EVROPSKA
KOMISIJA

Bruselj, 25.1.2017
COM(2017) 41 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, EVROPSKEMU SVETU IN SVETU

Četrto poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije

Četrto poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije

I. UVOD

To je četrto mesečno poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije, ki zajema najnovejše dogodke na področju dveh glavnih stebrov: *boja proti terorizmu in organiziranemu kriminalu ter sredstvom, ki se uporabljajo v ta namen, in krepitve naše zaščite in odpornosti proti navedenim nevarnostim*. V poročilu so poudarjena štiri ključna področja: informacijski sistemi in interoperabilnost, zaščita mehkih tarč, kibernetske grožnje ter varstvo podatkov v kazenskih preiskavah.

Napad na berlinski božični sejem decembra je znova izpostavil hude pomanjkljivosti naših informacijskih sistemov, ki jih je treba čim prej odpraviti, zlasti na ravni EU, da bodo lahko nacionalni mejni organi in organi kazenskega pregona na terenu učinkoviteje opravljali svoje delo. Dejstvo, da različni informacijski sistemi niso medsebojno povezani – kar napadalcem omogoča, da se z uporabo več identitet neopaženi gibljejo, tudi pri prečkanju meja –, in dejstvo, da države članice teh informacij ne nalagajo rutinsko v ustrezne podatkovne zbirke EU, sta praktični pomanjkljivosti pri izvajanju, ki ju je treba nujno odpraviti. Prav tako so potrebna nadaljnja prizadevanja pri uveljavljanju ukrepov kazenskega pregona na mejah in vračanju oseb, katerih prošnje za azil so bile zavrnjene[1].

Kar zadeva zaščito mehkih tarč, bo Komisija pospešila začeta prizadevanja za združitev strokovnjakov držav članic ter izmenjavo dobrih praks in skupno oblikovanje standardnih smernic.

Mediji obsežno poročajo o kibernetskih grožnjah, s katerimi se sooča EU, v tem poročilu pa so obravnavana različna s tem povezana delovna področja, na katerih so že bili sprejeti nekateri ukrepi. Pri tem sta zajeta preventivna stran – prek sodelovanja s panogo za spodbujanje vgrajene varnosti in izvajanja direktive o varnosti omrežij in informacij – ter spodbujanje sodelovanja med državami članicami in sodelovanja z mednarodnimi organizacijami in partnerji na področju sprotnega boja proti kibernetskim napadom. Komisija in Visoki predstavnik Unije za zunanje zadeve in varnostno politiko bosta v prihodnjih mesecih opredelila ukrepe, ki so potrebni za učinkovit vseevropski odziv na navedene grožnje, ki bo temeljil na strategiji EU za kibernetsko varnost iz leta 2013.

Varstvo zasebnosti posameznikov in njihovih osebnih podatkov je ključna pravica in temelj vsakršnega ukrepanja za vzpostavitev prave varnostne unije. Direktiva o varstvu podatkov za področji policije in kazenskega pravosodja, ki je bila sprejeta aprila 2016, zagotavlja skupen visok standard za varstvo podatkov in bo tako omogočila nemotene izmenjave relevantnih podatkov med organi kazenskega pregona držav članic. Komisija je v okviru svežnja o podatkih začela tudi pregled direktive o zasebnosti in elektronskih komunikacijah, da bi razširila njeno področje uporabe in vanj vključila vse ponudnike elektronskih komunikacij ter določbe direktive uskladila z določbami splošne uredbe o varstvu podatkov. Predlog je zasnovan tako, da zagotavlja zasebnost elektronskih komunikacij, obenem pa določa podlago za morebitno omejevanje področja uporabe

[1] Komisija bo v prihodnjih tednih predložila spremenjen akcijski načrt o vračanju; glej Poročilo Komisije Evropskemu parlamentu, Evropskemu svetu in Svetu o operacionalizaciji evropske mejne in obalne straže (COM(2017) 42).

uredbe o zasebnosti in elektronskih komunikacijah, med drugim zaradi zagotavljanja nacionalne varnosti ali izvajanja kazenskih preiskav.

