Zbirka odločb sodne prakse

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

Zadeva C-520/18

Ordre des barreaux francophones et germanophone,
Académie Fiscale ASBL,
UA,
Liga voor Mensenrechten ASBL,
Ligue des Droits de l'Homme ASBL,
VZ,
WY,
XX
proti
Conseil des ministres,
ob udeležbi
Child Focus

(Predlog za sprejetje predhodne odločbe, ki ga je vložilo Cour constitutionnelle (ustavno sodišče, Belgija))

„Predhodno odločanje – Obdelava osebnih podatkov in varstvo zasebnega življenja na področju elektronskih komunikacij – Direktiva 2002/58/ES – Področje uporabe – Člen 1(3) – Člen 15(1) – Člen 4(2) PEU – Listina Evropske unije o temeljnih pravicah – Členi 4, 6, 7, 8, 11 in 52(1) – Obveznost splošne in neselektivne hrambe podatkov o prometu in lokaciji – Učinkovitost kazenskih preiskav in drugi cilji v javnem interesu“

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

– sodba z dne 8. aprila 2014, Digital Rights Ireland in drugi[2], v kateri je razglasilo neveljavnost Direktive 2006/24/ES[3], ker je ta omogočala nesorazmeren poseg v pravice, priznane s členoma 7 in 8 Listine Evropske unije o temeljnih pravicah;

[1] Jezik izvirnika: španščina.

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

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

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

– sodba z dne 2. oktobra 2018, Ministerio Fiscal[6], v kateri je potrdilo razlago navedene določbe iz Direktive 2002/58.

2. Te sodbe (zlasti drugonavedena) organom nekaterih držav članic povzročajo skrbi, saj so po njihovem mnenju zaradi njih oropani instrumenta, ki ga štejejo za nujnega za zagotavljanje nacionalne varnosti ter za boj proti kriminalu in terorizmu. Zato se nekatere od teh držav članic zavzemajo za preklic oziroma za prilagoditev te sodne prakse.

3. Nekatera sodišča držav članic so to zaskrbljenost izrazila v štirih predlogih za sprejetje predhodne odločbe[7], v zvezi s katerimi sklepne predloge predstavljam na isti dan.

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

5. Ko je bila sodba Digital Rights razglašena, je Cour constitutionnelle (Belgija) razveljavilo nacionalne predpise, s katerimi je bila v nacionalno pravo delno prenesena Direktiva 2006/24, ki je bila z navedeno sodbo razglašena za neveljavno. Belgijski zakonodajalec je torej sprejel nove predpise, o združljivosti katerih s pravom Unije se ponovno dvomi zaradi sodbe Tele2 Sverige in Watson.

6. Posebnost tega predloga za sprejetje predhodne odločbe je, da se z njim izpostavlja možnost začasnega odloga učinkov nacionalnega predpisa, ki ga nacionalna sodišča morajo razveljaviti zaradi njegove nezdružljivosti s pravom Unije.

I. Pravni okvir

A. Pravo Unije

7. Napotujem na isto točko mojih sklepnih predlogov v zadevah C-511/18 in C-512/18.

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

5 Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514).

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

7 Poleg te (zadeva C-520/18, Ordre des barreaux francophones et germanophone in drugi) gre za zadevi C-511/18 in C-512/18, La Quadrature du Net in drugi, ter zadevo C-623/17, Privacy International.

8 Zadeva Privacy International, C-623/17.

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

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

B. Nacionalno pravo: loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques [11]

8. Člen 4 določa, da se člen 126 loi du 13 juin 2005 relative aux communications électroniques [12] glasi tako:

„1. Brez poseganja v loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel [(zakon z dne 8. decembra 1992 o varstvu zasebnega življenja pri obdelavi osebnih podatkov)] ponudniki, ki javnosti ponujajo storitve telefonije, tudi prek interneta, dostop do interneta in elektronsko pošto prek interneta, operaterji, ki ponujajo javna omrežja elektronskih komunikacij, ter operaterji, ki ponujajo le kakšno od teh storitev, hranijo podatke iz odstavka 3, ki jih ustvarijo ali obdelajo v okviru dobave teh komunikacijskih storitev.

Ta člen se ne nanaša na vsebino komunikacij.

[…]

2. Za namene in pod pogoji, naštetimi spodaj, lahko le naslednji organi zahtevajo pridobitev podatkov, ki se hranijo na podlagi tega člena, od ponudnikov in operaterjev iz odstavka 1, prvi pododstavek:

(1) pravosodni organi za namene odkrivanja, preiskave in pregona kršitev, za izvrševanje ukrepov iz členov 46a in 88a Code d'instruction criminelle [(zakonik o kazenskem postopku)] in pod pogoji, navedenimi v teh členih;

(2) obveščevalne in varnostne službe, ki zaradi opravljanja obveščevalne dejavnosti uporabljajo metode zbiranja podatkov, določene v členih 16/2, 18/7 in 18/8 loi du 30 novembre 1998 organique des services de renseignement et de Sécurité[13], pod pogoji, določenimi s tem zakonom;

(3) kriminalisti Institut [belge des services postaux et des télécommunications (belgijski inštitut za poštne in telekomunikacijske storitve; v nadaljevanju: Institut)] za namene odkrivanja, preiskave in pregona kršitev [pravil o varnosti omrežij] in kršitev tega člena;

(4) urgentne službe, ki zagotavljajo pomoč na kraju samem, kadar po nujnem klicu od zadevnega ponudnika ali operaterja ne dobijo podatkov za identifikacijo klicatelja […] ali dobijo nepopolne ali nepravilne podatke. Zahtevajo se lahko le podatki za identifikacijo klicatelja, in to najkasneje 24 ur po klicu;

(5) kriminalisti Cellule des personnes disparues de la Police Fédérale [(oddelek zvezne policije za pogrešane osebe)], kadar pomagajo osebi, ki je v nevarnosti, kadar iščejo osebe, katerih izginotje vzbuja skrb, ali kadar obstajajo sumi ali resni indici, da je telesna celovitost pogrešane osebe v neposredni nevarnosti. Od zadevnega operaterja ali ponudnika se prek

11 Zakon z dne 29. maja 2016 o zbiranju in hrambi podatkov na področju elektronskih komunikacij; v nadaljevanju: zakon z dne 29. maja 2016 (Moniteur belge z dne 18. julija 2016, str. 44717).

12 Zakon z dne 13. junija 2005 o elektronskih komunikacijah; v nadaljevanju: zakon iz leta 2005 (Moniteur belge z dne 20. junija 2005, str. 28070).

13 Sistemski zakon z dne 30. novembra 1998 o obveščevalnih in varnostnih službah; v nadaljevanju: zakon iz leta 1998 (Moniteur belge z dne 18. decembra 1998, str. 40312).

službe policije, ki jo določi kralj, lahko zahtevajo le podatki iz odstavka 3, prvi in drugi pododstavek, ki se nanašajo na pogrešano osebo, za zadnjih 48 ur pred vložitvijo zahteve za posredovanje podatkov;

(6) Service de médiation pour les télécommunications [(služba za mediacijo za telekomunikacije)] z namenom identifikacije osebe, ki je zlorabila omrežje ali storitev elektronskih komunikacij […]. Zahtevajo se lahko le podatki za identifikacijo.

Ponudniki in operaterji iz odstavka 1, prvi pododstavek, zagotovijo, da so podatki iz odstavka 3 neomejeno dostopni iz Belgije ter da se lahko ti podatki in vse druge potrebne informacije v zvezi s temi podatki posredujejo nemudoma in le organom iz tega odstavka.

Ponudniki in operaterji iz odstavka 1, prvi pododstavek, podatkov, ki se hranijo na podlagi odstavka 3, ne morejo uporabiti za druge namene, razen če z zakonom ni določeno drugače.

3. Podatki za identifikacijo uporabnika ali naročnika in komunikacijskih sredstev, razen podatkov, ki so izrecno navedeni v drugem in tretjem pododstavku, se hranijo 12 mesecev od dne, ko je komunikacija prek uporabljene storitve zadnjič mogoča.

Podatki v zvezi z dostopom in povezavo terminalske opreme z omrežjem in s storitvijo ter o lokaciji te opreme, vključno z omrežno priključno točko, se hranijo 12 mesecev od datuma komunikacije.

Komunikacijski podatki, razen vsebine, vključno z virom in ciljem teh podatkov, se hranijo 12 mesecev od datuma komunikacije.

Kralj z odlokom, ki ga obravnava svet ministrov na predlog ministra za pravosodje in ministra[, pristojnega za elektronske komunikacije,] na podlagi mnenja Commission de la protection de la vie privée [(komisija za varstvo zasebnega življenja)] in Institut določi podatke, ki jih je treba hraniti, za vsako od kategorij, naštetih v prvem, drugem in tretjem pododstavku, in zahteve, ki jih morajo ti podatki izpolnjevati.

4. V zvezi s hrambo podatkov iz odstavka 3 ponudniki in operaterji iz odstavka 1, prvi pododstavek:

(1) zagotovijo, da so shranjeni podatki enake kakovosti in zanje veljajo enake zahteve o varnosti in zaščiti kot za podatke na omrežju;

(2) zagotovijo, da se v zvezi s shranjenimi podatki sprejmejo primerni tehnični in organizacijski ukrepi, s katerimi se ti podatki zaščitijo pred nenamernim ali nezakonitim uničenjem, izgubo ali spremembami in nepooblaščenimi ali nezakonitimi oblikami hrambe, obdelave, dostopa ali razkrivanja;

(3) zagotovijo, da lahko do podatkov, ki se hranijo zaradi zahtev organov iz odstavka 2, dostopa le en ali več članov Cellule de coordination [(oddelek za koordinacijo)] iz člena 126/1(1);

(4) hranijo podatke na ozemlju Evropske unije;

(5) izvajajo ukrepe za tehnično zaščito, zaradi katerih hranjeni podatki postanejo neberljivi in neuporabni takoj, ko jih nepooblaščena oseba shrani;

(6) po poteku roka za hrambo, ki je za posamezno vrsto podatkov določen v odstavku 3, uničijo hranjene podatke na nosilcih, razen če ni drugače določeno v členih 122 in 123;

(7) zagotovijo sledljivost uporabe hranjenih podatkov za vsako zahtevo organa iz odstavka 2 za posredovanje teh podatkov.

Sledljivost iz prvega pododstavka, točka 7, se zagotavlja z dnevnikom. Institut in komisija za varstvo zasebnega življenja lahko dostopata do tega dnevnika ali zahtevata kopijo celotnega dnevnika ali njegovega dela. Institut in komisija za varstvo zasebnega življenja skleneta sporazum o sodelovanju v zvezi z vpogledom v vsebino tega dnevnika in nadzorom nad njo.

5. Vsako leto minister[, pristojen za elektronske komunikacije,]minister za pravosodje pošlje poslanski zbornici statistike o hrambi podatkov, ki so nastali ali so se obdelovali v okviru opravljanja storitev ali javnih komunikacijskih omrežij.

Te statistike zajemajo predvsem:

(1) zadeve, v katerih so bili podatki posredovani pristojnim organom v skladu z veljavnimi zakonskimi določbami;

(2) obdobje, ki je preteklo od datuma, ko so se podatki shranili, do datuma, ko so pristojni organi zahtevali njihovo posredovanje;

(3) zadeve, v katerih zahtev za podatke ni bilo mogoče izpolniti.

Te statistike ne smejo zajemati osebnih podatkov.

[…]“

9. Člen 5 določa, da se v zakon iz leta 2005 doda člen 126/1, ki ima tako besedilo:

„1. Vsak operater in vsak ponudnik iz člena 126(1), prvi pododstavek, ustanovi oddelek za usklajevanje, ki je zadolžen za to, da belgijskim organom, ki imajo za to pooblastilo v zakonu, na njihovo zahtevo posreduje podatke, ki se hranijo na podlagi členov 122, 123 in 126, podatke o identifikaciji klicatelja na podlagi člena 107(2), prvi pododstavek, in podatke, ki se lahko zahtevajo na podlagi členov 46a, 88a in 90b zakonika o kazenskem postopku in členov 18/7, 18/8, 18/16 in 18/17 [zakona iz leta 1998].

[…]

2. Operaterji in ponudniki iz člena 126(1), prvi pododstavek, določijo notranji postopek, ki omogoča, da odgovarjajo na zahteve organov za dostop do osebnih podatkov v zvezi z uporabniki. Institut morajo na njegovo zahtevo predložiti informacije o teh postopkih, o številu prejetih zahtev, o navedeni pravni podlagi in o njihovem odgovoru.

[…]

3. Operaterji in ponudniki iz člena 126(1), prvi pododstavek, imenujejo eno ali več pooblaščenih oseb za varstvo osebnih podatkov, ki mora izpolnjevati kumulativno naštete pogoje iz odstavka 1, tretji pododstavek.

[…]

Pooblaščena oseba za varstvo osebnih podatkov pri opravljanju svojih nalog ravna neodvisno in ima dostop do vseh osebnih podatkov, ki se posredujejo organom, in do vseh prostorov ponudnika ali operaterja, za katere je to potrebno.

