Zadeva C-520/18

Povzetek predloga za sprejetje predhodne odločbe v skladu s členom 98(1) Poslovnika Sodišča

Datum vložitve:

2. avgust 2018

Predložitveno sodišče:

Cour constitutionnelle (Belgija)

Datum predložitvene odločbe:

19. julij 2018

Tožeče stranke:

Ordre des barreaux francophones et germanophone

Académie Fiscale ASBL

UA

Liga voor Mensenrechten ASBL

Ligue des Droits de l'Homme ASBL

VZ

WY

XX

Tožena stranka:

Conseil des ministres (svet ministrov, belgijska vlada)

DELOVNI DOKUMENT

I. Predmet postopka v glavni stvari

1 Ordre des barreaux francophones et germanophone (zbornica francosko govorečih in nemško govorečih odvetnikov; v nadaljevanju: OBFG), nepridobitna združenja Académie Fiscale, Liga voor Mensenrechten in Ligue des Droits de l'Homme ter nekatere fizične osebe so na Cour constitutionnelle de Belgique (ustavno sodišče,

Belgija, v nadaljevanju: predložitveno sodišče) vložile tožbe za razglasitev ničnosti loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (zakon z dne 29. maja 2016 o zbiranju in hrambi podatkov na področju elektronskih komunikacij) (*Moniteur belge* z dne 18. julija 2016, str. 44717) (v nadaljevanju: izpodbijani zakon). Zadeve so bile združene.

2 Z izpodbijanim zakonom se spreminjajo različne določbe loi du 13 juin 2005 relative aux communications électroniques (zakon z dne 13. junija 2005 o elektronskih komunikacijah) (*Moniteur belge* z dne 20. junija 2005, str. 28070) (v nadaljevanju: zakon z dne 13. junija 2005), code d'instruction criminelle (zakonik o kazenskem postopku, v nadaljevanju: zakonik o kazenskem postopku) in loi du 30 novembre 1998 organique des services de renseignement et de sécurité (sistemski zakon z dne 30. novembra 1998 o obveščevalnih in varnostnih službah) (*Moniteur belge* z dne 18. decembra 1998, str. 40312) (v nadaljevanju: zakon z dne 30. novembra 1998).

3 Kraljevina Belgija je z loi du 30 juillet 2013, portant modification des articles 2, 126, et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle (zakon z dne 30. julija 2013 o spremembi členov 2, 126 in 145 zakona z dne 13. junija 2005 o elektronskih komunikacijah in člena 90i zakonika o kazenskem postopku) (*Moniteur belge* z dne 23. avgusta 2013, str. 56109) (v nadaljevanju: zakon z dne 30. julija 2013) v belgijsko pravo deloma prenesla Direktivo 2006/24/ES 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) in 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 (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514) (Direktiva o zasebnosti in elektronskih komunikacijah).

4 Sodišče je s sodbo z dne 8. aprila 2014, Digital Rights Ireland in drugi (C-293/12 in C-594/12, EU:C:2014:238) (v nadaljevanju: sodba Digital Rights Ireland in drugi) ugotovilo, da je direktiva 2006/24 neveljavna.

5 Predložitveno sodišče je s sodbo št. 84/2015 z dne 11. junija 2015 razglasilo ničnost člena 126 zakona z dne 13. junija 2005, kakor je bil spremenjen z zakonom z dne 30. julija 2013, zaradi enakih razlogov, kot so bili tisti, zaradi katerih je Sodišče ugotovilo, da je Direktiva 2006/24 neveljavna.

6 Belgijski zakonodajalec se je na to razglasitev ničnosti odzval z izpodbijanim zakonom.

DELOVNI DOKUMENT

II. Predmet in pravna podlaga predloga za sprejetje predhodne odločbe

7 Z izpodbijanim zakonom se spreminja zakon z dne 13. junija 2005, s katerim je bilo v belgijsko pravo prenesenih več direktiv, med drugim Direktiva 200[2]/58.

III. Pravni okvir vprašanj za predhodno odločanje

1. Pravo Evropske unije

A. Pogodba EU

8 Člen 5(4) PEU določa:

„V skladu z načelom sorazmernosti ukrepi Unije vsebinsko in formalno ne presegajo tistega, kar je potrebno za doseganje ciljev Pogodb.

Institucije Unije uporabljajo načelo sorazmernosti v skladu s Protokolom o uporabi načel subsidiarnosti in sorazmernosti.“

9 Člen 6 PEU določa:

„1. Unija priznava pravice, svoboščine in načela iz Listine Evropske unije o temeljnih pravicah z dne 7. decembra 2000, prilagojene 12. decembra 2007 v Strasbourgu, ki ima enako pravno veljavnost kot Pogodbi.

Z določbami Listine se na nikakršen način ne širijo pristojnosti Unije, opredeljene v Pogodbah.

Pravice, svoboščine in načela Listine se razlagajo v skladu s splošnimi določbami naslova VII Listine o njeni razlagi in uporabi ter ob ustreznem upoštevanju pojasnil iz Listine, ki navajajo vire teh določb.

2. Unija pristopi k Evropski konvenciji o varstvu človekovih pravic in temeljnih svoboščin. Ta pristop ne spreminja pristojnosti Unije, opredeljene v Pogodbah. […]“

B. Listina Evropske unije o temeljnih pravicah

10 Člen 4 Listine določa:

„Prepoved mučenja in nečloveškega ali ponižujočega ravnanja ali kaznovanja

Nihče ne sme biti podvržen mučenju ali nečloveškemu ali ponižujočemu ravnanju ali kaznovanju.“

11 Člen 6 Listine določa:

DELOVNI DOKUMENT

„Pravica do svobode in varnosti

Vsakdo ima pravico do svobode in varnosti.“

12 Člen 7 Listine določa:

„Spoštovanje zasebnega in družinskega življenja

Vsakdo ima pravico do spoštovanja svojega zasebnega in družinskega življenja, stanovanja ter komunikacij.“

13 Člen 8 Listine določa:

„Varstvo osebnih podatkov

1. Vsakdo ima pravico do varstva osebnih podatkov, ki se nanj nanašajo.

2. Osebni podatki se morajo obdelovati pošteno, za določene namene in na podlagi privolitve prizadete osebe ali na drugi legitimni podlagi, določeni z zakonom. Vsakdo ima pravico dostopa do podatkov, zbranih o njem, in pravico zahtevati, da se ti podatki popravijo.

3. Spoštovanje teh pravil nadzira neodvisen organ.“

14 Člen 11 Listine določa:

„Svoboda izražanja in obveščanja

1. Vsakdo ima pravico do svobodnega izražanja. Ta pravica vključuje svobodo mnenja ter sprejemanja in širjenja vesti ali idej brez vmešavanja javnih organov in ne glede na državne meje.

2. Spoštujeta se svoboda in pluralnost medijev.“

15 Člen 47 Listine določa:

„Pravica do učinkovitega pravnega sredstva in nepristranskega sodišča

Vsakdo, ki so mu kršene pravice in svoboščine, zagotovljene s pravom Unije, ima pravico do učinkovitega pravnega sredstva pred sodiščem v skladu s pogoji, določenimi v tem členu.

Vsakdo ima pravico, da o njegovi zadevi pravično, javno in v razumnem roku odloča neodvisno, nepristransko in z zakonom predhodno ustanovljeno sodišče. Vsakdo ima možnost svetovanja, obrambe in zastopanja.

Osebam, ki nimajo zadostnih sredstev, se odobri pravna pomoč, kolikor je ta potrebna za učinkovito zagotovitev dostopa do sodnega varstva.“

16 Člen 52 Listine določa:

DELOVNI DOKUMENT

„Obseg pravic in načel ter njihova razlaga

1. Kakršno koli omejevanje uresničevanja pravic in svoboščin, ki jih priznava ta listina, mora biti predpisano z zakonom in spoštovati bistveno vsebino teh pravic in svoboščin. Ob upoštevanju načela sorazmernosti so omejitve dovoljene samo, če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih. […]“

C. Direktiva 2002/58

17 Člen 15(1) Direktive 2002/58 določa:

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

Uredba (EU) 2016/679

18 Člen 95 Uredbe 2016/679 določa:

„Razmerje z Direktivo 2002/58/ES

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

2. Nacionalno pravo

19 Najbolj pomembne določbe upoštevne nacionalne zakonodaje, kakor so bile spremenjene z izpodbijanim zakonom, so:

A. Zakon z dne 13. junija 2005 o elektronskih komunikacijah

20 Zakon z dne 13. junija 2005, kakor je bil spremenjen z izpodbijanim zakonom, določa:

„[…]

DELOVNI DOKUMENT

Člen 126

„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, elektronsko pošto prek interneta, operaterji, ki ponujajo javna omrežja elektronskih komunikacij, in 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 zakonika o kazenskem postopku, pod pogoji, navedenimi v teh členih;

(2) obveščevalne in varnostne službe za namene opravljanja obveščevalne dejavnosti pri uporabi metod zbiranja podatkov iz členov 16/2, 18/7 in 18/8 [zakona z dne 30. novembra 1998] […];

(3) kriminalisti Institut [belge des services postaux et des télécommunications (belgijski institut 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 mestu, 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 nudijo pomoč osebi, ki je v nevarnosti, 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 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.

DELOVNI DOKUMENT

(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 in 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 ter o storitvi in 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 praovosodje in ministra [pristojnega za elektronske komunikacije] na podlagi mnenja Commission de la protection de la vie privée (komisija za varstvo zasebnega življenja) in Instituta določi podatke, ki jih je treba hraniti, po kategorijah, naštetih v prvem do 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 jih zaščiti 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);

DELOVNI DOKUMENT

(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 s pomočjo dnevnika. 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 in nadzorom nad vsebino tega dnevnika.