II. KREPITEV INFORMACIJSKIH SISTEMOV IN IZBOLJŠANJE INTEROPERABILNOSTI

Nagovor predsednika Jeana-Clauda Junckerja o stanju v Uniji septembra 2016 in sklepi Evropskega sveta iz decembra 2016 poudarjajo pomen odpravljanja trenutnih pomanjkljivosti pri upravljanju informacij in izboljšanja **interoperabilnosti in medsebojne povezanosti med obstoječimi informacijskimi sistemi**. Ob nedavnih dogodkih se je znova pokazala nujnost medsebojne povezave obstoječih podatkovnih zbirk EU, tudi da se mejnim organom in organom kazenskega pregona zagotovijo potrebna orodja za odkrivanje identitetnih prevar. Storilec terorističnega napada v Berlinu decembra 2016 je na primer uporabil vsaj 14 različnih identitet in je lahko tako neopazno prehajal med državami članicami. Očitno je, da je treba omogočiti sočasno iskanje po obstoječih in prihodnjih informacijskih sistemih EU z uporabo biometričnih identifikatorjev, da se teroristom in kriminalcem zapre ta pot.

Komisija je začela v zvezi s tem aprila 2016 pripravljati predloge za „trdnejše in pametnejše informacijske sisteme za meje in varnost“[2]. Pri tem je opredelila pomanjkljivosti v funkcionalnosti obstoječih sistemov, vrzeli v arhitekturi EU za upravljanje podatkov ter težave s kompleksnostjo različno upravljanih informacijskih sistemov in vsesplošno razdrobljenostjo, ki ji botruje dejstvo, da so bili obstoječi sistemi zasnovani posamezno in ne kot del celote. V okviru tega procesa je Komisija oblikovala **strokovno skupino na visoki ravni za informacijske sisteme in interoperabilnost** izmed uslužbencev agencij EU, držav članic in relevantnih zainteresiranih strani. V poročilu predsednika skupine z dne 21. decembra 2016[3] so bile predstavljene **vmesne ugotovitve** skupine, ki med drugim vključujejo prednostno možnost oblikovanja enotnega portala za iskanje, prek katerega bi nacionalni organi kazenskega pregona in mejni organi lahko izvajali sočasne poizvedbe po vseh obstoječih podatkovnih zbirkah in informacijskih sistemih EU. Vmesno poročilo poudarja tudi pomen kakovosti podatkov – saj je učinkovitost informacijskih sistemov premo sorazmerna kakovosti in formatu vanje vnesenih podatkov – in predlaga priporočila za izboljšanje kakovosti podatkov v sistemih EU s pomočjo avtomatiziranega nadzora kakovosti podatkov.

Komisija bo hitro sprejela ukrepe na podlagi možnosti oblikovanja enotnega portala za iskanje in skupaj z agencijo EU za operativno upravljanje obsežnih informacijskih sistemov, tj. agencijo eu-LISA, začela pripravljati portal, ki bo omogočal vzporedne poizvedbe po vseh relevantnih obstoječih sistemih EU. Do junija bi morala biti zaključena s tem povezana študija, ki bo podlaga za zasnovo in testiranje prototipa portala še pred koncem leta. Komisija meni, da bi moral Europol vzporedno s tem nadaljevati razvoj sistemskega vmesnika, ki bo policijskim organom držav članic pri poizvedbah po nacionalnih sistemih omogočal avtomatsko sočasno iskanje po Europolovih podatkovnih zbirkah.

[2] Sporočilo z naslovom „Trdnejši in pametnejši informacijski sistemi za meje in varnost“ (COM(2016) 205 final).