[…]

4. Kralj z odlokom, ki ga obravnava svet ministrov na podlagi mnenja komisije za varstvo zasebnega življenja in Institut, določi:

[…]

(2) zahteve, ki jih mora izpolnjevati oddelek za koordinacijo, ob upoštevanju položaja operaterjev in ponudnikov, ki od pravosodnih organov prejemajo le malo zahtev, ki v Belgiji nimajo prostorov ali ki delujejo v glavnem iz tujine;

(3) informacije, ki jih je treba zagotoviti Institut in komisiji za varstvo zasebnega življenja v skladu z odstavkoma 1 in 3, ter organe, ki imajo dostop do teh informacij;

(4) druga pravila o sodelovanju operaterjev in ponudnikov iz člena 126(1), prvi pododstavek, z belgijskimi organi ali z nekaterimi od teh organov zaradi posredovanja podatkov iz odstavka 1, vključno, po potrebi in glede na zadevni organ, z obliko in vsebino zahteve.

[…]“

10. Člen 8 določa, da se člen 46a(1) zakonika o kazenskem postopku glasi tako:

„1. Kraljevi tožilec lahko pri preiskavi kaznivih dejanj z obrazloženo pisno odločbo, pri čemer po potrebi zahteva sodelovanje operaterja elektronskega komunikacijskega omrežja ali ponudnika storitev elektronskih komunikacij ali službe policije, ki jo določi kralj, na podlagi vseh podatkov, s katerimi razpolaga, ali z dostopom do dokumentov strank operaterja ali ponudnika storitev opravi ali odredi, da se opravi:

(1) identifikacija naročnika ali osebe, ki običajno uporablja storitve elektronske komunikacije, ali uporabljenega elektronskega komunikacijskega sredstva;

(2) identifikacija storitev elektronske komunikacije, na katere je neka oseba naročena ali ki jih neka oseba običajno uporablja.

Iz obrazložitve mora izhajati sorazmernost glede na spoštovanje zasebnega življenja in subsidiarnost glede na vse druge preiskovalne ukrepe.

V primeru izredne nujnosti lahko vsak kriminalist po predhodnem ustnem soglasju kraljevega tožilca in z obrazloženo pisno odredbo zahteva te podatke. Kriminalist to obrazloženo pisno odredbo in zbrane informacije v štiriindvajsetih urah posreduje kraljevemu tožilcu in poleg tega utemelji izredno nujnost.

Za kazniva dejanja, za katera ni zagrožena glavna kazen zapora v višini enega leta ali več, lahko kraljevi tožilec ali – v primeru izredne nujnosti – kriminalist zahteva podatke iz prvega odstavka le za obdobje šestih mesecev pred sprejetjem odločbe.

2. Vsak operater elektronskega komunikacijskega omrežja in vsak ponudnik storitev elektronskih komunikacij, od katerega se zahteva posredovanje podatkov iz odstavka 1, da zahtevane podatke na voljo kraljevemu tožilcu ali kriminalistu v roku, ki ga določi kralj […].

[…]

Za vsakogar, ki se zaradi svojega položaja seznani z ukrepom ali pri njem sodeluje, velja obveznost varovanja zaupnosti. Vsaka kršitev zaupnosti se kaznuje v skladu s členom 458 kazenskega zakonika.

Zavrnitev posredovanja podatkov se kaznuje z globo od 26 EUR do 10.000 EUR.“

11. Člen 9 določa, da se člen 88a zakonika o kazenskem postopku glasi tako:

„1. Če obstajajo resni indici, da so kazniva dejanja taka, da se lahko zanje izreče glavna kazen zapora v višini enega leta ali več, in če preiskovalni sodnik meni, da obstajajo okoliščine, zaradi katerih je izsleditev elektronskih komunikacij ali določitev lokacije vira ali cilja elektronske komunikacije nujna za ugotovitev resnice, lahko – pri čemer po potrebi neposredno ali prek službe policije, ki jo določi kralj, zahteva tehnično sodelovanje operaterja elektronskega komunikacijskega omrežja ali ponudnika storitev elektronskih komunikacij – odredi:

(1) izsleditev podatkov o prometu elektronskih komunikacijskih sredstev, s katerih se elektronske komunikacije pošiljajo ali so se pošiljale in na katere so ali so bile naslovljene;

(2) določitev lokacije vira ali cilja elektronskih komunikacij.

V primerih iz prvega pododstavka se za vsako elektronsko komunikacijsko sredstvo, katerega klicni podatki se odkrijejo ali pri katerem se lokalizira vir ali cilj telekomunikacije, v zapisniku zabeležijo dan, ura, trajanje in po potrebi kraj elektronske komunikacije.

Preiskovalni sodnik v obrazloženi odredbi navede dejanske okoliščine zadeve, zaradi katerih je ukrep upravičen, sorazmeren glede na spoštovanje zasebnega življenja in subsidiaren v razmerju do drugih preiskovalnih ukrepov.

Navede tudi obdobje, v katerem se lahko ukrep izvaja v prihodnosti, pri čemer to trajanje ne sme preseči dveh mesecev od izdaje odredbe, razen v primeru podaljšanja, in po potrebi obdobje v preteklosti, na katero se v skladu z odstavkom 2 nanaša odredba.

[…]

2. V zvezi z uporabo ukrepa iz odstavka 1, prvi pododstavek, za podatke o prometu ali lokaciji, ki se hranijo na podlagi člena 126 zakona [iz leta] 2005 […], se uporabljajo te določbe:

– za kazniva dejanja iz knjige II, naslov Ib, kazenskega zakonika lahko preiskovalni sodnik z odredbo zahteva predložitev podatkov za obdobje 12 mesecev pred izdajo odredbe;

– za druga kazniva dejanja iz člena 90b, od (2) do (4), ki niso kaznivo dejanje iz prve alinee, ali za kazniva dejanja, ki so storjena v okviru hudodelske združbe iz člena 324a kazenskega zakonika, ali za kazniva dejanja, ki se kaznujejo z glavno kaznijo zapora v višini pet let ali več, lahko preiskovalni sodnik z odredbo zahteva predložitev podatkov za obdobje devetih mesecev pred izdajo odredbe;

– za ostala kazniva dejanja lahko preiskovalni sodnik zahteva predložitev podatkov le za obdobje šestih mesecev pred izdajo odredbe.

3. Ukrep se lahko na elektronska komunikacijska sredstva odvetnika ali zdravnika nanaša le, če je ta osumljen, da je storil kaznivo dejanje iz odstavka 1 ali da je bil pri njem udeležen, ali če je na podlagi podrobnih dejstev mogoče domnevati, da njegova elektronska komunikacijska sredstva uporabljajo tretje osebe, ki so osumljene storitve kaznivega dejanja iz odstavka 1.

Ukrep se lahko izvrši le, če je o njem obveščen predsednik lokalne odvetniške ali zdravniške zbornice. Preiskovalni sodnik te osebe obvesti o elementih, za katere meni, da zanje velja poklicna skrivnost. Ti elementi se ne zabeležijo v zapisniku.

4. […]

Za vsakogar, ki se zaradi svojega položaja seznani z ukrepom ali pri njem sodeluje, velja obveznost varovanja zaupnosti. Vsaka kršitev zaupnosti se kaznuje v skladu s členom 458 kazenskega zakonika.

[…]“

12. V skladu s členom 12 se člen 13 zakona iz leta 1998 glasi:

„Obveščevalne in varnostne službe lahko iščejo, zbirajo, prejemajo in obdelujejo informacije in osebne podatke, ki bi lahko bili koristni pri opravljanju njihovih nalog, ter posodabljajo dokumentacijo, ki se zlasti nanaša na dogodke, skupine in osebe, ki so zanimive z vidika opravljanja njihovih nalog.

Informacije, vsebovane v dokumentaciji, morajo biti povezane z namenom spisa in morajo biti omejene na zahteve, ki iz njega izhajajo.

Obveščevalne in varnostne službe skrbijo za varnost podatkov, ki se nanašajo na njihove vire, ter informacij in osebnih podatkov, ki jih ti viri zagotovijo.

Uslužbenci obveščevalnih in varnostnih služb imajo dostop do informacij, obvestil in osebnih podatkov, ki jih zberejo in obdelajo njihove službe, če so koristni za njihovo delo ali opravljanje njihovih nalog.“

13. Člen 14 določa novo besedilo člena 18/3, ki zdaj določa:

„1. Posebne metode zbiranja podatkov iz člena 18/2(1) se lahko izvajajo ob upoštevanju potencialne nevarnosti iz člena 18/1, če se šteje, da običajne metode zbiranja podatkov niso dovolj za pridobitev informacij, ki so nujne za opravo neke obveščevalne naloge. Posebna metoda se izbere glede na resnost potencialne nevarnosti, zaradi katere se ta metoda uporabi.

Posebna metoda se lahko uporabi le na podlagi obrazložene pisne odredbe vodje službe in po vročitvi te odredbe komisiji.

2. V odredbi vodje službe so navedeni:

(1) vrsta posebne metode;

(2) glede na primer fizične ali pravne osebe, združenja ali skupine, predmeti, kraji, dogodki ali informacije, za katere se posebna metoda uporabi;

(3) potencialna nevarnost, zaradi katere je upravičena uporaba posebne metode;

(4) dejstva, ki upravičujejo uporabo posebne metode, obrazložitev subsidiarnosti in sorazmernosti, vključno s povezavo med točkama (2) in (3);

(5) obdobje, v katerem se lahko posebna metoda uporablja, od vročitve odredbe komisiji;

[…]

(9) glede na primer resni indici, da odvetnik, zdravnik ali novinar osebno in aktivno sodeluje ali je sodeloval pri nastanku ali razvoju potencialne nevarnosti;

(10) v primeru iz člena 18/8 obrazložitev trajanja obdobja zbiranja podatkov;

[…]

8. Vodja službe prekine uporabo posebne metode, če je potencialna nevarnost, ki njeno uporabo upravičuje, prenehala, če metoda ni več smiselna za dosego namena, zaradi katerega je bila uporabljena, ali če ugotovi nezakonitost. O svoji odločitvi v najkrajšem možnem času obvesti komisijo.“

14. Člen 18/8 zakona iz leta 1998 določa:

„1. Obveščevalne in varnostne službe lahko pri opravljanju svojih nalog – pri čemer po potrebi zahtevajo tehnično pomoč operaterja elektronskega komunikacijskega omrežja ali ponudnika storitev elektronskih komunikacij – opravijo ali odredijo, da se opravijo:

(1) izsleditev podatkov o prometu elektronskih komunikacijskih sredstev, s katerih se elektronske komunikacije pošiljajo ali so se pošiljale in na katere so ali so bile naslovljene;

(2) določitev lokacije vira ali cilja elektronskih komunikacij.

[…]

2. V zvezi z uporabo metode iz odstavka 1 se za podatke, ki se hranijo na podlagi člena 126 zakona [iz leta] 2005 […], uporabljajo te določbe:

(1) za potencialno nevarnost, ki se nanaša na dejavnost, ki je lahko povezana s hudodelskimi združbami ali škodljivimi sektaškimi organizacijami, lahko vodja službe v odredbi zahteva posredovanje podatkov le za obdobje šestih mesecev pred sprejetjem odredbe;

(2) za potencialno nevarnost, ki ni zajeta s točkama (1) in (3), lahko vodja službe v odredbi zahteva posredovanje podatkov za obdobje devetih mesecev pred sprejetjem odredbe;

(3) za potencialno nevarnost, ki se nanaša na dejavnost, ki je lahko povezana s terorizmom ali ekstremizmom, lahko vodja službe v odredbi zahteva posredovanje podatkov za obdobje 12 mesecev pred sprejetjem odredbe. […]".

II. Dejansko stanje in vprašanja za prehodno odločanje

15. Cour constitutionnelle (ustavno sodišče) je v svoji sodbi z dne 11. junija 2015 [14] razveljavilo novo različico člena 126 zakona iz leta 2005 iz istih razlogov, kot so tisti, iz katerih je Sodišče v sodbi Digital Rights razglasilo Direktivo 2006/24 za neveljavno.

16. Nacionalni zakonodajalec je glede na to razveljavitev (preden je bila izdana sodba Tele 2 Sverige in Watson) sprejel zakon z dne 29. maja 2016.

17. Oseba VZ in drugi, Ordre des barreaux francophones et germanophone (v nadaljevanju: Ordre des barreaux), Liga voor Mensenrechten ASBL (v nadaljevanju: LMR), Ligue des Droits de l'Homme ASBL (v nadaljevanju: LDH) in Académie Fiscale ASBL (v nadaljevanju: Académie Fiscale) so pri predložitvenem sodišču vložili tožbo za razveljavitev zakona, pri tem pa v bistvu trdili, da ta zakon presega to, kar je nujno potrebno, in ne določa zadostnih varovalk v zvezi z varstvom.