[…]

Člen 126/1

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 z dne 30. novembra 1998].

[…].

Zahteve organov, ki se nanašajo na podatke iz prvega pododstavka, lahko obravnavajo le člani oddelka za koordinacijo. Če je to nujno potrebno, si lahko zagotovijo tehnično pomoč uslužbenca operaterja ali ponudnika, ki deluje pod njihovim nadzorom.

Člane oddelka za koordinacijo in uslužbence, ki zagotavljajo tehnično pomoč, veže dolžnost varovanja poklicne skrivnosti.

Operaterji in ponudniki iz člena 126(1), prvi pododstavek, varujejo zaupnost podatkov, ki jih obdeluje oddelek za koordinacijo ter Institutu in komisiji za varstvo zasebnega življenja takoj posredujejo kontaktne podatke oddelka za koordinacijo in njegovih članov ter vsako spremembo teh podatkov.

2. Operaterji in ponudniki iz člena 126(1), prvi pododstavek, določijo notranji postopek, ki omogoča, da odgovarjajo na zahteve organov za dostop

DELOVNI DOKUMENT

do osebnih podatkov v zvezi z uporabniki. Institutu morajo na njegovo zahtevo predložiti informacije o teh postopkih, o številu prejetih zahtev, o navedeni pravni podlagi in 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.

Ta pooblaščena oseba ne sme biti član oddelka za koordinacijo.

[…]

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.

Pooblaščena oseba zaradi opravljanja svojih nalog ne sme biti v slabšem položaju. Zlasti je brez temeljite obrazložitve zaradi opravljanja njej zaupanih nalog ni mogoče odpovedati pogodbe o zaposlitvi ali je nadomestiti.

Pooblaščena oseba mora imeti možnost neposredne komunikacije z upravo operaterja ali ponudnika.

Pooblaščena oseba za varstvo osebnih podatkov zagotavlja:

(1) da oddelek za koordinacijo obdeluje podatke v skladu z zakonom;

(2) da ponudnik ali operater zbira in hrani le tiste podatke, ki jih lahko zakonito hrani;

(3) da imajo dostop do hranjenih podatkov le organi, ki so za to pooblaščeni z zakonom;

(4) da se izvajajo ukrepi za varstvo in zaščito osebnih podatkov iz tega zakona in iz varnostne politike ponudnika ali operaterja;

Operaterji in ponudniki iz člena 126(1), prvi pododstavek, Institutu in komisiji za varstvo zasebnega življenja takoj posredujejo kontaktne podatke pooblaščenih oseb za varstvo osebnih podatkov ter vsako spremembo teh podatkov.

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

[…]

DELOVNI DOKUMENT

(1) 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 Institutu 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.

Člen 127:

1. Kralj na podlagi mnenja komisije za varstvo zasebnega življenja in Instituta določi tehnične in upravne ukrepe, ki jih morajo izpolnjevati operaterji in ponudniki iz člena 126(1), prvi pododstavek, in končni uporabniki, da bi se zagotovilo:

(1) identifikacijo klicne linije v primeru nujnega klica;

(2) identifikacijo končnega uporabnika, izsledite v, določitev lokacije, poslušanje, vpogled v zasebne komunikacije in njihovo snemanje pod pogoji iz členov 46a, 88a in od 90b do 90i zakonika o kazenskem postopku in [zakona z dne 30. novembra 1998].

[…]

2. Prepovedana sta ponujanje ali uporaba storitev ali opreme, ki oteži ali onemogoči izvajanje ukrepov iz odstavka 1, razen sistemov šifriranja, ki se lahko uporabljajo za zagotavljanje zaupnosti komunikacij in varnosti plačil.

[…]

Člen 145

1. Oseba, ki krši člene […] 126, 126/1 in 127 ter odloke za izvajanje členov […] 126, 126/1 in 127 se kaznuje z globo od 50 do 50.000 EUR.

[…]“.

B. Zakonik o kazenskem postopku

21 Zakonik o kazenskem postopku, kakor je bil spremenjen z izpodbijanim zakonom, določa:

DELOVNI DOKUMENT

„[…]

Člen 46a

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 določena oseba naročena ali ki jih določena 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. Lriminalist 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 šest 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.

Člen 88a

DELOVNI DOKUMENT

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 katerega 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 z dne 13. junija 2005 o elektronskih komunikacijah, se uporabljajo te določbe:

- za kaznivo dejanje iz knjige II, naslov Ib, Code pénal (kazenski zakonik) lahko preiskovalni sodnik z odredbo zahteva predložitev podatkov za obdobje 12 mesecev pred izdajo odredbe;

- za drugo kaznivo dejanje iz člena 90b, od (2) do (4), ki ni kaznivo dejanje iz prve alinee, ali za kaznivo dejanje, ki je storjeno v okviru hudodelske združbe iz člena 324 kazenskega zakonika ali za kaznivo dejanje, ki se kaznuje 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.

DELOVNI DOKUMENT

- za druga kazniva dejanja lahko preiskovalni sodnik zahteva predložitev podatkov le za obdobje šest mesecev pred izdajo odredbe.

3. Ukrep se lahko na elektronska komunikacijska sredstva odvetnika in 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. […] 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.

[…]“

C. Zakon z dne 30. novembra 1998

22 Zakon z dne 30. novembra 1998, kakor je bil spremenjen z izpodbijanim zakonom, določa:

„[…]

Člen 13

Obveščevalne in varnostne službe lahko iščejo, zbirajo, prejemajo in obdelujejo informacije in osebne podatke, ki bi lahko bili koristni pri opravljanju njihovih nalog in 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 in na informacije in osebne podatke, 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. […]

Člen 18/3

DELOVNI DOKUMENT

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 težo 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 (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. […]

Člen 18/8

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:

DELOVNI DOKUMENT

(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 za podatke, ki se hranijo na podlagi člena 126 zakona z dne 13. junija 2005 o elektronskih komunikacijah, se 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 šest mesecev pred sprejetjem odredbe;

(2) za potencialno nevarnost, ki ni zajeta z (1) in (3), lahko vodja službe v odredbi zahteva posredovanje podatkov za obdobje devet 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. […]“.

IV. Druge določbe in načela, na katera so se sklicevale stranke ali so bile navedene v obrazložitvi odločbe predložitvenega sodišča

23 Poleg zgoraj navedenih določb so upoštevne tudi druge določbe in načela, na katera so se sklicevale stranke ali so navedene v obrazložitvi odločbe predložitvenega sodišča:

– členi 5, 6, 8, 9, 10, 11, 14, 15, 17 in 18 Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin, podpisane v Rimu 4. novembra 1950 (v nadaljevanju: EKČP);

– člen 17 Mednarodnega pakta o državljanskih in političnih pravicah, podpisan v New Yorku 16. decembra 1966 (v nadaljevanju: Pakt);

– člen 2(a) in člen 13(1) Direktive Evropskega parlamenta in Sveta 95/46/ES 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);

– členi 10, 11, 12, 15, 19, 22, 29, 151(1), prvi pododstavek, Constitution belge (belgijska ustava);

DELOVNI DOKUMENT

– splošna načela pravne varnosti, sorazmernosti, zakonitosti v kazenskem pravu, razumnosti, domneve nedolžnosti, pravice do poštenega sojenja, varovanja poklicne skrivnosti, enakosti med državljani in informacijskega samoodločanja.

VI. Bistvene trditve strank

1. Tožbeni razlogi tožečih strank

24 Tožeče stranke se sklicujejo na kršitev več členov ustave, v povezavi ali brez nje z več členi Pogodbe EU, Listine, Direktive 2002/58 in drugimi določbami prava Unije, z drugimi določbami EKČP, členom 17 Pakta in s splošnimi pravnimi načeli.

25 Izpodbijani zakon operaterjem elektronskih komunikacij nalaga splošno obveznost, da morajo določeno obdobje hraniti podatke o prometu in lokaciji uporabnikov. Z izpodbijanim zakonom se vzpostavlja tudi pravni okvir za dostop pravosodnih organov ter obveščevalnih in varnostnih služb do teh podatkov.

– *Obveznost zbiranja in hrambe*

26 Tožeče stranke izpodbijanemu zakonu očitajo, da brez utemeljitve enako obravnava uporabnike telekomunikacijskih storitev in storitev elektronskih komunikacij, za katere velja poklicna skrivnost, med drugim odvetnike, in druge uporabnike teh storitev, ne da bi se upoštevali poseben položaj odvetnikov, bistven pomen poklicne skrivnosti, ki zanje velja, in nujna zaupnost odnosa med odvetnikom in njegovimi strankami, in tudi brez upoštevanja posebnega položaja računovodij in davčnih svetovalcev, bistvenega pomena poklicne skrivnosti, ki zanje velja, in nujne zaupnosti med njimi in njihovimi strankami, pa nazadnje tudi brez upoštevanja obveznosti zaupnosti, ki velja za druge osebe, ki jih ne veže poklicna skrivnost v ožjem smislu.

27 Diskriminacija, ki se ustvarja z izpodbijanim zakonom je enako škodljiva za odvetnike kot za pravne subjekte, saj je poklicna skrivnost odvetnika v splošnem interesu. Vsi, ki se zaupajo odvetniku, morajo biti gotovi, da to posvetovanje in okoliščine v zvezi z njim ter skrivnosti, zaupane njihovemu zastopniku, ne bodo razkrite ter se jih ne bo uporabilo zoper njih. Načelo poklicne skrivnosti odvetnikov je neposredno povezano s pravico do poštenega sojenja in spoštovanja zasebnega življenja. V to načelo se sme posegati le v izjemnih primerih, pri čemer morajo biti zagotovljene primerne in zadostne varovalke proti zlorabi.