[3] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1

Prizadevanja za interoperabilnost informacijskih sistemov so namenjena odpravljanju sedanje razdrobljenosti arhitekture EU za upravljanje podatkov za nadzor meje in varnost ter povezanih slepih peg. Kadar podatkovne zbirke uporabljajo skupno odložišče podatkov o identiteti – kot predvidevata predlagani evropski sistem vstopa/izstopa in predlagani evropski sistem za potovalne informacije in odobritve (ETIAS) –, se lahko posameznik v različne podatkovne zbirke vnese zgolj pod eno samo identiteto, s čimer se prepreči uporaba različnih lažnih identitet. Komisija je kot prvi ukrep v skladu s priporočilom vmesnih ugotovitev strokovne skupine na visoki ravni agenciji eu-LISA naložila, naj analizira tehnične in operativne vidike vzpostavitve skupne storitve za ugotavljanje ujemanja biometričnih podatkov. Takšna storitev bi omogočila poizvedbe po različnih podatkovnih zbirkah na podlagi biometričnih podatkov, kar bi lahko razkrilo lažne identitete, ki jih zadevna oseba uporablja v drugem sistemu. Poleg tega bi morala strokovna skupina na visoki ravni zdaj oceniti, ali je potrebno, tehnično izvedljivo in sorazmerno razširiti **skupno odložišče podatkov o identiteti**, ki ga predvidevata sistem vstopa/izstopa in ETIAS, na druge sisteme. Poleg biometričnih podatkov, shranjenih v storitvi za ugotavljanje ujemanja tovrstnih podatkov, bi takšno skupno odložišče podatkov o identiteti vključevalo tudi alfanumerične identifikacijske podatke. Skupina bi morala svoje ugotovitve glede tega predstaviti v svojem končnem poročilu do konca aprila 2017.

Nedavni varnostni dogodki poudarjajo potrebo po ponovni proučitvi vprašanja **obvezne izmenjave informacij** med državami članicami. Predlog Komisije iz decembra 2016 za okrepitev **schengenskega informacijskega sistema** prvič državam članicam nalaga obveznost razpisovanja ukrepov za osebe, povezane s terorističnimi kaznivimi dejanji. Pomembno je, da si zdaj sozakonodajalca prizadevata za hitro sprejetje predlaganih ukrepov. Komisija je pripravljena proučiti, ali bi bilo treba obveznost izmenjave informacij uvesti tudi za druge podatkovne zbirke EU.

III. ZAŠČITA NAŠIH MEHKIH TARČ PRED TERORISTIČNIMI NAPADI

Napad v Berlinu je zadnji napad v EU zoper tako imenovane mehke tarče, ki so navadno civilni objekti, kjer se ljudje združujejo v velikem številu (npr. javna mesta, bolnišnice, šole, športne dvorane, kulturna središča, kavarne in restavracije, nakupovalna središča ter prometna vozlišča). Po naravi so te lokacije ranljive in jih je težko zavarovati, poleg tega pa so v primeru napada zanje značilne množične žrtve. Prav zato jih teroristi radi izbirajo. Grožnja napadov na mehke tarče, vključno s prometno infrastrukturo, v prihodnosti ostaja velika, kot potrjujejo razpoložljive ocene, med drugim poročilo Europola o spremembah v načinu delovanja organizacije Daiš[4].

Evropska agenda za varnost iz leta 2015 in sporočilo o varnostni uniji iz leta 2016 sta poudarila potrebo po povečanju prizadevanj za izboljšanje varnosti ter uporabe inovativnih orodij in tehnologij za odkrivanje pri zaščiti mehkih tarč. Komisija si je prizadevala podpirati in spodbujati izmenjavo dobrih praks med državami članicami na področju razvoja boljših orodij za preprečevanje napadov na mehke tarče in odzivanje nanje. Na podlagi teh prizadevanj so bili pripravljeni operativni priročniki in navodila.

[4] Europol, *Changes in modus operandi of Islamic State (IS) revisited*, november 2016 – Europol Public Information, na voljo na strani: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited.

Komisija trenutno v tesnem sodelovanju s strokovnjaki držav članic razvija celovit priročnik o varnostnih postopkih in predloge, ki se lahko uporabljajo za različne mehke tarče (npr. nakupovalna središča, bolnišnice, športne in kulturne dogodke). Namen je v začetku leta 2017 izdati navodila za države članice glede zaščite mehkih tarč, ki bodo temeljila na dobrih praksah držav članic.

Ob tem bo Komisija februarja organizirala prvo delavnico z nacionalnimi organi na temo zaščite mehkih tarč z namenom izmenjave informacij in razvoja dobrih praks v zvezi s kompleksnim problemom njihove zaščite ter javne varnosti in zaščite ljudi. Komisija financira tudi pilotni projekt, ki ga izvajajo Belgija, Nizozemska in Luksemburg v okviru Sklada za notranjo varnost, v zvezi z vzpostavitvijo regionalnega centra odličnosti za posebne intervencije kazenskega pregona, ki bo ponujal usposabljanje za policiste, ki so v primeru napada prvi na kraju dogodka.