18. V teh okoliščinah je Cour constitutionnelle (ustavno sodišče) Sodišču predložilo ta vprašanja za predhodno odločanje:

„1. Ali je treba člen 15(1) Direktive 2002/58/ES v povezavi s pravico do varnosti, ki jo zagotavlja člen 6 Listine Evropske unije o temeljnih pravicah [(v nadaljevanju: Listina)], in pravico do spoštovanja osebnih podatkov, kot jo zagotavljajo členi 7, 8 in 52(1) Listine […], razlagati tako, da nasprotujeta nacionalni zakonodaji, kakršna je ta v postopku v glavni stvari, ki določa splošno obveznost, da operaterji in ponudniki storitev elektronskih komunikacij hranijo podatke o prometu in lokaciji v smislu Direktive 2002/58/ES, ki jih ustvarijo ali obdelajo pri opravljanju teh storitev, pri čemer cilj te nacionalne zakonodaje ni le preiskovanje, odkrivanje in pregon hudega kriminala, temveč tudi zagotavljanje državne varnosti, obrambe in javne varnosti, preiskovanje, odkrivanje in pregon drugih dejanj, ki niso hudi kriminal, preprečevanje prepovedane uporabe elektronskih komunikacijskih sistemov ali doseganje drugih ciljev, ki so našteti v členu 23(1) Uredbe (EU) 2016/679 [Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL 2016, L 119, str. 1)], ob tem da so v zvezi s to obveznostjo v tej zakonodaji natančno določena jamstva glede hrambe in dostopa do podatkov?

2. Ali je treba člen 15(1) Direktive 2002/58/ES v povezavi s členi 4, 7, 8, 11 in 52(1) Listine […] razlagati tako, da nasprotuje nacionalni zakonodaji, kakršna je ta v postopku v glavni stvari, ki določa splošno obveznost, da operaterji in ponudniki elektronskih komunikacijskih storitev hranijo podatke o prometu in lokaciji v smislu Direktive 2002/58/ES, ki jih ustvarijo ali obdelajo pri opravljanju teh storitev, če je cilj te zakonodaje med drugim izpolnitev pozitivnih obveznosti, ki jih ima organ na podlagi členov 4 in 8 Listine, da sprejme zakonski okvir, ki

[14] Sodba št. 84/2015, Moniteur belge z dne 11. avgusta 2015.

omogoča učinkovito kazensko preiskavo in učinkovito kaznovanje spolnih zlorab mladoletnikov ter ki omogoča uspešno identifikacijo storilcev teh kaznivih dejanj, tudi kadar se uporabijo sredstva za elektronsko komuniciranje?

3. Če bi Cour constitutionnelle (ustavno sodišče) na podlagi odgovorov na prvo ali drugo vprašanje za predhodno odločanje ugotovilo, da izpodbijani zakon krši eno ali več obveznosti, ki izhajajo iz določb, omenjenih v teh vprašanjih, ali lahko odloči, da se učinki [spornega zakona] začasno ohranijo, da se prepreči pravna negotovost in da se omogoči, da se prej zbrani in ohranjeni podatki še naprej lahko uporabljajo za cilje, navedene v zakonu?“

III. Postopek pred Sodiščem

19. Predlog za sprejetje predhodne odločbe je sodno tajništvo Sodišča prejelo 2. avgusta 2018.

20. Oseba VZ in drugi, Académie Fiscale, LMR, LDH, Ordre des barreaux, Fondation pour Enfants Disparus et Sexuellement Exploités (Child Focus), nemška, belgijska, britanska, češka, ciprska, danska, španska, estonska, francoska, madžarska, irska, nizozemska, poljska in švedska vlada ter Komisija so predložili pisna stališča.

21. Obravnava je bila 9. septembra 2019 in se je opravila skupaj z obravnavama v zadevah C-511/18, C-512/18 in C-623/17, udeležile pa so se je stranke iz štirih postopkov za sprejetje predhodne odločbe, zgoraj navedene vlade, vlada Norveške ter Komisija in Evropski nadzornik za varstvo podatkov.

IV. Analiza

22. Prvo vprašanje tega predloga se v bistvu ujema z vprašanji, ki se obravnavajo v zadevah C-511/18 in C-512/18. Vendar se od teh razlikuje glede ciljev, ki jim sledi nacionalna zakonodaja: ne gre samo za boj proti terorizmu in proti najhujšim oblikam kriminala ali za zagotavljanje nacionalne varnosti, temveč za „obrambo, javno varnost, preiskovanje, odkrivanje in pregon kaznivih dejanj, ki ne spadajo med huda kazniva dejanja“, in na splošno vsak cilj, določen v členu 23(1) Uredbe št. 2016/679.

23. Drugo vprašanje je povezano s prvim, vendar ga dopolnjuje v smislu, da se z njim sprašuje, ali pozitivne obveznosti, ki jih ima javni organ v zvezi s preiskovanjem in sankcioniranjem spolnih zlorab mladoletnih oseb, upravičujejo sporne ukrepe.

24. Tretje vprašanje se postavlja v primeru, da nacionalni predpis ne bi bil v skladu s pravom Unije. Predložitveno sodišče želi vedeti, ali lahko v tem primeru začasno ohrani učinke zakona z dne 29. maja 2016.

25. Teh vprašanj se bom lotil tako, da bom najprej analiziral možnost uporabe Direktive 2002/58, v zvezi s čimer bom napotil na moje sklepne predloge v drugih postopkih za sprejetje predhodne odločbe. Nato bom opisal glavne usmeritve sodne prakse Sodišča na tem področju in možnosti njenega razvoja. Nazadnje se bom lotil odgovora na vsako od predhodnih vprašanj.

A. Možnost uporabe Direktive 2002/58

26. Tako kot v drugih treh predlogih za sprejetje predhodne odločbe se je tudi v tem primeru dvomilo o možnosti uporabe Direktive 2002/58. Glede na enakost vprašanj, ki so jih države članice postavile glede tega, naj v zvezi s tem napotim na sklepne predloge v zadevah C-511/18 in C-512/18. [15]

B. Sodna praksa Sodišča o hrambi osebnih podatkov in dostopu javnih organov do njih v okviru Direktive 2002/58

1. Načelo zaupnosti komunikacij in z njimi povezanih podatkov

27. Določbe Direktive 2002/58 „podrobno opredeljujejo in dopolnjujejo“ Direktivo 95/46/ES [16] z namenom doseči visoko raven varstva osebnih podatkov v okviru opravljanja elektronskih komunikacijskih storitev. [17]

28. Člen 5(1) Direktive 2002/58 določa, da države članice v svoji nacionalni zakonodaji zagotovijo zaupnost komunikacij, ki se pošiljajo prek javnega komunikacijskega omrežja in javno razpoložljivih elektronskih komunikacijskih storitev, ter zaupnost s tem povezanih podatkov o prometu.

29. Zaupnost komunikacij med drugim pomeni (člen 5(1), drugi stavek, Direktive 2002/58) prepoved vsakomur razen uporabnikom, da brez privolitve zadevnih uporabnikov shranjuje podatke o prometu, povezane z elektronskimi komunikacijami. Izjeme so „osebe, ki jim je […] to zakonsko dovoljeno, in tehnično shranjevanje, ki je potrebno za prenos sporočila“. [18]

30. Cilj členov 5, 6 in 9(1) Direktive 2002/58 je ohranitev zaupnosti komunikacij in z njimi povezanih podatkov ter zmanjšanje tveganja zlorabe na minimum. Njihov domet je treba presojati glede na uvodno izjavo 30 navedene direktive, v skladu s katero morajo biti „[s]istemi za zagotavljanje elektronskih komunikacijskih omrežij in storitev […] zasnovani tako, da omejijo količino potrebnih osebnih podatkov na strogi minimum“. [19]

31. V zvezi s temi podatki je mogoče razlikovati:

– podatke o prometu, katerih obdelava in shranjevanje sta dovoljena le v obsegu in trajanju, ki sta potrebna za zaračunavanje, trženje in zagotovitev storitev z dodano vrednostjo (člen 6 Direktive 2002/58). Ko se to obdobje konča, je treba obdelane in shranjene podatke izbrisati ali predelati v anonimne; [20]

15 Točka 40 in naslednje.

16 Direktiva Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 15, str. 355). Glej člen 1(2) Direktive 2002/58. Direktiva 95/46 je bila z Uredbo št. 2016/679 s 25. majem 2018 razveljavljena. Torej ker Direktiva 2002/58 napoti na Direktivo 95/46 oziroma ker nima lastnih določb, je nujno upoštevati določbe te uredbe (glej člen 94(1) in (2) Uredbe št. 2016/679).

17 Sodba Tele2 Sverige in Watson, točki 82 in 83.

18 Prav tam, točka 85 in navedena sodna praksa.

19 Prav tam, točka 87. Moj poudarek.

20 Prav tam, točka 86 in navedena sodna praksa.

– podatke o lokaciji, ki niso podatki o prometu, ki se smejo obdelati samo pod nekaterimi pogoji in po tem, ko postanejo anonimni oziroma ko se pridobi soglasje uporabnikov ali naročnikov (člen 9(1) Direktive 2002/58). [21]

2. Določba o omejitvi iz člena 15(1) Direktive 2002/58

32. Člen 15(1) Direktive 2002/58 državam članicam dovoljuje, da „sprejmejo zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, določenih v členu 5, členu 6, členu 8(1), (2), (3) in (4) ter členu 9“ te direktive.

33. Katera koli omejitev mora „pomeni[ti] potreben, primeren in ustrezen ukrep znotraj demokratične družbe za zaščito državne varnosti (to je Državne varnosti), obrambe, javne varnosti in preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema iz člena 13(1) Direktive [95/46]“.

34. To naštevanje ciljev je izčrpno: [22] kot primer („med drugim“) se dovolijo „zakonsk[i] ukrep[i], ki določajo zadrževanje podatkov za določeno obdobje, upravičeno iz razlogov iz tega odstavka“.

35. Vsekakor so „[v]si ukrepi iz tega odstavka […] v skladu s splošnimi načeli zakonodaje Skupnosti, vključno s tistimi iz člena 6(1) in (2) Pogodbe o Evropski uniji“. Zato je treba člen 15(1) Direktive 2002/58 razlagati glede na temeljne pravice, zagotovljene z Listino. [23]

36. Od teh pravic, priznanih z Listino, je Sodišče omenilo – kolikor je pomembno za to zadevo – pravico do zasebnosti (člen 7), pravico do varstva osebnih podatkov (člen 8) in pravico do svobode izražanja (člen 11). [24]

37. Sodišče je prav tako poudarilo, in sicer kot smernico za njegovo razlago člena 15(1) Direktive 2002/58, da je treba obveznost zagotavljanja zaupnosti komunikacij in z njimi povezanih podatkov o prometu razlagati ozko.

38. Natančneje, zavrnilo je, „da odstopanje od te načelne obveznosti in zlasti od prepovedi hrambe teh podatkov, ki je določeno v členu 5 te direktive, postane pravilo, saj bi se sicer tej določbi v veliki meri odvzel pomen“. [25]

39. Ta dvojna ugotovitev se mi zdi odločilna za razumevanje, zakaj je Sodišče splošno in neselektivno hrambo podatkov o prometu in lokaciji v zvezi z elektronskimi komunikacijami štelo za nezdružljivo z Direktivo 2002/58.

21 Prav tam, točka 86, in fine.

22 Prav tam, točka 90.

23 Prav tam, točka 91 in navedena sodna praksa.

24 Prav tam, točka 93 in navedena sodna praksa.

25 Prav tam, točka 89.

40. S to izjavo je Sodišče zgolj „dosledno“ [26] uporabilo merilo sorazmernosti, ki ga je uporabilo že prej: [27] „varstvo temeljne pravice do spoštovanja zasebnega življenja na ravni Unije zahteva, da se odstopanja od varstva osebnih podatkov in njegove omejitve določijo v mejah tega, kar je nujno potrebno“. [28]

3. Sorazmernost pri hrambi podatkov

a) Nesorazmernost splošne in neselektivne hrambe

41. Sodišče je priznalo, da čeprav je boj proti hudemu kriminalu, zlasti proti organiziranemu kriminalu in terorizmu, nedvomno ključnega pomena za zagotavljanje javne varnosti, pa je njegova učinkovitost lahko precej odvisna od uporabe sodobnih preiskovalnih tehnik. Dodalo je, da pa „tak cilj v splošnem interesu, čeprav je temeljnega pomena, sam po sebi ne more upravičiti, da se ukrep hrambe, kot je uveden z Direktivo 2006/24, šteje za nujen za namene navedenega boja“. [29]

42. Da bi se ugotovilo, ali je bil tovrstni ukrep omejen na to, kaj je nujno potrebno, je Sodišče poudarilo predvsem posebno resnost njegovega posega v temeljne pravice, določene v členih 7 in 8 Listine. [30] Posebej resen poseg je izhajal ravno iz tega, da je nacionalna zakonodaja določala „splošno in neselektivno hrambo vseh podatkov o prometu in podatkov o lokaciji za vse naročnike in registrirane uporabnike glede vseh elektronskih komunikacijskih sredstev in da ponudnikom elektronskih komunikacijskih storitev nalaga, naj brez izjeme te podatke hranijo sistematično in kontinuirano“. [31]

43. Poseg v življenje državljanov, ki ga je pomenil ta ukrep, se odraža v tej presoji Sodišča o učinkih hrambe podatkov.

Na podlagi teh podatkov [32]

– „je mogoče najti in identificirati vir ter cilj komunikacije, datum, uro in trajanje te komunikacije, komunikacijsko opremo uporabnikov ter določiti lokacijo opreme za mobilno komunikacijo“; [33]

– „je mogoče predvsem izvedeti, s katero osebo je komuniciral naročnik ali registrirani uporabnik in katero sredstvo je uporabil za to, ter ugotoviti trajanje komunikacije in kraj, s katerega je potekala komunikacija. Poleg tega ti podatki omogočajo ugotoviti pogostost komunikacij naročnika ali registriranega uporabnika z določenimi osebami v danem obdobju“; [34]

26 Uporaba tega prislova v sodbi Tele2 Sverige in Watson, točka 95, izhaja iz uvodne izjave 11 Direktive 2002/58.

27 Sodba Digital Rights, točka 48: „[O]b upoštevanju, prvič, pomembne vloge varstva osebnih podatkov z vidika temeljne pravice do spoštovanja zasebnega življenja ter, drugič, obsega in teže poseganja v to pravico, ki jo pomeni Direktiva 2006/24, [je] polje proste presoje zakonodajalca Unije zmanjšano, tako da je treba izvajati strog nadzor.“

28 Sodba Tele2 Sverige in Watson, točka 96 in navedena sodna praksa.

29 Sodba Digital Rights, točka 51. V tem smislu sodba Tele2 Sverige in Watson, točka 103.

30 Sodbi Digital Rights, točka 65, ter Tele2 Sverige in Watson, točka 100.

31 Sodba Tele2 Sverige in Watson, točka 97. Moj poudarek.

32 Med katerimi so ime in naslov naročnika ali registriranega uporabnika, kličoča in klicana telefonska številka ter IP naslov za internetne storitve.