28 Tudi če se zbrani podatki ne nanašajo na vsebino komunikacij, omogočajo oblikovanje resnične digitalne osebne izkaznice zadevne osebe. Tako bo mogoče ugotoviti, ali je osumljenec kaznivega dejanja vzpostavil stik z odvetnikom, in izvedeti za datum, uro, trajanje komunikacije ter komunikacijsko sredstvo uporabnikov, kraj uporabe mobilne opreme in podobno. Ti podatki so celo bolj

DELOVNI DOKUMENT

podrobni kot podatki, zavedeni v službenem rokovniku odvetnika, ki pa je zaupen dokument.

29 Neobstoj razlikovanja med osebami, za katere velja poklicna skrivnost, in drugimi osebami je Sodišče grajalo v sodbi z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970) (v nadaljevanju: sodba Tele2 Sverige in Watson in drugi).

30 S tehničnega vidika bi bilo z vstopnim filtrom enostavno ločiti navadne metapodatke in tiste, ki se na nanašajo na osebe, za katere velja poklicna skrivnost. Zakonodajalec bi lahko operaterje prisilil, da med njihovimi strankami identificirajo osebe, za katere velja poklicna skrivnost, in da si te informacije izmenjajo. Tako operaterji metapodatkov, ki nastanejo ob komunikaciji odvetnikov in drugih oseb, za katere velja poklicna skrivnost, ne bi prenesli v baze podatkov, ki so jih vzpostavili.

31 Poleg tega ni določen noben mehanizem nadzora, ki bi osebi, za katero velja poklicna skrivnost, in upravičencem do nje omogočil, da nasprotujejo zbiranju, hrambi ali vpogledu v podatke, za katere velja poklicna skrivnost. Vpogled v te podatke, tudi če se predložijo šele kasneje za namene neke zadeve, zadostuje za kršitev poklicne skrivnosti. Pravice iz člena 6 EKČP in člena 47 Listine niso spoštovane, saj izpodbijani zakon ne določa nobenega sodnega nadzora.

32 Po drugi strani se z izpodbijanimi določbami enako obravnavajo pravni subjekti, zoper katere se uporabi preiskovalni ukrep ali ukrep pregona zaradi dejstev, zaradi katerih jih lahko doleti kazenska obsodba, in tisti, zoper katere se taki ukrepi niso uporabili. Kazensko pravo pa temelji na načelu nedolžnosti, iz katerega izhaja, da nosi dokazno breme državno tožilstvo in da ima v primeru dvoma od tega korist preganjana oseba. Zato se ni primerno sklicevati na dejstvo, da ima od ukrepa lahko korist tudi žrtev kaznivega dejanja. Tako so obveznosti hrambe, ki jih izpodbijani zakon nalaga, pretirane glede na cilje zakonodajalca.

33 Splošna hramba podatkov, vključno za osebe, ki nimajo nobene povezave s kaznivimi dejanji, torej krši načelo sorazmernosti. Da je to kršitev, potrjujejo sodbi Sodišča Digital Rights Ireland in drugi in Tele2 Sverige in Watson in drugi, sklepni predlogi generalnega pravobranilca Cruza Villalóna v združenih zadevah Digital Rights Ireland in drugi (C-293/12 in C-594/12, EU:C:2013:845) ter sodba predložitvenega sodišča št. 84/2015 z dne 11. junija 2015.

34 Obveznost splošne in neselektivne hrambe podatkov v zvezi z identifikacijo, dostopom in lokacijo ter podatki o osebni komunikaciji, ki je naložena z izpodbijanim zakonom, je tudi poseg v pravico do varstva zasebnega življenja, ki v demokratični družbi ni nujno potreben za zaščito nacionalne varnosti, to je državne varnosti, obrambe, javne varnosti, ali za zagotovitev preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj ali nepooblaščene uporabe elektronskega komunikacijskega sistema, kot to določa člen 13(1) Direktive 95/46.

DELOVNI DOKUMENT

35 V sodbi Tele2 Sverige in Watson in drugi je Sodišče potrdilo, da pravo Unije nasprotuje nacionalni ureditvi, ki določa splošno in neselektivno hrambo podatkov. Tudi če za tako splošno obveznost hrambe ne bi bilo mogoče šteti, da presega tisto, kar je nujno potrebno, pa mora biti opremljena z vsemi varovalkami, ki jih je Sodišče navedlo v sodbi Digital Rights Ireland in drugi in v sodbi Tele2 Sverige in Watson in drugi. Te varovalke so nujne, kumulativne in minimalne (sklepni predlogi generalnega pravobranilca Saugmandsgaarda Øeja v združenih zadevah Tele2 Sverige in drugi, C-203/15 in C-698/15, EU:C:2016:572).

36 Obveznost hrambe podatkov, ki jo določa izpodbijani zakon, v veliki meri ustreza obveznosti hrambe podatkov, ki je bila določena z Direktivo 2006/24, kot je Sodišče ugotovilo v točki 97 sodbe Tele2 Sverige in Watson in drugi.

37 Splošna obveznost hrambe podatkov, ki jo določa izpodbijani zakon, torej pomeni posebej resno kršitev pravice do spoštovanja zasebnega in družinskega življenja in pravice do varstva osebnih podatkov. Vpliva tudi na uporabo elektronskih komunikacijskih sredstev in torej na način, kako uporabniki teh komunikacijskih sredstev uporabljajo svojo svobodo izražanja. Iz tega izhajajo tudi kršitve mednarodnih in ustavnih določb, ki zagotavljajo to svobodo izražanja. Ob upoštevanju teže kršitve teh temeljnih pravic bi bil lahko ta ukrep upravičen le z razlogom boja proti hudemu kriminalu. Vendar pa zgolj z bojem proti hudemu kriminalu še ni mogoče upravičiti splošne in neselektivne hrambe vseh podatkov o prometu in podatkov o lokaciji (sodba Tele2 Sverige in Watson in drugi, točka 103). To bi namreč pomenilo, da hramba teh podatkov postane pravilo, medtem ko je v skladu z Direktivo 2002/58 pravilo prepoved hrambe teh podatkov, njihova hramba pa je izjema. Poleg tega se sodba Tele2 Sverige in Watson in drugi nanaša na vsako nacionalno ureditev boja proti kriminalu, ki določa splošno obveznost hrambe podatkov, in ne le na boj proti hudemu kriminalu. Čeprav je lahko s tako vrsto kriminala soočen vsak državljan, kot obdolženec, žrtev ali priča, zadevna ureditev spada na področje uporabe člena 15 Direktive 2002/58. Zato je treba zanjo uporabiti ugotovitve iz sodbe Tele2 Sverige in Watson in drugi.

38 V sodbi Tele2 Sverige in Watson in drugi je Sodišče pojasnilo, da je lahko nacionalna ureditev, ki preventivno dopušča ciljno hrambo podatkov o prometu in podatkov o lokaciji,z namenom boja proti hudemu kriminalu, dopustna le, če je to nujno potrebno pod pogoji, navedenimi v tej sodbi. Zakonodajalec v pripravljalnem gradivu trdi, da taka ciljna hramba podatkov ne bi bila mogoča. Razlogovanje État belge (država Belgija) dejansko temelji na politični volji, da se za vsako ceno nadaljuje s splošno hrambo podatkov, pod pretvezo tveganja, ki ga povzroča terorizem, in to kljub neustavnosti vzpostavljenega splošnega sistema nadzora. Tudi če bi se priznalo, da je dejansko nemogoče vnaprej določiti kategorije oseb, za katere ne obstaja verjetnost, da so udeležene v hudih kaznivih dejanjih ali da jih ta dejanja zadevajo, to ne bi moglo upravičiti tako resnega posega v zasebno življenje državljanov. Logični sklep bi moral biti, da se tak ukrep ne bi smel uvesti.

DELOVNI DOKUMENT

39 Nazadnje, čeprav se obrazložitev zakona sklicuje na pomen komunikacijskih podatkov za preiskavo terorizma, spolnih zlorab otrok, primerov v zvezi s pogrešanimi osebami, nezakonite trgovine z drogami, prodaje ponarejenih zdravil prek interneta, spodbujanja sovraštva ali nasilja, nadlegovanja, vdorov v bančne račune, in krajo identitete, iz več študij izhaja dvom o nujnosti splošne obveznosti hrambe z namenom boja proti hudemu kriminalu (sklepni predlogi generalnega pravobranilca Saugmandsgaarda Øeja v združenih zadevah Tele2 Sverige in drugi, C-203/15 in C-698/15, EU:C:2016:572).

40 Tožeče stranke podredno navajajo, da se lahko sodba Digital Rights Ireland in drugi razlaga na dva načina: po prvi razlagi je nezakonitost obveznosti splošne in neselektivne hrambe podatkov posledica neobstoja zadostnih varovalk v zvezi z dostopom do hranjenih podatkov in v zvezi z obdobjem hrambe, po drugi razlagi pa je hramba nezakonita ravno zato, ker je splošna in neselektivna. V obrazložitvi zakona se tudi priznava, da obveznost splošne in neselektivne hrambe podatkov ni v skladu s to sodbo, vendar se zastopa stališče, da je mogoče to izravnati z bolj strogo ureditvijo drugih vidikov, to je z razlikovanjem kategorij hranjenih podatkov in njihove uporabnosti, s pravili za dostop organov do teh podatkov in s pravili v zvezi z varnostjo teh podatkov pri operaterjih. Treba je torej ugotoviti, da obveznost splošne hrambe podatkov ne ustreza niti široki razlagi te sodbe, ker ni varovalk, s katerimi bi se poseg omejil na to, kar je nujno.

