komisija ističu, s jedne strane, da je prag koji se temelji isključivo na kazni od najmanje *tri godine zatvora* u apsolutnom smislu dovoljan kako bi se kazneno djelo kvalificiralo kao „teško" u smislu sudske prakse Suda o pristupu osobnim podacima koja proizlazi iz presude Digital Rights i, s druge strane, da takav prag nije očito nespojiv općenito s pravom Unije [130] te, konkretnije, s člankom 15. stavkom 1. Direktive 2002/58.

117. Međutim, prema mojem je mišljenju poželjno da Sud ne zauzme stajalište kojim se zagovara točna visina izrečene kazne jer ono što je prilagođeno određenim državama članicama neće nužno biti i drugima i jer nešto što je za jednu vrstu kaznenog djela danas na snazi neće to nužno i neopozivo biti i u budućnosti, kao što sam već napomenuo [131]. Budući da određivanje predmetnog praga zahtijeva složenu i potencijalno promjenjivu procjenu, prema mojem mišljenju valja ostati oprezan po tom pitanju i prepustiti taj postupak ocjeni zakonodavca Unije, u okviru ovlasti koje su mu dodijeljene, ili ocjeni zakonodavca svake države članice u granicama zahtjeva koji proizlaze iz prava Unije.

118. U tom potonjem pogledu, ističem da je u ovom slučaju sud koji je uputio zahtjev utvrdio opasnost od zamjene općeg pravila i odstupanja predviđenih Direktivom 2002/58, opasnost koja je gore navedena [132], time što je naveo da se „prag od tri godine zatvora [koji je španjolski zakonodavac uveo 2015. [133]] odnosi […] na veliku većinu kvalifikacija kaznenog djela". Drugim riječima, prema mišljenju tog suda, sadašnji popis kaznenih djela kojim se u Španjolskoj mogu opravdati ograničenja prava zaštićenih na temelju članaka 7. i 8. Povelje, a koji je uveden reformom Zakonika o kaznenom postupku, u praksi dovodi do toga da je većina kaznenih djela predviđenih Kaznenim zakonikom uključena u navedeni popis.

119. Međutim, pod pretpostavkom da Sud zadiranje u glavnom postupku smatra ozbiljnim i da se utvrdi posljedica koju je tako naveo sud koji je uputio zahtjev, potonja posljedica prema mojem mišljenju nije u skladu s obvezom proporcionalnosti kojoj podliježu takva ograničenja [134]. To prema mojem mišljenju vrijedi bez obzira na postojanje sudskog nadzora koje navodi španjolska vlada jer se izvršavanjem tog nadzora samo omogućuje sprečavanje provedbe mjera koje se, u svakom slučaju zasebno, smatraju proizvoljnim ili previše invazivnim, a ne općenito zaustavljanje primjene mjera te vrste ili njihov razvoj.

120. Konačno, ističem da je pristup koji se predlaže u cijelom ovom dijelu, prema mojem mišljenju, u skladu s pristupom koji je ESLJP primijenio u svojoj sudskoj praksi koja se odnosi na zaštitu osobnih podataka. Točno je da je, kao što navode irska vlada i Komisija, ESLJP ocijenio da su dovoljno jasna nacionalna zakonodavstva kojima se definiraju „teška" kaznena djela, kojima se može opravdati zadiranje u privatnost, time što upućuje na izrečenu kaznu koja je jednaka ili dulja od tri godine zatvora [135]. Međutim, smatram da nije u svrhu te definicije utvrdio navedenu visinu kazne prema apsolutnom i fiksnom kriteriju, uzimajući u obzir da je njegova sudska praksa usmjerena na zahtjev dovoljne predvidljivosti i jasnoće za građane s obzirom, ne toliko na izrečenu kaznu, nego na narav kaznenih djela kojom se omogućuje takvo zadiranje [136]. Nadalje, iako ESLJP državama priznaje

130 Vidjeti osobito, osim odredbi iz bilješki 125. i 126. ovog mišljenja, Direktivu (EU) 2016/681 Europskog parlamenta i Vijeća od 27. travnja 2016. o uporabi podataka iz evidencije podataka o putnicima (PNR) u svrhu sprečavanja, otkrivanja, istrage i kaznenog progona kaznenih djela terorizma i teških kaznenih djela (SL 2016., L 119, str. 132.), u čijem se članku 3. točki 9. „teška kaznena djela" definiraju kao „kaznena djela navedena u Prilogu II. koja su kažnjiva kaznom zatvora ili mjerom oduzimanja slobode od najmanje tri godine u skladu s nacionalnim pravom države članice".