33 Sodba Tele2 Sverige in Watson, točka 98.

34 Prav tam, točka 98.

– „je mogoče izpeljati zelo natančne ugotovitve o zasebnem življenju oseb, katerih podatki so bili shranjeni, kot so vsakodnevne navade, kraji stalnega ali začasnega prebivališča, dnevne ali druge poti, dejavnosti, socialni odnosi teh oseb in družbeni krogi, v katerih se gibljejo“;[35]

– „je mogoče ugotoviti profil zadevnih oseb, kar so zelo občutljive informacije z vidika pravice do spoštovanja zasebnega življenja ter same vsebine komunikacij“.[36]

44. Poseg lahko poleg tega „pri zadevnih osebah povzroči občutek, da se njihovo zasebno življenje stalno nadzoruje“, saj „se hramba podatkov izvede, ne da bi bili uporabniki elektronskih komunikacijskih storitev o tem obveščeni“.[37]

45. Ob upoštevanju velikosti posega lahko samo boj proti hudim kaznivim dejanjem utemelji ukrep hrambe podatkov s temi značilnostmi.[38] Vendar navedenega ukrepa ni mogoče spremeniti v splošno pravilo, saj „ureditev, ki jo je uvedla Direktiva 2002/58, […] zahteva, da je ta hramba podatkov izjema“.[39]

46. Poleg tega sta hkrati podani dve značilnosti, ki izhajata iz tega, da obravnavani ukrep ni določal „nobenega razlikovanja, omejitve ali izjeme glede na cilj, ki se ga poskuša doseči“,[40] in „ne zahteva nobene povezave med podatki, za katere se določa hramba, in grožnjo za javno varnost“:[41]

– po eni strani se je ukrep nanašal „na splošno na vse osebe, ki uporabljajo elektronske komunikacijske storitve, s tem da te osebe niso – čeprav posredno – v položaju, ki bi lahko pripeljal do kazenskega pregona. […] Poleg tega ne določa nobene izjeme, tako da se uporablja tudi za osebe, katerih komunikacije so v skladu z nacionalnimi predpisi poslovna skrivnost“;[42]

– po drugi strani ureditev „ni omejena na hrambo bodisi podatkov v zvezi z začasnim obdobjem in/ali določenim z geografskim območjem in/ali krogom oseb, ki so lahko tako ali drugače vpletene v hudo kaznivo dejanje, bodisi podatkov v zvezi z osebami, ki bi lahko iz drugih razlogov, s tem da bi se hranili njihovi podatki, prispevale k boju proti kriminalu“.[43]

47. V teh okoliščinah je analizirana nacionalna zakonodaja presegla meje tega, kar je nujno potrebno. Zato je ni bilo mogoče šteti za upravičeno v demokratični družbi, kot to zahteva člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8, 11 in 52(1) Listine.[44]

b) Izvedljivost ciljne hrambe podatkov

48. Sodišče je sprejelo, da je v skladu s pravom Unije nacionalna zakonodaja, „ki preventivno dopušča ciljno hrambo podatkov o prometu in podatkov o lokaciji z namenom boja proti hudemu kriminalu“.[45]

35 Prav tam, točka 99.

36 Prav tam, točka 99, in fine.

37 Prav tam, točka 100.

38 Prav tam, točka 102.

39 Prav tam, točka 104.

40 Prav tam, točka 105.

41 Prav tam, točka 106.

42 Prav tam, točka 105.

43 Prav tam, točka 106.

44 Prav tam, točka 107.

45 Prav tam, točka 108. Moj poudarek.

49. Veljavnost te ciljne hrambe podatkov je pogojena s tem, da „se hramba podatkov glede kategorij hranjenih podatkov, zadevnih komunikacijskih sredstev, vpletenih oseb in trajanja zadevne hrambe omeji le na to, kar je nujno potrebno“.

50. Smernice, ki jih daje sodba Tele 2 Sverige in Watson, za ugotavljanje, kdaj so izpolnjeni ti pogoji, niso (niti ne bi mogle biti) izčrpne in so oblikovane bolj na splošno. Za njihovo upoštevanje morajo države članice:

– sprejeti jasne in natančne določbe, ki urejajo obseg in uporabo ukrepa hrambe tovrstnih podatkov;[46]

– določiti nekatera „objektivn[a] meril[a], ki določajo razmerje med podatki, ki jih je treba hraniti, in uresničevanim ciljem“;[47] ter

– se opreti „na objektivn[e] element[e], na podlagi katerih je mogoče opredeliti javnost, katere podatki lahko izkažejo zvezo, vsaj posredno, s hudimi kaznivimi dejanji, da tako ali drugače prispevajo k boju proti hudemu kriminalu ali da preprečijo resno nevarnost za javno varnost“.[48]

51. V zvezi s temi objektivnimi elementi Sodišče kot primer navaja možnost uporabe geografskega merila, da se omejijo potencialno prizadeti krog oseb in položaji. Menim, da namen navedbe tega merila, ki so ga nekatere države članice kritizirale, ni, da se izbira dopustnih dejavnikov selektivnosti omeji samo nanj.

4. Sorazmernost pri dostopu do podatkov

a) Sodba Tele2 Sverige in Watson

52. Sodišče obravnava dostop nacionalnih organov do podatkov ne glede na obseg obveznosti hrambe, ki je naložena ponudnikom elektronskih komunikacijskih storitev, in zlasti ne glede na splošnost ali posebnost hrambe teh podatkov.[49]

53. Čeprav je smisel hrambe olajšati poznejši dostop do podatkov, lahko namreč eno in drugo povzroči različne kršitve temeljnih pravic, varovanih z Listino. Vendar to razlikovanje ne pomeni, da nekateri pomisleki v zvezi s hrambo ne bi bili prav tako uporabljivi za dostop do hranjenih podatkov.

54. V tem smislu:

– mora dostop „dejansko in strogo ustrezati kateremu od teh ciljev“, ki so navedeni v členu 15(1), prvi stavek, Direktive 2002/58. Prav tako mora obstajati povezava med resnostjo posega in uresničevanim ciljem. Če se poseg opredeli kot resen, ga je mogoče utemeljiti samo z bojem proti hudemu kriminalu;[50]

46 Prav tam, točka 109. Zlasti morajo določiti, „v kakšnih okoliščinah in pod kakšnimi pogoji se lahko preventivno sprejme ukrep hrambe podatkov in s tem zagotovi, da se ta ukrep omeji na nujno potrebno“.

47 Prav tam, točka 110.

48 Prav tam, točka 111.

49 Prav tam, točka 113.

50 Prav tam, točka 115.

– je dostop mogoče dovoliti samo v mejah tega, kar je nujno potrebno.[51] Poleg tega morajo zakonodajni ukrepi določiti „jasna in natančna pravila, ki določajo, v katerih okoliščinah in pod kakšnimi pogoji morajo ponudniki elektronskih komunikacijskih storitev pristojnim nacionalnim organom omogočiti dostop do podatkov. Tak ukrep mora biti tudi zakonsko zavezujoč v nacionalnem pravu“;[52]

– natančneje, nacionalne ureditve morajo določiti „vsebinske in postopkovne pogoje, ki urejajo dostop pristojnih nacionalnih organov do hranjenih podatkov“.[53]

55. Iz zgoraj navedenega je mogoče izpeljati, da „ni mogoče šteti, da je splošni dostop do vseh hranjenih podatkov, neodvisno od kakršne koli vezi, tudi posredne, s ciljem, ki se mu sledi, omejen na nujno potrebno“.[54]

56. Po mnenju Sodišča „se mora zadevna nacionalna ureditev pri določitvi okoliščin in pogojev, pod katerimi se pristojnim nacionalnim organom omogoči dostop do podatkov naročnikov ali registriranih uporabnikov, opreti na objektivna merila“.[55] V zvezi s tem „je dostop v povezavi z namenom boja proti kriminalu načeloma mogoče odobriti le do podatkov oseb, za katere obstaja sum, da nameravajo izvršiti ali da so izvršile hudo kaznivo dejanje ali da so tako ali drugače povezane s tem kaznivim dejanjem“.[56]

57. Povedano drugače, nacionalni predpisi, ki pristojnim nacionalnim organom dovoljujejo dostop do hranjenih podatkov, morajo imeti dovolj omejen obseg. Obstajati mora povezava med prizadetimi osebami in uresničevanim ciljem, tako da dostop ne zajema precejšnjega števila oseb ali celo vseh oseb, vseh sredstev elektronske komunikacije in vseh hranjenih podatkov.

58. Vendar se lahko ta pravila v nekaterih okoliščinah omilijo. Sodišče omenja „posebn[e] okoliščin[e], kakršne so te, v katerih dejanja terorizma ogrožajo bistvene interese nacionalne varnosti, obrambe ali javne varnosti“. V takih primerih bi bilo mogoče „dostop do podatkov drugih oseb prav tako odobriti, kadar obstajajo objektivni elementi, na podlagi katerih je mogoče šteti, da bi ti podatki lahko v konkretnem primeru učinkovito prispevali k boju proti takim dejavnostim“.[57]

59. Ta obrazložitev Sodišča državam članicam omogoča, da vzpostavijo posebno ureditev obsežnejšega dostopa do podatkov, če bi bilo to izjemno pomembno za boj proti ogrožanju bistvenih državnih interesov (nacionalna varnost, obramba in javna varnost),[58] tako da zajema tudi osebe, ki so samo posredno povezane z navedenimi tveganji.

51 Prav tam, točka 116.

52 Prav tam, točka 117.

53 Prav tam, točka 118.

54 Prav tam, točka 119.

55 Idem.

56 Idem. Moj poudarek.

57 Idem.

58 Poleg terorističnih dejavnosti bi bila lahko ta izjema utemeljena z drugimi možnostmi, kot je obsežen kibernetski napad na ključne infrastrukture države ali nevarnost v zvezi s širjenjem jedrskega orožja.

60. Za dostop nacionalnih organov do hranjenih podatkov morajo biti ne glede na njihovo vrsto izpolnjeni trije pogoji:

– „načeloma, razen v nujnih primerih, ki so ustrezno utemeljeni, sodišče ali neodvisen upravni organ opravi predhoden nadzor“. Odločba tega sodišča ali tega organa [se] izda na obrazložen predlog, ki se ga predloži v postopku preprečevanja, odkrivanja ali pregona kaznivih dejanj“; [59]

– „[p]ristojni nacionalni organi, ki jim je bil odobren dostop do hranjenih podatkov, v okviru veljavnih nacionalnih postopkov o tem obvestijo zadevne osebe takoj, ko to sporočilo ne more ogroziti preiskav, ki jih vodijo ti organi“; [60]

– države članice morajo sprejeti predpise o varnosti in varstvu podatkov, ki jih imajo ponudniki elektronskih komunikacijskih storitev, da bi se preprečila zloraba in nepooblaščen dostop do podatkov. [61]

b) Sodba Ministerio Fiscal

61. V tej zadevi se je spraševalo, ali je v skladu s členom 15(1) Direktive 2002/58, ki se razlaga glede na člena 7 in 8 Listine, nacionalni predpis, ki določa dostop pristojnih organov do podatkov v zvezi z istovetnostjo imetnikov nekaterih kartic SIM.