41 Operaterji sicer podatke že hranijo zaradi izstavljanja računov. Vendar pa jim izpodbijani zakon prepoveduje uporabo podatkov, ki se hranijo na podlagi tega zakona, za druge namene, kot so ti, ki so določeni v zakonu, vključno z zaračunavanjem njihovih storitev. Poleg tega jim sporni zakon nalaga, da hranijo elemente, ki jih sicer ne bi, ne v tej obliki, in vsekakor ne v istem časovnem obdobju.

42 Poleg tega obstaja nezanemarljivo tveganje, da bodo operaterji, ki so do kontrol, ki jih povzroča ta nova obveznost, zadržani, upoštevne zbirke podatkov vodili malomarno.

43 Noben neodvisen organ ne nadzoruje, ali operaterji spoštujejo raven zagotavljanja varnosti in zaščite hranjenih podatkov. Odgovorne osebe, ki jih v zvezi s tem določa izpodbijani zakon, so zaposleni pri operaterju in so v podrejenem položaju.

44 Izpodbijani zakon operaterjem tudi omogoča, da podatke, zbrane z namenom hrambe, posredujejo podizvajalcem v druge države članice Evropske unije, kljub občutljivosti in zaupnosti nekaterih podatkov, kar znatno poveča tveganje, da bodo do njih dostopale tretje osebe in da bodo razkriti. Poleg tega nacionalne ureditve, ki se uporabljajo v drugih državah članicah, na primer francoska zakonodaja, obveščevalnim službam omogočajo, da od operaterjev pridobijo informacije o podatkih, ki jih obdelujejo ti operaterji.

DELOVNI DOKUMENT

– *ii) Rok hrambe*

45 V zvezi z rokom hrambe izpodbijani zakon v bistvu določa obdobje 12 mesecev, ki je tako ali tako predolgo. Za kršitve, ki se ne kaznujejo z glavno kaznijo zapora v višini enega leta ali več, se sicer zahtevani podatki lahko nanašajo le na obdobje šestih mesecev pred vložitvijo zahteve. Vendar je takih kršitev le malo.

46 Začetek teka roka hrambe tudi ni povezan z okoliščinami, ki bi lahko upravičevale to hrambo. Poleg tega se lahko podatki za identifikacijo dejansko hranijo veliko daljše obdobje od 12 mesecev, ker začne rok hrambe teči „od dne, ko je komunikacija prek uporabljene storitve zadnjič mogoča“.

47 V drugih evropskih državah so določeni krajši roki hrambe. Treba je spomniti na sodbo nemškega ustavnega sodišča, ki je razveljavilo nemški zakon o hrambi podatkov in na sodbo Digital Rights Ireland in drugi.

48 Rok hrambe podatkov je mogoče grajati tudi zaradi tega, ker je enak za vse kategorije podatkov, moral pa bi se razlikovati glede na kategorije podatkov, njihovo uporabnost z vidika cilja, ki se želi doseči, ali zadevne osebe, ob tem da bi moral biti omejen na to, kar je nujno potrebno. To enako obravnavanje neenakih kategorij podatkov ni razumno upravičeno in je zato diskriminatorno.

49 Nazadnje, izpodbijani zakon od organa, ki je dostopal do podatkov, ne zahteva, da jih uniči, če nimajo nobene zveze z namenom, zaradi katerega so bili zbrani ali niso več nujno potrebni za boj proti hudemu kriminalu.

– *iii) Dostop do podatkov*

50 Izpodbijani zakon dostop do hranjenih podatkov omogoča šestim različnim organom, namesto da bi ta dostop strogo omejil na organe, ki so vključeni v boj proti kriminalu, ali vsaj hudemu kriminalu.

51 Izpodbijani zakon omogoča organom, da dostopajo do hranjenih podatkov, ne da bi bil ta dostop omejen na hud kriminal. Dodatne varovalke, ki so v izpodbijanem zakonu določene glede poklicne skrivnosti, se ne nanašajo na osebe, za katere velja poklicna skrivnost in niso odvetniki, zdravniki ali novinarji. Člen 458 kazenskega zakonika [določba, ki nalaga varovanje poklicne skrivnosti] pa se nanaša na več oseb od tistih, ki opravljajo te tri poklice. Poleg tega za nekatere osebe, organe in organizacije ne velja poklicna skrivnost, čeprav mora za komunikacijo z njimi na podlagi drugih določb kljub temu veljati neka zaupnost. Poleg tega kraljevi tožilec ni sodni organ ali neodvisen upravni organ.

52 Dalje, izpodbijani zakon obveščevalnim in varnostim službam omogoča dostop do hranjenih podatkov. Področje delovanja teh služb je opredeljeno preveč na široko. Zahtevajo se lahko podatki o komunikaciji vseh državljanov za obdobje šestih, devetih ali 12 mesecev pred odredbo o dostopu, glede na vrsto potencialne nevarnosti. Izpodbijani zakon lahko torej vodi do zlorabe pooblastil v škodo posameznikov ali organizacij, ki so kritični do vlade ali političnega sistema.

DELOVNI DOKUMENT

Ogrožena je tudi svoboda tiska, ker lahko obveščevalne in varnostne službe zahtevajo vse telefonske in internetne komunikacije novinarjev. Izpodbijani zakon lahko spodbudi ali okrepi samocenzuro pri državljanu, ki se mu dozdeva, da je nadzorovan, kar lahko vpliva na izvrševanje njegove svobode izražanja in obveščanja in lahko pomeni vmešavanje v smislu člena 11 Listine.

53 Ne obstaja noben jasen opis okoliščin ali pogojev za dodelitev dostopa. Za dostop tudi ne veljajo nobeni materialni ali procesni pogoji, ponudniki imajo preprosto dolžnost, da pozitivno odgovorijo na vsako zahtevo šestih imenovanih organov. Sodišče pa je v sodbi Tele2 Sverige in Watson in drugi potrdilo, da mora nacionalna ureditev določiti primerne varovalke, to je jasna in natančna pravila, ki določajo, v katerih okoliščinah in pod kakšnimi pogoji morajo ponudniki pristojnim nacionalnim organom omogočiti dostop do podatkov. V isti sodbi je pojasnjeno, da se lahko dostop načeloma odobri 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. Poleg tega mora pred dostopom sodišče ali neodvisen upravni organ opraviti predhoden nadzor. V izpodbijanem zakonu pa ni določeno nobeno postopkovno pravilo in tudi ni določen noben organ za presojo zahteve za posredovanje podatkov. Določen je le naknaden nadzor.

54 Po drugi strani se v sodbi Tele2 Sverige in Watson in drugi uporablja besedna zveza „resna nevarnost za javno varnost“. Izpodbijani zakon pa ne spoštuje tega merila, saj se nanaša na običajne in posebne metode obveščevalnih služb, ki se nanašajo na manj resne kršitve varnosti kot specialne metode.

55 Nazadnje, izpodbijani zakon ne določa nobene obveznosti opozarjanja oseb, da je bil odobren dostop do njihovih zasebnih podatkov, zaradi česar tudi nimajo pravice do učinkovitega in dejanskega pravnega sredstva.

56 V zvezi z rokom za dostop zakon določa le eno vrsto razlikovanja, v zvezi z vrsto kršitve in nevarnosti, ne pa tudi v zvezi z vrsto hranjenih podatkov.

2. Tožbeni razlogi État belge

57 Svet ministrov meni, da izpodbijani zakon upošteva očitke, ki sta jih navedli Sodišče in predložitveno sodišče v zvezi s prejšnjo upoštevno zakonodajo.

58 Poklicna skrivnost odvetnikov, čeprav spada med temeljna načela, ni absolutna. Načelo sorazmernosti „mora omogočiti presojo omejitev, ki izhajajo iz nujnosti ali drugih načel ali vrednot, ki so, odvisno od primera, v konfliktu s poklicno skrivnostjo“.

59 V zvezi z dostopom do podatkov izpodbijani zakon določa omejitve v zvezi s poklicno skrivnostjo, zlasti odvetnikov. Zakon se nanaša le na metapodatke, ne pa na vsebino komunikacij. Zato dejansko ne vpliva na zaupnost komunikacije med odvetnikom in njegovo stranko. Bilo pa bi nesorazmerno, če bi bila komunikacija

DELOVNI DOKUMENT

od in do nosilcev poklicev, za katere velja poklicna skrivnost, popolnoma izvzeta iz zakonskega urejanja. To, da nek naslov elektronske pošte uporablja nosilec poklicne skrivnosti, namreč ne pomeni, da so vsa sporočila, ki pridejo na ta naslov ali so iz njega poslana, dejansko varovana s poklicno skrivnostjo. Tudi nosilci poklicnih skrivnosti lahko storijo huda kazniva dejanja.

60 V zvezi s pravnimi subjekti, ki naj se ne bi več mogli zaupati svojemu odvetniku, je zakonodajalec sprejel vse preventivne ukrepe, da se cilj, ki se ga želi doseči in katerega zakonitosti se ne izpodbija, lahko doseže brez nesorazmernih posegov v pravico do zasebnega življenja in pravico do poštenega sojenja.

61 V zvezi s hrambo ali nehrambo podatkov glede na to, ali za zadevno osebo velja poklicna skrivnost ali ne, so bile v pripravljalnem gradivu k zakonu izpostavljene tehnične težave takih rešitev in dejstvo, da druge države članice Unije niso mogle najti tehnične formule za razlikovanje. Poleg tega tako razlikovanje ne bi varovalo poklicne skrivnosti same, ampak tistega, ki zaradi svojega poklica take skrivnosti izve. To razlikovanje bi učinkovalo tako, da bi s področja uporabe zakona izključilo ne le tisto, za kar velja poklicna skrivnost, temveč tudi to, kar z njo sploh ni povezano, z izgovorom, da zbrane informacije uporabljajo isti kanal kot informacije, za katere velja poklicna skrivnost.