131 Vidjeti točku 97. ovog mišljenja.

132 Vidjeti točku 101. ovog mišljenja.

133 Reforma navedena u točki 15. i sljedećim točkama ovog mišljenja.

134 Vidjeti i točku 115. ovog mišljenja.

135 Vidjeti u tom smislu presudu ESLJP-a od 18. svibnja 2010. Kennedy protiv Ujedinjene Kraljevine (CE:ECHR:2010:0518JUD002683905, t. 34. i 159.), kao i presudu ESLJP-a od 4. prosinca 2015. Roman Zakharov protiv Rusije (CE:ECHR:2015:1204JUD004714306, t. 244.).

136 Vidjeti točku 106. ovog mišljenja.

određenu slobodu u ocjeni postojanja i opsega potrebe za takvim zadiranjem, tu marginu prosudbe ipak podvrgava nadzoru na europskoj razini [137]. Konkretno, osigurava da se spriječe opasnosti od zlouporabe na temelju zakonodavstava koja upućuju na tako širok raspon kaznenih djela da dovode do toga da se većinom kaznenih djela omogućuje opravdanje invazivnih mjera [138].

121. Zaključno, smatram da u slučaju da Sud presudi, suprotno onome što predlažem, da valja uzeti u obzir isključivo izrečenu kaznu kako bi se kazneno djelo kvalificiralo kao „teško" u smislu sudske prakse koja proizlazi iz presude Digital Rights, tada na drugo prethodno pitanje valja odgovoriti da su države članice slobodne utvrditi najmanju visinu kazne relevantne u tu svrhu, pod uvjetom da postupaju u skladu sa zahtjevima koji proizlaze iz prava Unije i osobito u skladu sa zahtjevima prema kojima zadiranja u temeljna prava zajamčena člancima 7. i 8. Povelje trebaju ostati iznimke i poštovati načelo proporcionalnosti.

V. Zaključak

122. S obzirom na prethodna razmatranja, predlažem Sudu da na prethodna pitanja koja je uputio Audiencia Provincial de Tarragona (Provincijski sud u Tarragoni, Španjolska) odgovori kako slijedi:

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), kako je izmijenjena Direktivom 2009/136/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009., u vezi s člancima 7. i 8. te s člankom 52. stavkom 1. Povelje Europske unije o temeljnim pravima, treba tumačiti na način da mjera kojom se nadležnim nacionalnim tijelima omogućuje da, u svrhu borbe protiv kaznenih djela, imaju pristup identifikacijskim podacima korisnika telefonskih brojeva aktiviranih s određenog mobilnog telefona i tijekom ograničenog razdoblja, u okolnostima kao što su one u glavnom postupku, dovodi do zadiranja u temeljna prava zajamčena navedenom direktivom i Poveljom, koje nije dovoljno ozbiljno da bi takav pristup trebalo ograničiti na slučajeve u kojima je predmetno kazneno djelo teško.

137 Vidjeti osobito presudu ESLJP-a od 6. rujna 1978. Klass i drugi protiv Njemačke (CE:ECHR:1978:0906JUD000502971, t. 49.), kao i presudu ESLJP-a od 18. svibnja 2010. Kennedy protiv Ujedinjene Kraljevine (CE:ECHR:2010:0518JUD002683905, t. 153. i 154.).

138 Vidjeti presudu ESLJP-a od 10. veljače 2009. Iordachi i drugi protiv Moldove (CE:ECHR:2009:0210JUD002519802, t. 44.), u kojoj se moldavsko zakonodavstvo smatralo nedovoljno jasnim, među ostalim, zbog toga što je polovina kaznenih djela predviđenih Kaznenim zakonikom bila obuhvaćena kategorijom kaznenih djela koja mogu dovesti do mjere presretanja telefonskih poziva. Vidjeti također presudu ESLJP-a od 4. prosinca 2015. Roman Zakharov protiv Rusije (CE:ECHR:2015:1204JUD004714306, t. 248.).