62. Sodišče je ugotovilo, da člen 15(1), prvi stavek, Direktive 2002/58 ne omejuje cilja preprečevanja, preiskovanja, odkrivanja in preganjanja kaznivih dejanj samo na boj proti hudim kaznivim dejanjem, temveč da se sklicuje na „kazniva dejanja“ na splošno. [62]

63. Dodalo je, da mora za utemeljitev dostopa do podatkov s strani pristojnih nacionalnih organov obstajati skladnost med resnostjo posega in težo zadevnih kaznivih dejanj. Zato:

– „hud poseg upraviči le cilj boja proti kriminalu, ki mora biti prav tako opredeljen kot ‚hud‘“; [63]

– nasprotno, „[k]adar poseg, ki ga pomeni dostop do podatkov, ni hud, se navedeni dostop lahko upraviči tudi s ciljem preprečevanja, preiskovanja, odkrivanja in pregona ‚kaznivih dejanj‘ na splošno“. [64]

64. Izhajajoč iz te domneve in drugače od tega, do česar je prišlo v sodbi Tele2 Sverige in Watson, Sodišče posega v pravice, ki jih varujeta člena 7 in 8 Listine, ni opredelilo kot „hudega“, saj je bil edini cilj zahteve za dostop „identifikacija imetnikov kartic SIM, ki so bile v obdobju dvanajstih dni aktivirane s številko IMEI ukradenega mobilnega telefona“. [65]

[59] Sodba Tele2 Sverige in Watson, točka 120.

[60] Prav tam, točka 121.

[61] Prav tam, točka 122.

[62] Sodba Ministerio Fiscal, točka 53.

[63] Prav tam, točka 56.

[64] Prav tam, točka 57.

[65] Prav tam, točka 59. Šlo je za dostop „do telefonskih številk, ki ustrezajo tem karticam SIM, in do podatkov o osebni istovetnosti imetnikov navedenih kartic, kot so priimek, ime in po potrebi naslov. Nasprotno pa se, kot sta na obravnavi potrdila španska vlada in državno tožilstvo, ti podatki ne nanašajo na komunikacije, ki so bile opravljene z ukradenim mobilnim telefonom, niti na njegovo lokacijo.“

65. Da bi Sodišče poudarilo manjšo resnost posega, je pojasnilo, da „podatki iz zahteve za dostop iz postopka v glavni stvari omogočajo zgolj povezavo – v nekem obdobju – med kartico ali karticami SIM, aktiviranimi z ukradenim mobilnim telefonom, in osebno istovetnostjo imetnikov teh kartic SIM. Brez prekrivanja s podatki, ki se nanašajo na komunikacije, opravljene z navedenimi karticami SIM, in podatki o lokaciji navedeni podatki ne omogočajo seznanitve z datumom, uro, trajanjem in prejemniki komunikacij, opravljenih z zadevno kartico ali karticami SIM, niti z okoljem, v katerem so bile te komunikacije opravljene, ali z njihovo pogostostjo z določenimi osebami v danem obdobju. Navedeni podatki zato ne omogočajo izpeljave natančnih ugotovitev o zasebnem življenju oseb, za podatke katerih gre.“ [66]

66. V zadevi, obravnavani v sodbi Ministerio Fiscal, se ni spraševalo, ali so ponudniki elektronskih komunikacij hranili osebne podatke, do katerih se je dostopalo, v skladu s pogoji, določenimi v členu 15(1) Direktive 2002/58 v povezavi s členoma 7 in 8 Listine. [67] Niti se ni obravnavalo vprašanje, ali so bili izpolnjeni drugi pogoji za dostop, ki izhajajo iz tega člena, ali ne.

67. Zato iz sodbe Ministerio Fiscal ni mogoče sklepati o nikakršni spremembi sodne prakse Sodišča o nezdružljivosti nacionalne ureditve, ki dovoljuje splošno in neselektivno shranjevanje podatkov, s pravom Unije v smislu sodbe Tele2 Sverige in Watson.

68. Vendar menim, da Sodišče, ker je priznalo veljavnost ureditve dostopa, omejenega na nekatere osebne podatke (v zvezi z istovetnostjo imetnikov kartic SIM), implicitno sprejema hrambo teh istih podatkov s strani ponudnikov storitve.

C. Glavne kritike sodne prakse Sodišča

69. Tako predložitveno sodišče kot večina držav članic, ki so predložile pisna stališča, pozivajo Sodišče, naj pojasni, podrobneje opredeli ali celo ponovno premisli o številnih vidikih svoje sodne prakse na tem področju, ki je tarča njihovih kritik.

70. Večina teh kritik, prikritih ali neposrednih, je bila že izražena glede sodbe Digital Rights in jih je Sodišče zavrnilo v sodbi Tele 2 Sverige in Watson. Zdaj so se pojavile ponovno, da bi se z njimi, če povzamem, izpostavilo, da bi zadostovalo nekaj strogih predpisov glede dostopa do podatkov v rokah ponudnikov elektronskih komunikacijskih storitev, ki bi nekako kompenzirali resnost posega, ki ga pomeni splošna in neselektivna hramba teh podatkov.

71. V številnih od teh kritik se prav tako poudarja nujnost, da se sprejmejo resnično učinkoviti ukrepi za boj proti hudim grožnjam varnosti in proti kriminalu na splošno, ter je Sodišče zaprošeno, naj upošteva pravico do varnosti (člen 6 Listine) in diskrecijsko pravico držav članic, da zagotavljajo nacionalno varnost. V enem primeru je dodano, da Sodišče ni pretehtalo preventivne narave posredovanja varnostnih in obveščevalnih služb.

66 Prav tam, točka 60.

67 Sodba Ministerio Fiscal, točka 49.

D. Moje mnenje o teh kritikah in manjših spremembah, ki bi se lahko uvedle v sodno prakso Sodišča

72. Menim, da bi moralo Sodišče vztrajati pri načelnem stališču, ki ga je zavzelo v prejšnjih sodbah: splošna in neselektivna obveznost hrambe vseh podatkov o prometu in lokaciji vseh registriranih naročnikov in uporabnikov nesorazmerno krši temeljne pravice, varovane s členi 7, 8 in 11 Listine.

73. A sensu contrario, nacionalna zakonodaja, s katero bi bile določene ustrezne omejitve hrambe nekaterih od teh podatkov, ustvarjenih v okviru opravljanja elektronskih komunikacijskih storitev, bi lahko bila skladna s pravom Unije. Rešitev je torej v omejeni hrambi teh podatkov.

74. Kakor bom pojasnil v nadaljevanju, ta omejena hramba ne bi smela biti samo tista, katere predmet je geografsko območje ali kategorija konkretnih oseb: razprave o teh merilih hrambe razkrivajo, da bi ta merila gotovo bila neuresničljiva ali neučinkovita za zasledovane namene ali celo da bi se pretvorila v vir diskriminacije.

75. Za začetek se ne strinjam s kritičnim argumentom, ki zagovarja binom „bolj razširjena hramba v zameno za bolj omejen dostop“. Razlogovanje Sodišča, s katerim se strinjam, je, da sta hramba in dostop do podatkov dve različni vrsti posega. Čeprav je hramba podatkov smiselna z vidika mogočega poznejšega dostopa s strani pristojnih organov, je treba vsakega od teh posegov utemeljiti ločeno, s posebnim preizkusom glede na uresničevani cilj.

76. Nacionalnega sistema, ki določa splošno in neselektivno hrambo podatkov, torej ni mogoče utemeljiti s tem, da zadevni predpisi hkrati uvajajo stroge materialne in procesne zahteve za dostop do navedenih podatkov.

77. Torej je treba imeti nekatere predpise, ki so posebej povezani s hrambo podatkov, za katero veljajo nekateri pogoji, da se prepreči njena splošnost in neselektivnost. Samo tako se zagotovi njena skladnost s členom 15(1) Direktive 2002/58 v povezavi s členi 7, 8, 11 in 52(1) Listine.

78. Poleg tega je to pristop, ki so ga sprejele delovne skupine v okviru Sveta za opredelitev pravil o hrambi in dostopu, skladnih s sodno prakso Sodišča, pri čemer so hkrati preučevale ti dve vrsti posegov.[68]

79. Z uporabo omejitev za vsako od teh dveh vrst posegov se lahko oceni, ali je morebitni kumulativni učinek teh omejitev v kombinaciji s strogimi zaščitnimi ukrepi tak, da omili učinek hrambe podatkov na temeljne pravice, varovane s členi 7, 8 in 11 Listine, hkrati pa zagotavlja učinkovitost preiskav.

80. Da bi sistem varoval te pravice, mora biti z njim:

– določena hramba podatkov, ki vsebuje nekatere omejitve in razlike glede na uresničevani cilj;

– urejen dostop do teh podatkov samo v obsegu, ki je nujno potreben za uresničevani namen, in pod nadzorom sodišča ali neodvisnega upravnega organa.

[68] Države članice od leta 2017 sodelujejo v delovni skupini, katere namen je, da prilagodijo svoje zakonodaje merilom, določenim na tem področju v sodni praksi Sodišča (Groupe Échange d'informations et protection des données (DAPIX)).

81. Utemeljitev za to, da ponudniki elektronskih komunikacijskih storitev hranijo nekatere podatke, in to ne samo za upravljanje svojih pogodbenih obveznosti, ki jih imajo do uporabnikov, se povečuje skupaj s tehnološkim napredkom. Če se prizna, da je ta hramba koristna za preprečevanje kriminala in boj proti njemu (kar je težko izpodbijati[69]), se ne bi zdelo logično omejiti njenega obsega zgolj na uporabo podatkov, ki jih ponudniki hranijo zaradi opravljanja svojih komercialnih dejavnosti, in samo za čas, ki je potreben za navedene dejavnosti.

82. Ko se enkrat prizna koristnost obveznosti hrambe podatkov za zagotavljanje nacionalne varnosti in boj proti kriminalu, ki presega to, kar lahko ponudniki izvedejo za svoje tehnične in komercialne potrebe, je nujno opredeliti okvire te obveznosti.

83. Vsaka ureditev hrambe mora biti strogo prilagojena uresničevanemu cilju, tako da se ne more pretvoriti v neselektivno hrambo.[70] Prav tako se mora pri tej ureditvi izključiti, da bi vsi ti podatki skupaj omogočili ustvaritev profila zadevne osebe (to je profila o njenih običajnih dejavnostih in socialnih odnosih), ki bi se približal ali bi bil podoben tistemu, ki bi se pridobil, če bi bila znana vsebina komunikacij.

84. Za razjasnitev nekaterih nesporazumov in nekaterih nerazumevanj je treba upoštevati, česa Sodišče ni ugotovilo v svojih sodbah Digital Rigths ter Tele2 Sverige in Watson. V njih ni obsodilo samega obstoja ureditve hrambe podatkov kot koristnega instrumenta za boj proti kriminalu. Nasprotno, priznalo je legitimnost cilja preprečevanja in zatiranja kaznivih dejanj, pa tudi koristnost ureditve hrambe podatkov za doseganje tega cilja.

85. Če ponovim, je torej zavrnilo, in to odločno, da bi Unija ali njene države članice ob sklicevanju na ta cilj lahko naložile neselektivno hrambo vseh podatkov, ki nastanejo pri opravljanju elektronskih komunikacijskih storitev, in splošen dostop do navedenih podatkov.

86. Zato je treba najti oblike hrambe podatkov, ki ne bo ustrezala tem pridevnikom („splošna in neselektivna“), ki niso skladni z varstvom, ki se zahteva s členi 7, 8 in 11 Listine.

87. Ena od teh oblik bi bila ciljna hramba podatkov, ki bi se nanašali bodisi na neko javnost (v teoriji tisto, ki ima določene povezave, bolj ali manj neposredne, z najresnejšimi grožnjami) ali pa na neko geografsko območje.

88. Vendar ta pristop povzroči nekaj težav:

– identifikacija skupine potencialnih storilcev bi bila verjetno nezadostna, če ti uporabljajo tehnike anonimizacije ali ponarejajo svoje identitete. Izbira teh skupin bi lahko poleg tega pripeljala do uvedbe take ureditve, kjer bi se na splošno sumili nekateri sloji prebivalstva, in bi se glede na uporabljeni algoritem opredelila kot diskriminatorna;

– izbira glede na geografska merila (ki bi se morala, da bi bila učinkovita, nanašati na ne preveč zmanjšana območja) povzroča te iste težave in dodaja druge, kot je na obravnavi navedel Evropski nadzornik za varstvo podatkov, saj bi lahko stigmatizirala nekatera območja.

89. Poleg tega bi lahko obstajalo neko protislovje med preventivnostjo hrambe, usmerjeno na neko javnost ali geografsko območje, in tem, da storilci kaznivih dejanj niso znani vnaprej, kakor tudi ne kraj in čas storitve teh kaznivih dejanj.

69 Vsekakor je določitev preiskovalnih tehnik in presoja njihove učinkovitosti v polju proste presoje držav članic.

70 Sodba Digital Rights, točka 57, ter sodba Tele2 Sverige in Watson, točka 105.

90. Kakor koli že, ni treba izključiti, da se najdejo formule selektivne hrambe, ki temeljijo na teh merilih in ki bi bile koristne za uresničevanje že opisanih ciljev. Naloga zakonodajne oblasti v vsaki državi članici ali za celotno Unijo je, da oblikuje te formule, ki spoštujejo varstvo temeljnih pravic, ki jih Sodišče varuje.

91. Napačno bi bilo misliti, da je ciljna hramba podatkov, ki se nanašajo na določeno javnost ali na določeno geografsko območje, edina formula, za katero je Sodišče štelo, da je združljiva s členom 15(1) Direktive 2002/58 v povezavi s členoma 7 in 8 Listine.