62 V zvezi z neobstojem pravnega sredstva zoper odločbo, s katero se določa ukrep vpogleda v hranjene podatke, in zoper ukrepe, ki se sprejmejo na podlagi te odločbe, je treba navesti, da se sodni nadzor nad dostopom do hranjenih podatkov, v primeru da imajo dostop do informacij obveščevalne službe, dejansko izvaja v okviru kazenske preiskave, ki jo izvaja komisija BIM [upravna komisija, ki je zadolžena za nadzor nad posebnimi in izrednimi metodami zbiranja podatkov s strani obveščevalnih in varnostnih služb], ki je sestavljena iz neodvisnih sodnikov oz. državnih tožilcev. Kraljevi tožilec je prav tako neodvisen organ, ko v okviru zakonika o kazenskem postopku izvaja svoja preiskovalna pooblastila, in zagotavlja, da izvajanje njegovih pooblastil v pravico do varstva zasebnega življenja ne bo posegalo na nerazumen način.

63 V zvezi z rokom hrambe podatkov zakon pri dostopu določa postopnost, ki v bistvu temelji na teži kršitve. Obveznost hrambe je logični pogoj za dostop do hranjenih podatkov. Teža kršitve ali nevarnosti bo razvidna šele iz zahteve za dostop. Ker zakon določa, da je dostop do zadevnih podatkov odvisen od teže kršitve ali nevarnosti, je težko vnaprej opredeliti, po kategorijah informacij, kakšna bo korist neke informacije v posamični preiskavi. Nazadnje tožeča stranka ne navaja, zakaj naj bi bili tako določeni roki nesorazmerni.

64 Zakonodajalec je preučil vse možnosti za uskladitev s sodno prakso Sodišča. Različno obravnavanje glede na rok hrambe podatkov se je po poglobljeni preučitvi tega vprašanja izkazalo za nemogoče. Izkazalo se je, da je za boj proti terorističnim kaznivim dejanjem potreben rok 12 mesecev.

DELOVNI DOKUMENT

65 Glede neobstoja razlikovanja med pravnimi subjekti glede na to, ali se proti njim vodi preiskava ali se preganjajo ali ne, je treba ugotoviti, da izpodbijani zakon ravno preiskovalcem omogoča, da dostopajo do nekaterih metapodatkov v zvezi z osebo, proti kateri se vodi taka preiskava. To pomeni, da se morajo metapodatki hraniti pred preiskavo in torej v časovnem obdobju, v katerem razlikovanja še ni bilo mogoče opraviti.

66 V zvezi s tveganjem, da bodo operaterji malomarno obdelovali hranjene podatke, je treba ugotoviti, da regulator za to področje nadzoruje, ali operaterji spoštujejo zakonske obveznosti, pri čemer so v okviru tega nadzora določene sankcije, ki lahko v najtežjih primerih povzročijo odvzem dovoljenja za opravljanje dejavnosti. Izpodbijani zakon določa številne varovalke na področju ukrepov za zagotavljanje varnosti podatkov.

67 To, da se podatki, za katere velja poklicna skrivnost, hranijo in da se po potrebi do njih dostopa, je nujen element vsakega preventivnega sistema. Da bi se ugotovilo, ali za neko informacijo velja poklicna skrivnost, jo je treba najprej obdelati.

68 Cilj nacionalnih ureditev Švedske in Združenega kraljestva, ki jih je Sodišče preučilo v sodbi Tele2 Sverige in Watson in drugi, je bil boj proti hudemu kriminalu, medtem ko je cilj izpodbijanega zakona širši. Zato neprimernosti ali nesorazmernosti nacionalne zakonodaje glede na cilj boja proti hudemu kriminalu, ki ju je ugotovilo Sodišče, ni mogoče *mutatis mutandis* prenesti na nacionalno zakonodajo, ki ima drugačen cilj.

69 Sodišče je sicer presodilo, da ureditev, ki dopušča zbiranje, hrambo in dostop pristojnih nacionalnih organov do podatkov v zvezi z elektronskimi komunikacijami, ni v nasprotju s pravom Unije, če je ta ureditev ciljno usmerjena. Vendar pa je ta rešitev, ki jo je ponudilo Sodišče, teoretična. Sodišče namreč v tej sodbi ni preizkusilo skladnosti neke konkretne ureditve, ki bi bila tako ciljno usmerjena. O tem, da bi bil lahko tak sistem vzpostavljen brez kršitev načela enakosti med državljani, pa je mogoče dvomiti.

70 Iz pripravljalnega gradiva je razvidno, da je cilj izpodbijanega zakona drugačen od konkretnega položaja, ki ga je Sodišče preizkusilo v sodbah Digital Rights Ireland in drugi in Tele2 Sverige in Watson in drugi. V teh sodbah se je Sodišče namreč moralo izreči o vprašanju, ali je obveznost splošne in neselektivne hrambe podatkov nujna in sorazmerna glede na cilj boja proti hudemu kriminalu. Izpodbijani zakon pa ima drug cilj. Gre za zagotavljanje celovitosti kazenskega sistema in izboljšanje zaupanja državljanov v delovanje pravosodja prek iskanja resnice, v interesu žrtve, obdolženca in vseh zadevnih oseb.

71 Med splošno obveznost hrambe podatkov in ciljem, ki se ga želi doseči, obstaja razumna sorazmernost, ki je poleg tega popolnoma skladna s členom 15(1) Direktive 2002/58. Čeprav vsak državljan ni potencialni kriminalec, je namreč lahko vsak državljan soočen s kriminalom, kot žrtev, obtoženec ali priča, zaradi česar ima interes, da se resnica razišče. Kljub splošni obveznosti hrambe podatkov

DELOVNI DOKUMENT

so varovalke, ki so potrebne za varstvo zasebnega življenja, urejene tako pri hrambi teh podatkov kot pri dostopu do teh podatkov. Ob upoštevanju teh varovalk obveznost, ki jo določa zakon, ni nesorazmerna. Izpodbijani zakon ni v nasprotju s sodno prakso Sodišča.

72 Za prejšnjo zakonodajo je bilo presojeno, da nesorazmerno posega v spoštovanje zasebnega življenja zaradi kombinacije štirih elementov: dejstva, da se je hramba podatkov nanašala na vse osebe, neobstoja različnega obravnavanja glede na kategorije hranjenih podatkov in njihovo uporabnost ter neobstoja ali nezadostnosti pravil, kar naj bi pomenilo poseg v pravico do varstva zasebnega življenja.

73 Vendar pa niti Sodišče niti predložitveno sodišče nista presodila, da bi zgolj eden od teh štirih elementov lahko zadoščal za ugotovitev nesorazmernosti ukrepa. Presoja načela sorazmernosti namreč zahteva celovit pristop. Splošno obveznost hrambe podatkov spremljajo zadostne varovalke glede dostopa do podatkov, rokov hrambe ter zaščite in varnosti podatkov, tako da je poseg omejen na to, kar je nujno potrebno.

74 Izpodbijani zakon je skladen s členom 15(1) Direktive 2002/58, vključno v delu, v katerem se nanaša na hrambo podatkov in njihovo posredovanje organom, ki so pristojni za odkrivanje, preiskavo in pregon ostalih oblik kriminala, ki niso hudi kriminal, če obstaja nevarnost za življenje ali telesno celovitost oseb ali stvari ali če se elektronski komunikacijski sistemi uporabljajo nezakonito.

75 Sodba Tele2 Sverige in Watson in drugi ne zahteva, da varovalke obstajajo kumulativno in z ničemer ne nasprotuje tej ugotovitvi.

76 Nazadnje se État belge sklicuje na pripravljalno gradivo za izpodbijani zakon.

VII. Kratka predstavitev obrazložitve predloga

77 Prejšnjo zakonodajo, ki jo je nadomestil izpodbijani zakon, je predložitveno sodišče razglasilo za nično s sodbo št. 84/2015 z dne 11. junija 2015, katere obrazložitev je v tem predlogu za sprejetje predhodne odločbe večkrat citirana. Ta sodba je na voljo na spletni strani Cour constitutionnelle de Belgique (ustavno sodišče, Belgija): http://www.const-court.be/public/f/2015/2015-084f.pdf.

78 Predložitveno sodišče se nato sklicuje na pripravljalno gradivo za zakon (Doc. parl. Chambre, 2015-2016, DOC 54-1567), ki je na voljo na naslovu https://www.lachambre.be/kvvcr/showpage.cfm?section=/flwb&language=fr&cfm=/site/wwwcfm/flwb/flwbn.cfm?lang=F&legislat=54&dossierID=1567).

79 Predložitveno sodišče poudarja, da iz pripravljalnega gradiva izpodbijanega zakona izhaja, da je zakonodajalec poglobljeno preučil tako njegovo zgoraj omenjeno sodbo št. 84/2015 z dne 11. junija 2015 kot sodbo Sodišča Tele2 Sverige in Watson in drugi, na kateri temelji.

DELOVNI DOKUMENT

80 Iz tega izhaja, da cilj, ki ga želi doseči zakonodajalec z izpodbijanim zakonom ni zgolj boj proti terorizmu in spolnim zlorabam otrok, temveč tudi možnost uporabe hranjenih podatkov v zelo različnih primerih, v katerih so lahko ti podatki pomembni za začetek postopka ali pa za neko fazo kazenskega postopka.