92. Vztrajam pri tem, da je mogoče najti druge oblike ciljne hrambe podatkov poleg tistih, ki se osredotočajo na določene skupine oseb ali geografska območja. Tako so namreč menile delovne skupine Sveta, ki sem jih omenil zgoraj: pri raziskovanju drugih oblik so obravnavale zlasti omejitev kategorij shranjenih podatkov[71]; psevdonimizacijo podatkov[72]; uvedbo omejenih obdobij hrambe[73]; izključitev nekaterih kategorij ponudnikov elektronskih komunikacijskih storitev[74]; obnovljiva dovoljenja za hrambo[75]; obveznost hrambe shranjenih podatkov v Uniji ali sistematični in redni nadzor s strani neodvisnega upravnega organa nad jamstvi, ki jih dajo ponudniki elektronskih komunikacijskih storitev v zvezi z zlorabo podatkov.

93. Menim, da bi začasna hramba nekaterih kategorij podatkov o prometu in lokaciji, ki bi bile omejene glede na nujno potrebo po varnosti in ki kot celota ne bi omogočale pridobitve natančne in podrobne slike o življenju zadevnih oseb, zato da bi bila skladna s sodno prakso Sodišča, morala imeti prednost.

94. V praksi to pomeni, da se morajo poleg dveh glavnih kategorij (podatki o prometu in podatki o lokaciji) hraniti prek ustreznih filtrov samo minimalni podatki, ki se štejejo za absolutno nujne za učinkovito preprečevanje in nadzor kriminala in za zagotavljanje nacionalne varnosti.

95. Naloga držav članic ali institucij Unije je, da se po zakonodajni poti (s pomočjo lastnih strokovnjakov) odločijo za eno od teh možnosti, pri tem pa morajo opustiti kakršen koli poskus, da naložijo splošno in neselektivno hrambo vseh podatkov o prometu in lokaciji.

71 Podatki, ki niso nujno in objektivno potrebni za preprečevanje in preganjanje kaznivih dejanj ter varstvo javne varnosti, bi bili izključeni iz obveznosti hrambe. Zlasti bi bilo treba v skladu z uresničevanim ciljem navesti, katere vrste podatkov naročnikov, podatkov o prometu in podatkov o lokaciji bi bilo treba obvezno shraniti, da bi se uresničil navedeni cilj. Zlasti bi bili izključeni podatki, ki se ne štejejo za nujne za preiskovanje in pregon kaznivih dejanj.

72 Metoda, s katero se imena nadomestijo z vzdevkom, s čimer se podatki ne povežejo več z imenom. Drugače od anonimizacije psevdonimizacija omogoča, da se podatki ponovno povežejo z imenom posameznika, na katerega se nanašajo osebni podatki.

73 Mogoče bi bilo razmisliti o možnosti spremembe obdobij hrambe glede na različne kategorije podatkov ob upoštevanju njihove narave, ki bolj ali manj posega v zasebno življenje oseb. Poleg tega bi bilo treba določiti, da se po koncu obdobja hrambe podatki trajno izbrišejo.

74 Mogoče bi bilo razmisliti o možnosti, da se obveznost hrambe podatkov ne naloži vsem ponudnikom elektronskih komunikacijskih storitev, temveč da se ta obveznost naloži glede na njihovo velikost in vrsto storitev, ki jih ponujajo, pri tem pa se izključijo na primer tisti, ki ponujajo visoko specializirane storitve.

75 Sistemi avtorizacije bi lahko temeljili na rednih ocenah ogroženosti v vsaki državi članici. Zagotoviti je treba, da se povezava med shranjenimi podatki in uresničevanim ciljem ustvari in prilagodi konkretnemu položaju vsake države članice. Zato bi bilo mogoče, da bi lahko dovoljenja za hrambo, podeljena ponudnikom, privedla do hrambe nekaterih vrst podatkov v nekem obdobju, odvisno od ocene ogroženosti. Ta dovoljenja bi lahko podelilo sodišče ali neodvisni upravni organ in bi bila predmet rednega preverjanja, ali je ta hramba nujno potrebna.

96. Poleg omejitve glede na kategorije se smejo hranjeni podatki hraniti samo za obdobje hrambe, zato da ni mogoče dobiti podrobne slike o življenju zadevnih oseb. To obdobje hrambe se mora poleg tega prilagoditi glede na naravo podatkov, zato da se tisti podatki, ki dajejo najnatančnejše informacije o načinu življenja in navadah teh oseb, hranijo najkrajši čas.[76]

97. Povedano drugače, razlikovanje obdobja hrambe vsake kategorije podatkov glede na njihovo koristnost pri uresničevanju varnostnih ciljev je ena pot, ki jo je treba raziskati. Z omejitvijo časa, ko se ene in druge kategorije podatkov hranijo hkrati (in se torej lahko uporabijo za odkrivanje korelacij, ki razkrijejo način življenja zadevnih oseb), se razširi varstvo pravice, ki jo varuje člen 8 Listine.

98. V tem smislu se je med obravnavo izrekel Evropski nadzornik za varstvo podatkov: kolikor več je kategorij shranjenih metapodatkov in kolikor daljše je obdobje hrambe, toliko enostavneje je narediti podroben profil osebe, in obratno.[77]

99. Kot je bilo ravno tako izpostavljeno na obravnavi, je sicer težko zarisati mejo med določenimi metapodatki elektronskih komunikacij in vsebino teh komunikacij. Nekateri metapodatki lahko razkrijejo toliko kot sama vsebina teh komunikacij ali celo več: tako je lahko v primeru naslovov (URL) obiskanih spletnih strani.[78] Zato bi bilo treba tej vrsti podatkov in drugim podobnim podatkom posvetiti posebno pozornost, da se kar najbolj omeji nujnost njihove hrambe in njeno trajanje.

100. Ni enostavno najti uravnotežene rešitve, saj navzkrižno preverjanje hranjenih podatkov in iskanje korelacij med njimi preiskovalnim in nadzornim službam omogoča identifikacijo osumljenca ali grožnje, odvisno od primera. Vendar obstaja razlika v stopnji med hrambo podatkov za odkrivanje tega osumljenca ali te grožnje in hrambo, katere rezultat je podrobna slika o življenju osebe.

101. Ob čakanju na skupno ureditev za celotno Unijo na tem konkretnem področju menim, da je lahko Sodišče zaprošeno, naj prevzame regulatorno nalogo in podrobno opredeli, katere kategorije podatkov se lahko hranijo in koliko časa. Naloga institucij Unije in držav članic je, da se – ko bodo omejitve, ki po mnenju Sodišča izhajajo iz Listine, določene – osredotočijo na pravo mesto, da dosežejo ravnotežje med ohranjanjem varnosti in temeljnimi pravicami, varovanimi z Listino.

102. Res je, da bi neupoštevanje informacij, ki jih je mogoče izpeljati iz večjega števila shranjenih podatkov, lahko v nekaterih primerih otežilo boj proti potencialnim grožnjam. Vendar je to davek kot vsi drugi, ki jih morajo javni organi plačati, če si naložijo obveznost varovanja temeljnih pravic.

103. Tako kot nihče ne podpira ex ante obveznosti splošne in neselektivne hrambe vsebin zasebnih elektronskih komunikacij (niti če zakoni zagotavljajo poznejši omejen dostop do navedenih vsebin), ne smejo biti niti metapodatki teh komunikacij, ki bi lahko odražali tako občutljive informacije, kot so same vsebine, predmet neselektivne in splošne hrambe.

[76] Zdi se, da je to sistem, ki se uporablja v Zvezni republiki Nemčiji, katere vlada je na obravnavi navedla, da je v skladu z njeno zakonodajo rok hrambe podatkov o prometu deset tednov, medtem kot je rok hrambe podatkov o lokaciji samo štiri tedne. Po drugi strani Francoska republika meni, da je za hrambo podatkov o prometu in lokaciji nujno potrebno obdobje enega leta. Po mnenju te države članice bi skrajšanje tega roka na manj kot eno leto povzročilo zmanjšanje učinkovitosti opravljanja nalog kriminalistične policije.

[77] Seveda je treba zagotoviti, da ponudniki elektronskih komunikacijskih storitev trajno izbrišejo podatke po koncu obdobja hrambe (razen tistih, ki jih v skladu z Direktivo 2002/58 lahko še naprej shranjujejo iz komercialnih razlogov).

[78] Francoska vlada je na obravnavi potrdila, da so URL izključeni iz podatkov o povezavi, za katere je v njeni zakonodaji določena splošna obveznost hrambe.

104. V zakonodaji se sicer pojavi težava (ki jo priznavam), da se natančno opredelijo primeri in pogoji, v katerih je treba izvesti ciljno hrambo, vendar ta težava ne upravičuje, da države članice s tem, da izjema postane pravilo, spremenijo splošno hrambo osebnih podatkov v temeljno načelo svojih zakonodaj. Če bi bilo tako, bi se dopustila neomejena veljavnost pomembne kršitve pravice do varstva osebnih podatkov.

105. Moram dodati, da nič ne preprečuje, da nacionalna zakonodaja v res izjemnih primerih, za katere je značilna neposredna grožnja ali izredno tveganje in ki utemeljujejo uradno razglasitev izrednega stanja v državi članici, za določen čas določi možnost naložitve obveznosti hrambe podatkov, ki je tako obsežna in splošna, kolikor se šteje za nujno potrebno.

106. V teh okoliščinah bi se lahko sprejela ureditev, ki posebej dovoljuje obsežnejšo hrambo podatkov (in dostop do njih), v skladu s pogoji in postopki, ki zagotavljajo, da so ti ukrepi izredni z vidika materialnega obsega in časovnega trajanja, ter ustrezna sodna jamstva.

107. Primerjalna analiza zakonodajnih ureditev, ki urejajo izredne razmere, pokaže, da ni nemogoče navesti dejanskih primerov, ki bi lahko sprožili uporabo posebne zakonodajne ureditve, ki bi določala, da organ lahko sprejme to odločitev, pod kakšnimi pogoji in pod kakšnim nadzorom.[79]

E. Konkretni odgovori na tri vprašanja za predhodno odločanje

1. Uvodni preudarek

108. Predložitveno sodišče prosi za razlago člena 15(1) Direktive 2002/58 v povezavi z več pravicami, zagotovljenimi z Listino: pravico do spoštovanja zasebnega in družinskega življenja (člen 7), pravico do varstva osebnih podatkov (člen 8) ter pravico do svobode izražanja in obveščanja (člen 11).

109. Kot sem pojasnil v sklepnih predlogih v zadevah C-511/18 in C-512/18, so to namreč pravice, ki bi bile po mnenju Sodišča v teh primerih lahko prizadete.

110. Vendar Cour constitutionnelle (ustavno sodišče) omenja tudi člena 4 in 6 Listine, na katera se nanašata drugo oziroma prvo vprašanje za predhodno odločanje.

111. Člen 6 Listine, ki zagotavlja pravico do svobode in varnosti, je bil omenjen tudi v zadevah C-511/18 in C-512/18, o njegovi upoštevnosti pa sem se izrekel v povezanih sklepnih predlogih, na katere napotujem.[80]

112. V zvezi s členom 4 Listine, glede na to, da odgovor ni odvisen toliko od analize nacionalne zakonodaje, ki bi jo preverjali glede na pravo Unije, kot od razlage te določbe, se mi zdi nanj primerno odgovoriti najprej.

[79] Ackerman, B., „The Emergency Constitution“, Yale Law Journal, zv. 113, 2004, str. od 1029 do 1092; Ferejohn, J., in Pasquino, P., „The Law of the Exception: A typology of Emergency Powers“, International Journal of Constitutional Law, zv. 2, 2004, str. od 210 do 239.

[80] Sklepni predlogi v zadevah C-511/18 in C-512/18, točka 95 in naslednje.

2. Drugo vprašanje za predhodno odločanje

113. Sklicevanje na prepoved mučenja in nečloveškega ali ponižujočega ravnanja ali kaznovanja, določeno v členu 4 Listine, se namreč pojavi samo v tem predlogu za sprejetje predhodne odločbe, zaradi česar se ji moram posvetiti.

114. S sklicevanjem na člen 4 Listine želi predložitveno sodišče izpostaviti, da se z nacionalnim predpisom želi izpolniti pozitivna obveznost, ki jo ima javni organ, da vzpostavi „zakonski okvir, ki omogoča učinkovito kazensko preiskavo in učinkovito kaznovanje spolnih zlorab mladoletnikov ter ki omogoča uspešno identifikacijo storilcev teh kaznivih dejanj, tudi kadar se uporabijo sredstva za elektronsko komuniciranje“. [81]

115. Menim, da se ta konkretna pozitivna obveznost ne razlikuje preveč od vsake od konkretnih dolžnosti, v katere se za državo spremeni razglasitev seznama temeljnih pravic. Pravica do življenja (člen 2 Listine), pravica do osebne celovitosti (člen 3 Listine) ali varstvo podatkov (člen 8 Listine) kot tudi svoboda izražanja (člen 11 Listine) ali misli, vesti in vere (člen 10 Listine) pomenijo za državo obveznost, da določi normativni okvir, v katerem se zagotovi njihovo učinkovito uresničevanje, po potrebi z uporabo sile, nad katero ima monopol javna oblast, v razmerju do vsakogar, ki skuša ovirati ali otežiti njihovo uresničevanje. [82]

116. ESČP v zvezi s spolno zlorabo mladoletnih oseb meni, da imajo otroci in ostale ranljive osebe kvalificirano pravico do varstva s strani države prek sprejetja kazenskopravnih predpisov, ki učinkovito in odvračilno sankcionirajo storitev teh kaznivih dejanj. [83]

117. Ta kvalificirana pravica do varstva ima svoj okvir ne samo v členu 4 Listine, ampak bi se lahko seveda navedel tudi člen 1 (človekovo dostojanstvo) ali člen 3 (pravica do telesne in duševne celovitosti).

118. Čeprav pozitivne obveznosti javnih organov, da zagotovijo varstvo otrok in drugih ranljivih oseb, ni mogoče pustiti ob strani, ko se tehtajo pravne dobrine, ki so prizadete z nacionalno zakonodajo, [84] pa prav tako ne more postati „nesorazmerno breme“ za javni organ [85] niti se ne more izpolniti ne glede na zakonitost ali spoštovanje ostalih temeljnih pravic. [86]

81 Izraženo v drugem vprašanju, in fine. Ta omemba sredstev za elektronsko komuniciranje pojasnjuje, da je v vprašanju omenjena druga pozitivna obveznost, ki jo imajo države, in sicer ta, ki jo nalaga člen 8 Listine v zvezi z varstvom osebnih podatkov. Dvojno sklicevanje na člen 8 Listine kaže na to, da predložitveno sodišče pravicam iz Listine pripisuje dvojno nalogo glede na njihovo naravo: kot omejitev sporne obveznosti in kot utemeljitev navedene obveznosti.

82 Ta obveznost učinkovitosti se izraža v mandatu javnega organa, da dosega rezultate, v socialni državi ali državi blaginje, v kateri je poleg uradnega priznanja pravic pomembno praktično izvajanje njihove materialne vsebine.

83 Sodba ESČP z dne 2. decembra 2008, K. U. proti Finski (ECHR:2008:1202JUD000287202, točka 46).

84 V zvezi s tem menim, da bi bilo mogoče k pravicam, ki jih navaja predložitveno sodišče (kot omejitve sporne obveznosti, ne kot njena utemeljitev), dodati pravico do učinkovitega pravnega sredstva (člen 47 Listine) ali pravico do obrambe (člen 48 Listine), o morebitni kršitvi katere se je prav tako razpravljalo v postopkih v glavni stvari. Vendar se izrek predložitvene odločbe nanaša samo na člene 7, 8, 11 in 52(1) Listine.

85 Sodba ESČP z dne 28. oktobra 1998, Osman proti Združenemu kraljestvu (CE:ECHR:1998:1028JUD002345294, točka 116).

86 Prav tam, točka 116, in fine: „zagotoviti [je treba], da policija svoja pooblastila za boj in preprečevanje kriminala izvaja ob popolnem upoštevanju zakonskih poti in drugih jamstev, ki legitimno omejujejo obseg njenih dejanj v okviru kazenske preiskave“. Glej tudi sodbo ESČP z dne 2. decembra 2008, K. U. proti Finski (ECHR:2008:1202JUD000287202, točka 48). V tem smislu je Sodišče v sodbi z dne 29. julija 2019, Gambino in Hyka (C-38/18, EU:C:2019:628, točka 49), razglasilo, da pravice v korist žrtve ne morejo posegati v učinkovito uveljavljanje procesnih pravic, priznanih obdolžencu.

3. Prvo vprašanje za predhodno odločanje

119. Predložitveno sodišče želi skratka izvedeti, ali pravo Unije nasprotuje nacionalnemu zakonu, glede katerega je bilo pozvano, naj se izreče v okviru tožbe za razveljavitev zakona.

120. Ker je Sodišče že podalo razlago Direktive 2002/58, ki je v skladu z ustreznimi določbami Listine, se mora pri odgovoru na vprašanje za predhodno odločanje upoštevati sodna praksa iz sodbe Tele2 Sverige in Watson, po potrebi z manjšimi spremembami, ki se bodo dodale zdaj.

121. Na podlagi te premise se morajo razlagalne smernice, ki se lahko dajo Cour constitutionnelle (ustavno sodišče), da bi to samo preizkusilo skladnost nacionalnega predpisa s pravom Unije, nanašati ločeno na hrambo in na dostop do podatkov, kakor sta urejena v tem nacionalnem predpisu.

a) Pogoji hrambe podatkov

122. Belgijska vlada poudarja, da je želela vzpostaviti jasen pravni okvir, ki bi vključeval jamstva, potrebna za varstvo zasebnega življenja, namesto da bi temeljil na praksi operaterjev elektronskih komunikacijskih storitev v zvezi s hrambo podatkov zaradi izdajanja računov in obravnave zahtev strank po informacijah.

123. Za to vlado predvideni namen splošne in preventivne obveznosti hrambe podatkov ni samo odkrivanje, preiskovanje in preganjanje hudih kaznivih dejanj, temveč tudi zagotavljanje nacionalne varnosti, obramba in javna varnost, preiskovanje, odkrivanje in pregon dejanj, ki niso huda kazniva dejanja, ali preprečevanje prepovedane uporabe sistemov elektronskih komunikacij,[87] ali kateri koli drug cilj, opredeljen v členu 23(1) Uredbe 2016/679.

124. Po mnenju belgijske vlade:

– Na podlagi hrambe podatkov kot take ni mogoče izpeljati zelo natančnih sklepov o zasebnem življenju zadevnih oseb: možnost izpeljave takih sklepov bi obstajala samo, če bi se olajšal dostop do shranjenih podatkov.

– Zakon vsebuje previdnostne ukrepe za zaščito zasebnosti; med drugim, hramba podatkov ne vpliva na vsebino komunikacij; jamstva v zvezi z utemeljitvijo hrambe, pravica do dostopa, pravica do popravka in druge pravice veljajo v celoti; za ponudnike in operaterje veljajo v zvezi s shranjenimi podatki iste obveznosti ter varnostni in zaščitni ukrepi, ki veljajo za podatke v omrežju, s čimer se preprečuje njihovo nenamerno ali nezakonito uničenje, njihova naključna izguba ali sprememba.

– Podatki se lahko hranijo dva meseca (po koncu tega obdobja jih je treba uničiti) in samo na ozemlju Unije.

– Ponudniki in operaterji morajo uporabiti ukrepe za tehnično zaščito, zaradi katerih hranjeni podatki takoj, ko se zabeležijo, postanejo neberljivi in neuporabni za vsako osebo, ki ni pooblaščena, da do njih dostopa.

[87] Prav tako je utemeljena pri odzivu na klic na urgentno službo ali zaradi iskanja pogrešane osebe, katere telesna celovitost je v neposredni nevarnosti.

– Vsekakor se te operacije izvajajo pod nadzorom belgijskega regulativnega organa v poštnem in telekomunikacijskem sektorju ter organa za varstvo podatkov.

125. Kljub temu je res, da belgijska zakonodaja operaterjem in ponudnikom elektronskih komunikacijskih storitev nalaga splošno in neselektivno obveznost, da hranijo podatke o prometu in lokaciji v smislu Direktive 2002/58, ki se obdelujejo v okviru opravljanja teh storitev. Obdobje hrambe je, kot je bilo že navedeno, na splošno dvanajst mesecev: ni določena nobena časovna omejitev glede na kategorije shranjenih podatkov.

126. Ta obveznost splošne in neselektivne hrambe velja stalno in neprekinjeno. Čeprav bi bil njen cilj preprečevanje, preiskovanje in preganjanje vseh vrst kaznivih dejanj (od tistih, ki so povezana z nacionalno varnostjo, obrambo ali posebej hudimi kaznivimi dejanji, do tistih, za katere je zagrožena zaporna kazen do enega leta), obveznost s takimi značilnostmi ni v skladu s sodno prakso Sodišča, tako da je ni mogoče šteti za združljivo z Listino.

127. Da bi se belgijski zakonodajalec uskladil s to sodno prakso, mora raziskati druge poti (drugačne od prej omenjenih), ki uvajajo formule omejene hrambe. Te formule, ki se razlikujejo glede na kategorije podatkov, morajo upoštevati načelo, da je treba hraniti le nujen minimum podatkov glede na tveganje ali grožnjo ter za omejen čas, ki bo odvisen od narave shranjene informacije. Vsekakor iz hrambe ne sme biti razvidna natančna slika o zasebnem življenju, navadah, ravnanju ali socialnih odnosih zadevnih oseb.

b) Pogoji dostopa javnih organov do shranjenih podatkov

128. Menim, da so pogoji, navedeni v sodbi Tele2 Sverige in Watson,[88] še vedno pomembni tudi za dostop: z nacionalno ureditvijo morajo biti določene vsebinske in postopkovne zahteve, ki urejajo dostop pristojnih organov do hranjenih podatkov.[89]

129. Belgijska vlada navaja, da člen 126(2) zakona iz leta 2005 (o elektronskih komunikacijah)[90] natančno določa nacionalne organe, ki lahko pridobijo shranjene podatke v skladu z odstavkom 1 istega člena.

130. Med temi organi so sami pravosodni organi in državno tožilstvo, varnostne sile države; splošna obveščevalna in varnostna služba pod nadzorom posameznih neodvisnih komisij; uradniki kriminalistične policije belgijskega inštituta za poštne in telekomunikacijske storitve; urgentne službe; uradniki kriminalistične policije oddelka zvezne policije za pogrešane osebe; služba za mediacijo za telekomunikacije in organ za nadzor finančnega sektorja.

131. Na splošno belgijska vlada trdi, da nacionalna zakonodaja ne omogoča, da bi različne službe imele dostop do podatkov za dejavno preganjanje neopredeljenih groženj ali brez konkretnih indicev. Nacionalni organi naj torej ne bi mogli dostopati do neobdelanih komunikacijskih podatkov kar tako in jih samodejno obdelovati zaradi pridobivanja informacij in aktivnega preprečevanja groženj varnosti.

132. Po mnenju te vlade je dostop do podatkov predmet strogih pogojev glede na poslovnik vsakega od pristojnih nacionalnih organov.

88 Glej točko 60 teh sklepnih predlogov.

89 Sodba Tele2 Sverige in Watson, točka 118.

90 Člen 126, kakor je bil spremenjen z zakonom z dne 29. maja 2016.

133. Odgovor na prvo vprašanje za predhodno odločanje po mojem mnenju od Sodišča ne zahteva izčrpne analize pogojev, ki veljajo za vsakega od teh organov, da lahko pridobi shranjene podatke. To je bolj naloga predložitvenega sodišča, ki mora tako analizo izvesti glede na smernice iz sodne prakse Tele2 Sverige in Watson ter Ministerio Fiscal.

134. Glede na podatke, ki jih je predložila belgijska vlada, obstajajo poleg tega opazne razlike med pogoji za dostop, ki se nanašajo na pravosodne organe ali državno tožilstvo,[91] z namenom preiskovanja, odkrivanja in preganjanja kaznivih dejanj v skladu s členoma 46a[92] in 88a[93] zakonika o kazenskem postopku, in tistimi, ki veljajo za druge organe.

135. Glede obveščevalnih in varnostnih služb zakon iz leta 1998 določa, da mora zahteva za dostop do podatkov o prometu in lokaciji, ki jih imajo operaterji, temeljiti na objektivnih merilih zaradi zagotavljanja, da se omeji na to, kar je nujno potrebno na podlagi vnaprej opredeljene grožnje.[94] Določeni so različni roki za dostop (šest, devet ali dvanajst mesecev) glede na potencialno grožnjo, zahteva pa mora upoštevati načeli sorazmernosti in subsidiarnosti. Prav tako je bil uveden mehanizem nadzora s strani neodvisnega organa.[95]

136. Uradniki kriminalistične policije belgijskega inštituta za poštne in telekomunikacijske storitve (BIPT) lahko dostopajo do podatkov, ki jih imajo telekomunikacijski operaterji pod nadzorom državnega tožilstva v konkretnih zelo omejenih primerih,[96] ne da bi njihova dejavnost po mnenju belgijske vlade zajemala osebe, katerih podatki se hranijo.

137. Urgentne službe, ki zagotavljajo pomoč na kraju samem, lahko zahtevajo podatke o tistem, ki je opravil nujni klic, če po prejemu klica od ponudnika ali operaterja ne dobijo podatkov za identifikacijo navedene osebe oziroma dobijo nepopolne ali nepravilne podatke.

138. Agenti kriminalistične policije, ki so dodeljeni oddelku zvezne policije za pogrešane osebe, lahko od operaterja zahtevajo podatke, ki so potrebni za iskanje pogrešane osebe, katere telesna celovitost je v neposredni nevarnosti. Dostop, ki je predmet strogih pogojev, je omejen na podatke, ki omogočajo identifikacijo uporabnika in podatke v zvezi z dostopom in povezavo terminalske opreme z omrežjem ter storitvijo in o lokaciji te opreme in ki so bili shranjeni 48 ur pred zahtevo.

91 O upravičenosti državnega tožilstva, da sprejme tovrstne ukrepe, se razpravlja v predlogu za sprejetje predhodne odločbe C-746/18, HK/Prokuratur, v zvezi s katerim postopek še teče.