81 Zakonodajalec je menil, da je bilo glede na želeni cilj nemogoče uvesti obveznost ciljne in selektivne hrambe, in se je odločil, da bo obveznosti splošne in neselektivne hrambe dodal stroge varovalke, tako glede varstva pri hrambi kot glede dostopa, da bi poseg v pravico do spoštovanja zasebnega življenja omejil na najmanjšo možno mero. V zvezi s tem je poudaril, da je preprosto nemogoče opraviti vnaprejšnje razlikovanje glede na osebe, časovna obdobja in geografska območja. Zakaj to ni mogoče je bilo podrobno obrazloženo v pripravljalnem gradivu (glej dokument 1, točke od 7 do 10, http://www.lachambre.be/FLWB/PDF/54/1567/54K1567001.pdf).

82 Sodišče je v sodbi z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970), to je po sprejetju izpodbijanega zakona, odgovorilo na predhodni vprašanji v zvezi z razlago člena 15(1) Direktive 2002/58.

83 Sodišče je v točki 78 te sodbe presodilo, da „se zakonski ukrep, s katerim država članica na podlagi člena 15(1) Direktive 2002/58 za namene, navedene v tej določbi, nalaga ponudnikom elektronskih komunikacijskih storitev, da nacionalnim organom pod pogoji, ki jih določa ta ukrep, odobrijo dostop do podatkov, ki jih hranijo ti ponudniki, nanaša na obdelavo osebnih podatkov s strani teh ponudnikov, pri čimer gre za obdelavo, ki spada na področje uporabe te direktive.“

84 Sodišče je opozorilo, da člen 5(1) te direktive določa, da države članice s svojo nacionalno zakonodajo zagotovijo zaupnost sporočil in s tem povezanih podatkov o prometu, ki se pošiljajo prek javnega komunikacijskega omrežja in javno razpoložljivih elektronskih komunikacijskih storitev. Načelo zaupnosti pomeni, da tretje osebe brez dovoljenja uporabnikov ne smejo hraniti podatkov o prometu, ki se nanašajo na njihove elektronske komunikacije (točki 84 in 85).

85 Sodišče je spomnilo tudi, da člen 15(1) Direktive državam članicam omogoča, da uvedejo izjeme od načelne obveznosti iz zgoraj omenjenega člena 5(1), ki se v skladu z ustaljeno sodno prakso Sodišča razlagajo ozko. „[Člen 15] torej ne more upravičiti tega, 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“ (točki 88 in 89).

86 V zvezi s tem je treba navesti, da „člen 15(1), prvi stavek, Direktive 2002/58 določa, da mora biti namen zakonskih ukrepov iz tega člena, ki odstopajo od načela zaupnosti komunikacij in z njimi povezanih podatkov o prometu, ‚zaščita državne varnosti (to je Državne varnosti), obramba, javna varnost […] in preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih [kaznivih] dejanj

DELOVNI DOKUMENT

ali nedovoljene uporabe elektronskega komunikacijskega sistema‘ ali morajo imeti drug cilj, naveden v členu 13(1) Direktive 95/46, na katerega napotuje člen 15(1), prvi stavek, Direktive 2002/58 (glej v tem smislu sodbo z dne 29. januarja 2008, Promusicae, C-275/06, EU:C:2008:54, točka 53). Tako naštevanje namenov je izčrpno, kot to izhaja iz člena 15(1), drugi stavek, te direktive, v skladu s katerim morajo biti zakonski ukrepi upravičeni iz ‚razlogov‘ iz člena 15(1), prvi stavek, navedene direktive. Zato lahko države članice te ukrepe sprejmejo le zaradi ciljev, navedenih v tej zadnji določbi“ (točka 90).

87 V zvezi s področjem uporabe člena 15(1) Direktive Sodišče ugotavlja:

„[D]ržave članice [lahko] sprejmejo ukrep, ki odstopa od načela zaupnosti komunikacij in z njimi povezanih podatkov o prometu, kadar je ‚potreben, primeren in ustrezen znotraj demokratične družbe‘ glede na cilje te določbe. V uvodni izjavi 11 te direktive je pojasnjeno, da mora biti tak ukrep ‚dosledno‘ sorazmeren z namenom. Člen 15(1), drugi stavek, navedene direktive zlasti glede hrambe podatkov zahteva, da se ta ukrep sprejme le ‚za določeno obdobje‘ in če je to ‚upravičeno‘ s cilji, navedenimi v členu 15(1), prvi stavek, iste direktive“ (točka 95).

88 Sodišče je nato preizkusilo, ali nacionalna zakonodaja, kakršna se uporablja v prvi zadevi, v kateri so bila postavljena vprašanja za predhodno odločanje, ki so mu bila predložena, izpolnjuje te pogoje. Ugotovilo je, da zadevna nacionalna ureditev določa 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. Na podlagi tako hranjenih podatkov 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 (točki 97 in 98).

89 Po mnenju Sodišča je mogoče na podlagi teh podatkov, če se obdelujejo skupaj, izpeljati zelo natančne ugotovitve glede zasebnega življenja oseb, katerih podatki se hranijo. Ti podatki so zato sredstva za ugotavljanje profila zadevnih oseb, kar so zelo občutljive informacije z vidika pravice do spoštovanja zasebnega življenja ter same vsebine komunikacij.

90 Predložitveno sodišče se v celoti sklicuje na točke od 100 do 112 sodbe Tele2 Sverige in Watson in drugi.

91 Na drugo vprašanje v zadevi C-203/15 in na prvo vprašanje v zadevi C-698/15 je Sodišče odgovorilo, da je treba člen 15(1) Direktive 2002/58 glede na člene 7, 8, 11 in 52(1) Listine razlagati tako, da nasprotuje nacionalni zakonodaji, ki ureja varstvo in varnost podatkov o prometu in podatkov o lokaciji, ter zlasti dostop pristojnih nacionalnih organov do hranjenih podatkov, ne da bi v okviru boja proti kriminalu navedeni dostop omejil zgolj na namen boja proti hudemu kriminalu, ne

DELOVNI DOKUMENT

da bi določil, da mora nadzor nad navedenim dostopom predhodno opraviti sodišče ali neodvisni upravni organ, in ne da bi zahteval, da se zadevni podatki hranijo na ozemlju Unije (točka 125).

92 Evropsko sodišče za človekove pravice (ESČP) pa je medtem presodilo, da je švedska zakonodaja o masovnem prestrezanju elektronskih komunikacij skladna s členom 8 EKČP (ESČP, 19. junij 2018, Centrum för Rättvisa proti Švedski, CE:ECHR:2018:0619JUD003525208). Ugotovitev neobstoja kršitve je oprlo na merila, ki jih je razvilo v prejšnji sodni praksi (ESČP, 4. december 2015, Roman Zakharov proti Rusiji, CE:ECHR:2015:1204JUD004714306). Navedlo je zlasti:

„Sodišče je izrecno priznalo, da imajo nacionalni organi široko polje proste presoje pri izbiri sredstev za zagotavljanje nacionalne varnosti (glej zgoraj navedeno sodbo Weber in Saravia, točka 106). V zadevah Weber in Saravia ter Liberty in drugi je sodišče priznalo, da pravila za masovno prestrezanje sama po sebi ne presegajo tega polja proste presoje. Ob upoštevanju razlogovanja sodišča v teh sodbah in ob upoštevanju groženj, s katerimi se trenutno soočajo številne države pogodbenice (zlasti svetovni terorizem in druge hude oblike kriminala, kot so trgovina z drogo, trgovanje z ljudmi, spolno zlorabljanje otrok in internetni kriminal), tehnološkega razvoja, ki je teroristom in kriminalcem omogočil, da se lažje izognejo odkritju na internetu in nepredvidljivosti poti, po katerih se elektronske komunikacije prenašajo, sodišče meni, da je odločitev o uporabi sistema za masovno prestrezanje zaradi odkrivanja doslej nepoznanih groženj za nacionalno varnost odločitev, ki še vedno spada v okvir proste presoje držav“ (ESČP, 19. junij 2018, Centrum för Rättvisa proti Švedski, CE:ECHR:2018:0619JUD003525208, točka 112).

93 OBFG izpodbijanemu zakonu očita, da enako obravnava uporabnike telekomunikacijskih storitev in elektronskih komunikacij, za katere velja poklicna skrivnost, zlasti odvetnike, in druge uporabnike teh storitev. Ta tožeča stranka ugotavlja, da zakon še vedno uvaja splošno obveznost snemanja in hrambe nekaterih metapodatkov, na podlagi katerih je mogoče ugotoviti, ali je bila fizična ali pravna oseba na posvetu z odvetnikom, identificirati odvetnika, identificirati njegove sogovornike in zlasti njegove stranke ter datum in uro komunikacije. Ta splošna obveznost je naložena vsem ponudnikom, ki javnosti ponujajo storitve fiksne telefonije, mobilne telefonije, dostop do interneta, elektronsko pošto prek interneta, telefonijo prek interneta in javne mreže za elektronsko komunikacijo.

Ta tožeča stranka izpodbijanemu zakonu očita tudi, da določa splošno obveznost hrambe podatkov, ne da bi razlikovala med pravnimi subjekti glede na to, ali se zoper njih vodi preiskava ali pregon zaradi dejanj, za katera je mogoče izreči kazenske sankcije, ali ne.

94 Poleg tega trdi, da so kategorije podatkov, na katere se nanaša zakon, izredno široke in raznolike, ker se nanašajo na podatke, s katerimi se identificira uporabnika ali naročnika in komunikacijska sredstva, na podatke v zvezi z dostopom in povezavo terminalske opreme na omrežje in v zvezi s storitvijo ter

DELOVNI DOKUMENT

določitvijo lokacije te opreme, vključno z omrežno priključno točko, ter na podatke o komunikaciji, tudi če so podatki o vsebini komunikacije izključeni.