92 Državno tožilstvo je pristojno, da od operaterjev zahteva podatke o identifikaciji z obrazloženo in pisno (v nujnih primerih ustno) odločbo, ki izkazuje sorazmernost ukrepa v zvezi s spoštovanjem zasebnega življenja in njegovo subsidiarnost s katero koli drugo obveznostjo preiskovanja. Za kazniva dejanja, ki se ne kaznujejo z glavno kaznijo zapora v višini enega leta ali s hujšo kaznijo, lahko državno tožilstvo prosi za podatke v obdobju šestih mesecev pred izdajo odločbe.

93 Preiskovalni sodnik je pristojen, da od operaterjev zahteva sledenje elektronskim komunikacijam ali shranjenim podatkom o prometu in lokaciji, in lahko ta ukrep odredi, če obstajajo resni znaki storitve kaznivega dejanja, ki se kaznuje z določenimi kaznimi, z obrazloženim in pisnim (v nujnem primeru ustnim) sklepom, za katerega veljajo iste zahteve po sorazmernosti in subsidiarnosti kot za državno tožilstvo. Obstajajo nekatere izjeme, če je ukrep naslovljen na nekatere zaščitene kategorije poklicev (na primer na odvetnike ali zdravnike).

94 V odločbi se navedejo, odvisno od primera, fizične ali pravne osebe, združenja ali skupine, predmeti, kraji, dogodki ali informacije, za katere se posebna metoda uporabi. Prav tako mora biti navedeno razmerje med namenom zahtevanih podatkov in potencialno grožnjo, ki posebej utemeljuje to metodo.

95 Upravna komisija za nadzor nad posebnimi in izjemnimi metodami zbiranja podatkov s strani obveščevalnih in varnostnih služb (komisija BIM) in stalni odbor za nadzor nad obveščevalnimi službami (odbor R). Belgijska vlada je izjavila, da je komisija BIM odgovorna za spremljanje metod iskanja, ki jih uporabljajo obveščevalne in varnostne službe, nad katerimi izvaja nadzor na prvi stopnji. Ta komisija, sestavljena iz sodnikov, izvaja svoje naloge popolnoma neodvisno. Prav tako je organiziran neodvisen nadzor na drugi stopnji, in sicer ga izvaja odbor R.

96 To se dovoli za odkrivanje, preiskovanje in preganjanje kršitev iz členov 114 (varnost omrežij), 124 (zaupnost elektronskih sporočil) in 126 (hramba podatkov in dostop) iz zakona z dne 13. junija 2005 o elektronskih komunikacijah.

139. Služba za mediacijo za telekomunikacije lahko zahteva podatke o identifikaciji osebe, ki je zlorabila omrežje ali storitev elektronskih komunikacij. V tem primeru ne obstaja predhodni nadzor pravosodnega organa ali neodvisnega upravnega organa (ki se razlikuje od same službe).

140. Nazadnje, z namenom boja proti finančnemu kriminalu organ za nadzor finančnega sektorja lahko dostopa do podatkov o prometu ali lokaciji na podlagi predhodnega dovoljenja preiskovalnega sodnika.

141. Osvetlitev teh oblik in pogojev za dostop do shranjenih podatkov, ki veljajo za vsakega od organov, ki imajo dovoljenje za pridobitev teh podatkov, kaže na različnost primerov in zaščitnih ukrepov, katerih podrobno usklajenost z merili, ki jih uporablja Sodišče v svoji sodni praksi,[97] presoja predložitveno sodišče.

142. Opažam na primer, da iz sporne zakonodaje ne izhaja, da imajo pristojni nacionalni organi sistematično dolžnost zadevne osebe (razen če ta informacija ogroža preiskavo v teku) obvestiti, da so vpogledali v njihove podatke. Prav tako se ne zdi, da se vsaj v nekaterih primerih, kot so tisti v zvezi s finančnimi kaznivimi ravnanji, vnaprej določijo pravila o teži teh dejanj, da se utemelji dostop do ustreznih podatkov. Povezava med intenzivnostjo posega in težo preiskovanega kaznivega dejanja v smislu sodbe Ministerio Fiscal ni jasna v vseh primerih.

143. Kakor koli že, menim, da se premisleki v zvezi z dostopom organov do podatkov umaknejo v ozadje, če je zaradi že pojasnjenega sama splošna in neselektivna hramba teh podatkov glavni razlog, zaradi katerega nacionalna zakonodaja, na katero se nanaša ta predlog za sprejetje predhodne odločbe, ni v skladu s pravom Unije.

4. Tretje vprašanje za predhodno odločanje

144. Cour constitutionnelle (ustavno sodišče) želi izvedeti, ali bi se lahko, če se glede na odgovor Sodišča razglasi, da nacionalna zakonodaja ni v skladu s pravom Unije, začasno ohranili učinki navedene zakonodaje. S tem bi se preprečila pravna negotovost in bi se omogočilo, da bi se zbrani in shranjeni podatki lahko še naprej uporabljali za uresničevane cilje.

145. Ustaljena sodna praksa je, da „lahko le Sodišče izjemoma in iz nujnih razlogov pravne varnosti prizna začasno odložitev učinka izrinjenja, ki ga ima pravilo prava Unije v razmerju do nacionalnega prava, ki je v nasprotju z njim“. Če „bi imela nacionalna sodišča možnost, da nacionalnim določbam priznajo – pa čeprav le začasno – prednost pred pravom Unije, s katerim so v nasprotju, bi bila namreč ogrožena enotna uporaba prava Unije“.[98]

146. Komisija meni, da ker Sodišče ni omejilo časovnih učinkov razlage člena 15(1) Direktive 2002/58, bi bilo treba na to vprašanje predložitvenega sodišča odgovoriti nikalno.[99]

97 Napotujem na točko 60 teh sklepnih predlogov.

98 Sodba z dne 28. julija 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603, točka 33).

99 Točka 100 pisnega stališča Komisije.

147. Kljub temu je Sodišče v sodbi z dne 28. februarja 2012, Inter-Environnement Wallonie in Terre wallonne [100], odločilo, da se lahko nacionalnemu sodišču glede na obstoj nujne skrbi, povezane z varstvom okolja, izjemoma dovoli uporaba nacionalne določbe, ki mu dopušča, da ohrani nekatere učinke nacionalnega akta, ki je bil razglašen za ničnega zaradi kršitve predpisa Unije. [101]

148. Ta smer sodne prakse je bila potrjena s sodbo z dne 29. julija 2019, Inter-Environnement Wallonie in Bond Beter Leefmilieu Vlaanderen [102]. Čeprav je bila izdana na področju varstva okolja in je temeljila na zanesljivosti oskrbe z električno energijo, ne vidim razlogov, da bi zavrnil njeno uporabo na drugih področjih prava Unije, zlasti na tem, ki ga tu obravnavam.

149. Če „obstoj nujne skrbi, povezane z varstvom okolja“, lahko utemelji, da nacionalna sodišča izjemoma ohranijo nekatere učinke nacionalne določbe, ki ni skladna s pravom Unije, je to zato, ker je varstvo okolja „eden od bistvenih ciljev Unije in je tako razsežen kot tudi temeljen“. [103]

150. Torej se med cilje Unije prišteva tudi vzpostavitev območja varnosti (člen 3 PEU), ki vključuje spoštovanje temeljnih državnih funkcij, zlasti tistih, katerih cilj je vzdrževanje javnega reda in varovanje nacionalne varnosti (člen 4(2) PEU). Gre za cilj, ki ni nič manj „razsežen in temeljen“ kot varstvo okolja, saj je njegovo uresničevanje nujni pogoj za vzpostavitev normativnega okvira, ki lahko zagotavlja učinkovito uresničevanje pravic in temeljnih svoboščin.

151. Menim, da bi lahko nujni razlogi, povezani z zagotavljanjem nacionalne varnosti, v tej zadevi utemeljili, da Sodišče izjemoma dovoli predložitvenemu sodišču ohraniti vsaj nekatere učinke spornega zakona.

152. Ta ohranitev bi od predložitvenega sodišča zahtevala, da glede na odločitev Sodišča šteje nacionalni predpis za neskladen s pravom Unije in razglasi, da bi bile posledice, ki bi jih lahko imela njegova takojšnja razveljavitev (če bi bila razveljavitev po nacionalnem pravu posledica take neskladnosti) ali neuporaba za javno varnost ali varnost države, skrajno moteče.

153. Za začasno ohranitev (vseh ali dela) učinkov nacionalnega predpisa bi se poleg tega zahtevalo, da:

– bi bil namen tega podaljšanja preprečevanje pravne praznine v zvezi z učinki, ki so tako nevarni kot tisti, ki izhajajo iz uporabe sporne zakonodaje, kar je praznina, ki jo je nemogoče zapolniti z drugimi sredstvi in ki bi pomenila, da se nacionalnim organom odvzame dragocen instrument za zagotavljanje varnosti države; in

– bi navedena ohranitev učinkov trajala samo toliko, kolikor je nujno potrebno za sprejetje ukrepov, s katerimi bi bilo mogoče odpraviti neskladnost s pravom Unije, na katero je bilo opozorjeno. [104]

100 Zadeva C-41/11, EU:C:2012:103.

101 Sodba z dne 28. februarja 2012, Inter-Environnement Wallonie in Terre wallonne (C-41/11, EU:C:2012:103, točka 58). V sodbi z dne 28. julija 2016, Association France Nature Environnement (C-379/15, EU:C:2016:603, točka 34), je Sodišče iz te trditve sklepalo, da „je Sodišče nameravalo v vsakem primeru posebej in izjemoma nacionalnemu sodišču priznati možnost, da prilagodi učinke razglasitve ničnosti nacionalne določbe, za katero je bilo ugotovljeno, da ni v skladu s pravom Unije“.

102 Zadeva C-411/17 (EU:C:2019:622, točka 178).

103 Sodba z dne 28. februarja 2012, Inter-Environnement Wallonie in Terre wallonne (C-41/11, EU:C:2012:103, točka 57).

104 Sodba z dne 28. februarja 2012, Inter-Environnement Wallonie in Terre wallonne (C-41/11, EU:C:2012:103, točka 62).

154. V prid te rešitve sta poleg tega težavnost uskladitve nacionalnih zakonodaj s sodno prakso, določeno v zadevi Tele2 Sverige in Watson,[105] in to, da je volja belgijskega zakonodajalca uskladiti se s sodbo Digital Rights postala očitna s spremembo njegove zakonodaje. Iz tega precedensa je mogoče sklepati, da bo prav tako prilagodil zakon z dne 29. maja 2016 (ki je bil sprejet, preden se je seznanil s sodbo Tele2 Sverige in Watson) s sodno prakso, sprejeto v tej zadnji sodbi.

V. Predlog

155. Glede na vse zgoraj predstavljeno Sodišču predlagam, naj Cour constitutionnelle (ustavno sodišče, Belgija) odgovori:

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

   – nasprotuje nacionalni zakonodaji, ki operaterjem in ponudnikom elektronskih komunikacijskih storitev nalaga obveznost, da splošno in neselektivno hranijo podatke vseh naročnikov in uporabnikov o prometu in lokaciji glede vseh elektronskih komunikacijskih sredstev;

   – zgoraj navedenega ne ovira to, da cilji te nacionalne zakonodaje niso le preiskovanje, odkrivanje in pregon kaznivih dejanj, bodisi hudih ali manj hudih, temveč tudi zagotavljanje državne varnosti, obrambe in javne varnosti, preprečevanje prepovedane uporabe elektronskih komunikacijskih sistemov ali kateri koli drug cilj, določen v členu 23(1) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov);

   – zgoraj navedenega ne ovira niti to, da je dostop do hranjenih podatkov predmet natančno določenih varovalk. Naloga predložitvenega sodišča je, da preveri, ali nacionalna zakonodaja, ki ureja pogoje za navedeni dostop s strani pristojnih organov, omejuje dostop na posebne primere, zaradi resnosti katerih je poseg nujen, ta dostop pogojuje s predhodnim nadzorom (razen v nujnih primerih) sodišča ali neodvisnega organa in predvideva, da so zadevne osebe obveščene o tem dostopu, če to obvestilo ne ogrozi dejanj navedenih organov.

2. Člena 4 in 6 Listine Evropske unije o temeljnih pravicah ne vplivata na razlago člena 15(1) Direktive 2002/58 v povezavi z ostalimi zgoraj omenjenimi členi navedene listine, tako da bi ta člena preprečevala ugotovitev neskladnosti nacionalne zakonodaje, kakršna se obravnava v sporu o glavni stvari, s pravom Unije.

3. Nacionalno sodišče lahko, če nacionalno pravo to dopušča, izjemoma in začasno ohrani učinke zakonodaje, kot je ta iz postopka v glavni stvari, čeprav bi bilo to nezdružljivo s pravom Unije, če to ohranitev upravičujejo nujni razlogi, povezani z grožnjami javni ali nacionalni varnosti, s katerimi se ne bi bilo mogoče spopasti z drugimi sredstvi in drugimi načini. Ta ohranitev lahko traja le toliko časa, kolikor je nujno potrebno za odpravo te nezdružljivosti s pravom Unije.

[105] Točka 45 pisnega stališča danske vlade.