95 Nepridobitno združenje Académie fiscale in eden od posameznikov izpodbijanemu zakonu očitata, da enako obravnava uporabnike telekomunikacijskih storitev ali elektronskih komunikacij, za katere velja poklicna skrivnost, zlasti računovodje, davčne svetovalce, in druge uporabnike teh storitev, ne da bi se upoštevali poseben status računovodij in davčnih svetovalcev, bistven pomen poklicne skrivnosti, ki zanje velja, in nujnost zaupnosti razmerja, ki ga imajo s svojimi strankami.

96 Izpodbijanemu zakonu očitata tudi, da enako obravnava pravne subjekte, zoper katere se vodi preiskava ali pregon zaradi dejanj, ki lahko spadajo v okvir namena hrambe spornih elektronskih podatkov, in tiste, zoper katere taki ukrepi niso usmerjeni.

97 Nepridobitni združenji Liga voor Mensenrechten in Ligue des Droits de l'Homme izpodbijanemu zakonu očitata, da določa splošno obveznost hrambe podatkov, ki operaterje in ponudnike javnih telefonskih storitev (vključno z internetno telefonijo), dostopa do interneta in do elektronske pošte prek interneta in ponudnike javnih omrežij za elektronsko komunikacijo zavezuje, da 12 mesecev, dejansko za vse Belgijce, če so osumljenci ali ne, hranijo podatke o prometu pri fiksni telefoniji, mobilni telefoniji in internetni telefoniji in podatke v zvezi z dostopom do interneta, in jih dajejo na razpolago policiji in pravosodju, obveščevalnim in varnostnim službam, urgentnim službam, oddelku zvezne policije za pogrešane osebe in službi za mediacijo za telekomunikacije.

98 Nekatere fizične osebe, ki prebivajo v Belgiji in uporabljajo različne storitve elektronskih komunikacij na podlagi pogodbe, sklenjene z operaterjem, izpodbijanemu zakonu očitajo, da ponudnikom storitev telefonije, vključno prek interneta, dostopa do interneta, elektronske pošte prek interneta, in operaterjem, ki ponujajo javna omrežja za elektronsko komunikacijo, ter operaterjem, ki ponujajo le kakšno od teh storitev, nalaga obveznost splošne in neselektivne hrambe podatkov za identifikacijo, o povezavi in o lokaciji ter osebnih podatkov o komunikaciji.

99 Zakonodajalec je nameraval določiti tri kategorije metapodatkov, ki se morajo hraniti – podatki za identifikacijo, podatki o dostopu in povezavi in podatki o komunikaciji –, zaostriti pogoje za dostop pristojnih organov do podatkov in izboljšati varnost podatkov, ki jih hranijo operaterji, s čimer je želel upoštevati sodbe Sodišča, s katerimi je lahko splošna obveznost hrambe podatkov dopustna, če jo spremljajo take varovalke.

100 Člen 95 Uredbe 2016/679 določa, da ta uredba ne uvaja dodatnih obveznosti za fizične ali pravne osebe v zvezi z obdelavo, povezano z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev v javnih komunikacijskih

DELOVNI DOKUMENT

omrežjih v Uniji v povezavi z zadevami, za katere veljajo posebne obveznosti z istim ciljem iz Direktive 2002/58.

101 Člen 15(1) Direktive 2002/58 določa, da lahko države članice med drugim sprejmejo zakonske ukrepe, ki določajo zadrževanje podatkov za določeno obdobje, iz razlogov, navedenih v tem odstavku, med drugim za zaščito državne varnosti, obrambe, javne varnosti, za preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema, pod pogoji, ki so navedeni v tem odstavku.

102 Izpodbijani zakon med drugim določa pogoje, pod katerimi lahko obveščevalne in varnostne službe pridobijo podatke od ponudnikov in operaterjev.

103 V zvezi s tem je treba ugotoviti, da je v zadevi Privacy International, C-623/17, neko sodišče iz Unije na Sodišče naslovilo naslednja vprašanja:

„V okoliščinah, v katerih:

a. je zmožnost [varnostno-obveščevalnih agencij (Security and Intelligence Agencies, OVA)], da uporabljajo posredovane jim [zbirne komunikacijske podatke (Bulk Communications Data, BCD)], bistvena za varovanje nacionalne varnosti Združenega kraljestva, vključno na področju boja proti terorizmu, vohunjenju in širjenju jedrskega orožja;

b. je temeljna značilnost uporabe BCD s strani OVA odkrivanje prej neznanih groženj nacionalni varnosti s tehnikami neusmerjenega zbiranja, ki temeljijo na zbiranju BCD na enem mestu. Glavna uporabnost tega je hitro identificiranje in razvoj ciljev ter zagotavljanje podlage za ukrepanje ob neposrednih grožnjah;

c. se od ponudnika elektronskega komunikacijskega omrežja nato ne zahteva hramba BCD (za dalj časa kot pri običajnem poslovanju), ki jih hrani izključno država (OVA);

d. je nacionalno sodišče (z nekaterimi pridržanimi vprašanji) presodilo, da so jamstva v zvezi z uporabo BCD s strani OVA skladna z zahtevami EKČP; in

e. je nacionalno sodišče presodilo, da bi se z naložitvijo zahtev iz točk od 119 do 125 sodbe [z dne 21. decembra 2016, Tele2 Sverige ter Watson in drugi (C 203/15 in C 698/15, EU:C:2016:970)] (v nadaljevanju: zahteve iz sodbe Watson), če se uporabljajo, ogrozili ukrepi OVA za varovanje nacionalne varnosti, s tem pa bi se ogrozila nacionalna varnost Združenega kraljestva;

1. Ali ob upoštevanju člena 4 PEU in člena 1(3) Direktive 2002/58/ES o zasebnosti in elektronskih komunikacijah (v nadaljevanju: Direktiva o e-zasebnosti) zahteva v navodilu Secretary of State, da mora ponudnik elektronskega komunikacijskega omrežja varnostno-obveščevalnim agencijam (Security and Intelligence Agencies, OVA) države članice posredovati zbirne

DELOVNI DOKUMENT

komunikacijske podatke, spada na področje uporabe prava Unije in Direktive o e-zasebnosti?

2. Če je odgovor na prvo vprašanje pritrdilen, ali se za tako navodilo Secretary of State uporabljajo katere od zahtev iz sodbe Watson ali katere druge zahteve poleg tistih iz EKČP? In če se, kako in v kakšnem obsegu se take zahteve uporabljajo ob upoštevanju bistvene potrebe OVA, da uporabljajo tehnike zbirnega pridobivanja in samodejne obdelave za varovanje nacionalne varnosti, in obsega, v katerem so lahko take zmožnosti, če so sicer skladne z EKČP, bistveno ogrožene z naložitvijo takih zahtev?“

104 Predložitveno sodišče bo moralo pri svojem preizkusu upoštevati odgovor na ti vprašanji za predhodno odločanje.

105 Izpodbijani zakon določa tudi pogoje, pod katerimi lahko pravosodni organi zaradi odkrivanja, preiskave in pregona kaznivih dejanj pridobijo podatke.

106 Zato je treba počakati tudi na odgovor Sodišča na vprašanje za predhodno odločanje, ki mu je bilo postavljeno v zadevi Ministerio Fiscal, C-207/16:

„Ali se lahko zadostna resnost kaznivih dejanj kot merilo, ki upravičuje poseganje v temeljne pravice, priznane v členih 7 in 8 Listine, ugotovi zgolj glede na kazen, ki se lahko naloži za preiskovano kaznivo dejanje, ali pa je treba poleg tega pri kriminalnem dejanju ugotoviti posebne stopnje škodljivosti za posamične in/ali kolektivne pravne dobrine?

Če je določitev resnosti kaznivega dejanja zgolj na podlagi zagrožene kazni v skladu z ustavnimi načeli Unije, ki jih je Sodišče uporabilo v sodbi Digital Rights kot merila za strog nadzor nad Direktivo, ki je bila v tej sodbi razglašena za neveljavno, kakšen bi moral biti ta spodnji prag? Ali bi bil v skladu s splošno zahtevo po najmanj triletni zaporni kazni?“.

Iz sklepnih predlogov generalnega pravobranilca Saugmandsgaarda Øeja v tej zadevi (C-207/16, EU:C:2018:300) izhaja, da je mogoče upoštevne določbe razlagati na več načinov.

107 Poleg tega se stališča strank pred predložitvenim sodiščem razlikujejo glede razlage več določb, med drugim člena 15(1) Direktive 2002/58 in členov 7, 8, 11 in 52 Listine, ki jih mora predložitveno sodišče uporabiti pri preizkusu izpodbijanega zakona.

108 Kot navajajo tožeče stranke pa je Sodišče v sodbi Tele2 Sverige in Watson in drugi presodilo, da člen 5(1) Direktive 2002/58 določa načelno obveznost zagotavljanja zaupnosti komunikacij in z njimi povezanih podatkov o prometu in da je treba člen 15(1) iste direktive, ki vsebuje izjeme od tega načela, razlagati ozko, da bi se preprečilo, da bi izjema od načelne obveznosti, določene v členu 5 te direktive, postala pravilo, saj bi se sicer tej določbi v veliki meri odvzel pomen.

DELOVNI DOKUMENT

109 Sodišče je poleg tega poudarilo, da lahko zgolj cilji, navedeni v členu 15, upravičijo ukrep, ki odstopa od načela zaupnosti komunikacij in z njimi povezanih podatkov o prometu, saj člen 15 v zvezi s tem zahteva, da se podatki hranijo le za določeno obdobje in le če je to upravičeno iz razlogov, naštetih v tem členu.

110 Poleg tega, kot poudarjajo tožeče stranke, v skladu s stališčem Sodišča nacionalna ureditev, ki zahteva splošno in neselektivno hrambo vseh podatkov o prometu in podatkov o lokaciji vseh naročnikov in registriranih uporabnikov glede vseh elektronskih komunikacijskih sredstev, ne da bi bili uporabniki o tem obveščeni, pomeni posebno resen poseg v temeljne pravice iz členov 7 in 8 Listine, tako da se lahko tak ukrep upraviči le z bojem proti hudemu kriminalu. Sodišče je dodalo, da čeprav je to cilj v splošnem interesu, zgolj z njim ni mogoče utemeljiti tega, da bi se lahko štelo, da je nacionalna ureditev, ki določa splošno in neselektivno hrambo vseh podatkov o prometu in podatkov o lokaciji, nujna za namene tega boja.

111 Sodišče je na podlagi tega sklenilo, da nacionalna ureditev, ki ne določa nobenega razlikovanja, omejitve ali izjeme glede na cilj, ki se ga poskuša doseči, in ki se na splošno nanaša na vse osebe, ki uporabljajo elektronske komunikacijske storitve, brez razlikovanja po kraju ali po času, brez upoštevanja tega, ali so te osebe vsaj posredno v položaju, ki bi lahko pripeljal do kazenskega pregona, in tega, da se posredovanje podatkov uporablja tudi za osebe, za katerih komunikacije velja poklicna skrivnost, ter ki ne zahteva nobene povezave med podatki, za katere se določa hramba, in grožnjo za javno varnost, presega meje nujno potrebnega in je ni mogoče šteti za upravičeno v demokratični družbi, kot to zahteva člen 15(1) Direktive glede na člene 7, 8, 11 in 52(1) Listine.

112 Kot navajajo tožeče stranke Sodišče sicer navaja, da člen 15(1) Direktive 2002/58 ne nasprotuje nacionalnim ureditvam, ki dopuščajo ciljno hrambo podatkov o prometu in podatkov o lokaciji za boj proti hudemu kriminalu, če se hramba podatkov glede kategorij hranjenih podatkov, zadevnih komunikacijskih sredstev, vpletenih oseb in trajanja zadevne hrambe omeji le na to, kar je nujno potrebno. To pomeni, da mora nacionalna ureditev določiti jasna in natančna pravila in da morajo imeti osebe, na katere se hramba podatkov nanaša, na voljo zadostne varovalke, ki omogočajo učinkovito varstvo njihovih osebnih podatkov zoper tveganje zlorabe. Sodišče dodaja, da mora nacionalna ureditev zlasti določiti, v kakšnih okoliščinah in pod kakšnimi pogoji se lahko preventivno sprejme ukrep hrambe podatkov. Taka ureditev mora temeljiti na objektivnih elementih, na podlagi katerih je mogoče opredeliti javnost, katere podatki lahko izkažejo zvezo s hudimi kaznivimi dejanji ali ki predstavlja resno nevarnost za javno varnost, pri čemer se lahko taka razmejitev zagotovi z geografskim merilom, kadar pristojni nacionalni organi na podlagi objektivnih elementov menijo, da obstaja v enem ali več geografskih območjih visoko tveganje za pripravo ali izvršitev takih dejanj.

113 S sprejetjem izpodbijanega zakona pa želi zakonodajalec doseči cilje, ki so širši od boja proti hudemu kriminalu ali tveganjem resnih kršitev javne varnosti.

DELOVNI DOKUMENT

114 Zakonodajalec je v pripravljalnem gradivu tudi večkrat navedel, da je, kar se tiče načela obveznosti hrambe podatkov, vključil vse osebe, tudi če zoper njih še ne teče preiskava; poleg tega ni uvedel razlikovanja glede na časovno obdobje, geografsko območje ali krog oseb in tudi ni določil izjeme v zvezi z osebami, za katerih komunikacije velja poklicna skrivnost.

115 Po mnenju tožečih strank, čeprav so bili pogoji za dostop do hranjenih podatkov v izpodbijanem zakonu precej zaostreni, splošna obveznost hrambe podatkov, določena v tem zakonu, ne izpolnjuje zahtev iz člena 15(1) Direktive 2002/58 v povezavi s členi 7, 8, 11 in 52(1) Listine, kot jih je Sodišče razlagalo v sodbi Tele2 Sverige in Watson in drugi. Taka obveznost namreč presega to, kar je nujno potrebno in se ne more šteti za upravičeno v demokratični družbi, kot to zahtevajo zgoraj navedene evropske določbe.

116 Svet ministrov poudarja, da se želi z izpodbijano zakonodajo doseči več ciljev. Zakonodajalec želi najprej okrepiti položaj, ki obstaja že dolgo in v katerem je dostop do podatkov na področju telekomunikacij možen v okviru kazenskih preiskav, kar ustvarja pravni okvir, ki zagotavlja potrebne varovalke na področju varstva zasebnega življenja. Obveznost hrambe je uvedena tudi zaradi odkrivanja resnice pri različnih oblikah kriminala, tako da se želi z njo zagotoviti celovitost kazenskega sistema. To iskanje resnice je v interesu žrtve, obtoženca (ki lahko na primer dokaže, da se je v ključnem trenutku nahajal drugje) in tudi drugih zadevnih oseb. Obveznost hrambe je potrebna tudi zaradi ukrepanja na podlagi klica na urgentne službe ali zaradi iskanja pogrešane osebe, katere telesna celovitost je v neposredni nevarnosti. Ta element pomeni pomembno razliko glede na položaje, ki so bili navedeni v prejšnjih sodbah Sodišča. Med splošno obveznostjo hrambe in ciljem, ki si ga je zastavil zakonodajalec, obstaja torej vez sorazmernosti.

117 Svet ministrov poudarja tudi, da zakonodajalec ni menil, da je glede na želeni cilj mogoče uvesti obveznost ciljne in selektivne hrambe, in se je odločil, da bo obveznosti splošne in neselektivne hrambe dodal stroge varovalke, tako glede varstva pri hrambi kot glede dostopa, da bi poseg v pravico do varstva zasebnega življenja omejil na najmanjšo možno mero. V zvezi s tem je svet ministrov poudaril, da je preprosto nemogoče opraviti vnaprejšnje razlikovanje glede na osebe, časovna obdobja in geografska območja. Skliceval se je tudi na sklepne predloge generalnega pravobranilca Saugmandsgaarda Øeja v združenih zadevah Tele2 Sverige in drugi, C-203/15 in C-698/15, EU:C:2016:572.

118 Iz elementov, s katerimi razpolaga predložitveno sodišče izhaja, da ima poleg tega večina držav članic velike težave pri usklajevanju svoje zakonodaje o hrambi podatkov z zahtevami, ki jih je Sodišče navedlo v svoji sodni praksi (glej: Data retention across the EU, http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention; dopis nizozemskega ministra za pravosodje in varnost z dne 26. marca 2018 predsedniku „Tweede Kamer der Staten-Generaal“ drugi senat, seja 2017-2018, 34 537, št. 7).

DELOVNI DOKUMENT

119 Zato je treba Sodišču postaviti prvo vprašanje za predhodno odločanje, ki je navedeno v izreku.

120 Z izpodbijanim zakonom se želi omogočiti tudi učinkovito preiskovanje kaznivih dejanj in učinkovito kaznovanje spolnih zlorab mladoletnikov in omogočiti uspešno identifikacijo storilca takega kaznivega dejanja, tudi kadar se uporabijo sredstva za elektronsko komuniciranje. Na obravnavi je bila v zvezi s tem pozornost posvečena pozitivnim obveznostim, ki izhajajo iz členov 3 in 8 EKČP v zvezi z varovanjem telesne celovitosti in morale mladoletnikov in drugih ranljivih oseb, kot jih razlaga ESČP (ESČP, 2. december 2008, K.U. proti Finski, CE:ECHR:2008:1202JUD000287202, §§46-49). Te obveznosti lahko izhajajo tudi iz ustreznih določb Listine, kar bi lahko imelo posledice za razlago člena 15(1) Direktive 2002/58.

121 Zato je treba postaviti drugo vprašanje za predhodno odločanje, navedeno v izreku.

122 Nazadnje je treba postaviti tudi tretje vprašanje za predhodno odločanje, navedeno v izreku.

VIII. Vprašanja za predhodno odločanje

123 Cour constitutionnelle (ustavno sodišče, Belgija) Sodišču Evropske unije postavlja naslednja vprašanja:

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, in pravico do spoštovanja osebnih podatkov, kot jo zagotavljajo členi 7, 8 in 52(1) Listine Evropske unije o temeljnih pravicah, razlagati tako, da nasprotuje nacionalni zakonodaji, kakršna je 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, ali preprečevanje prepovedane uporabe sistemov elektronskih komunikacij ali doseganje drugih ciljev, ki so našteti v členu 23(1) Uredbe (EU) 2016/679, 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 Evropske unije o temeljnih pravicah razlagati tako, da nasprotuje nacionalni zakonodaji, kakršna je 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, če je cilj te zakonodaje med drugim izpolnitev pozitivnih obveznosti, ki jih ima organ na podlagi členov 4 in 8 Listine,

DELOVNI DOKUMENT

da sprejme zakonski okvir, ki omogoča učinkovito kazensko preiskavo in učinkovito kaznovanje spolnih zlorab mladoletnikov in 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 loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (zakon z dne 29. maja 2016 o zbiranju in hrambi podatkov na področju elektronskih komunikacij) 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?

DELOVNI DOKUMENT