Odzivanje ob napadih na mehke tarče je ključni sestavni del prizadevanj Komisije na področju civilne zaščite. Komisija je decembra napovedala, katere ukrepe namerava izvajati z državami članicami, da bi zaščitila državljane EU in omejila ranljivosti takoj po terorističnih napadih. Ti ukrepi bodo okrepili usklajevanje med vsemi akterji, ki so vključeni v obvladovanje posledic napadov. Komisija se je zavezala, da bo podprla prizadevanja držav članic, tako da bo omogočila skupno usposabljanje in urjenje ter vodila trajnostni dialog prek obstoječih žarišč in strokovnih skupin. Komisija bo poleg tega podpirala razvoj specializiranih modulov za odzivanje na teroristične napade v okviru mehanizma Unije na področju civilne zaščite ter pobud za izmenjavo izkušenj in ozaveščanje javnosti.

Komisija bo skupaj z državami članicami tudi proučila, kakšna podpora EU je na voljo za povečanje odpornosti in okrepitev varnosti v okolici potencialnih mehkih tarč. Države članice lahko poleg tega Evropsko investicijsko banko (vključno z Evropskim skladom za strateške naložbe) zaprosijo za financiranje v skladu s politikami skupine EU in EIB. Vsak projekt se presoja v običajnem postopku odločanja, kot določa zakonodaja.

Kar zadeva specifične mehke tarče v zvezi z javnimi mesti javnega prevoza, kot so javnosti dostopni deli letališč ali železniških postaj, je bila na namenski delavnici Komisije novembra 2016, ki so se je udeležile najrazličnejše zainteresirane strani, poudarjena potreba po ohranjanju ravnovesja med varnostnimi potrebami, udobjem za potnike in prevozi. Med ugotovitvami so bili izpostavljeni pomen izgradnje kulture varnosti, ki ne zajema zgolj osebja, ampak tudi potnike, pomen lokalnih ocen tveganj kot podlaga za opredelitev ustreznih protiukrepov ter potreba po okrepitvi komunikacij med vsemi vpletenimi stranmi.

IV. SOOČANJE Z IZZIVI KIBERNETSKIH GROŽENJ

Kibernetska kriminaliteta in kibernetski napadi so ključni izzivi za Unijo, pri čemer lahko ukrepanje na ravni EU glede teh izzivov prispeva h krepitvi naše skupne odpornosti. Kibernetski incidenti dnevno resno oškodujejo človeška življenja in povzročajo veliko gospodarsko škodo evropskemu gospodarstvu in podjetjem. Kibernetski napadi so ključni del hibridnih groženj. Če so natančno načrtovani, tako da sovpadajo s fizičnimi grožnjami, na primer v povezavi s terorizmom, imajo lahko uničujoč učinek. Povzročijo lahko tudi destabilizacijo države ali omajejo njene politične institucije ter temeljne demokratične procese. S povečanjem našega zanašanja na spletne tehnologije se bo povečala tudi ranljivost naših kritičnih infrastruktur (od bolnišnic do jedrskih elektrarn).

Strategija EU za kibernetsko varnost iz leta 2013 je del glavnega političnega odziva na kibernetske izzive. Podlaga za osrednje ukrepanje na tem področju je direktiva o varnosti omrežij in informacij[5], ki je bila sprejeta julija lani. Je osnova za izboljšano sodelovanje na ravni EU in kibernetsko odpornost, saj podpira sodelovanje in izmenjavo informacij med državami članicami ter spodbuja operativno sodelovanje ob specifičnih kibernetskih incidentih in izmenjavo informacij o tveganjih. Za zagotovitev doslednega izvajanja določb direktive v različnih sektorjih in preko meja bo Komisija februarja vodila prvo srečanje skupine za sodelovanje glede varnosti omrežij in informacij z državami članicami.

Komisija in Visoki predstavnik EU sta aprila 2016 sprejela skupni okvir o preprečevanju hibridnih groženj[6], v katerem predlagata 22 operativnih ukrepov, namenjenih ozaveščanju, krepitvi odpornosti, boljšemu odzivanju na krizne razmere in okrepitvi sodelovanja med EU in Natom. Po pozivu Sveta bosta Komisija in Visoki predstavnik EU do julija 2017 pripravila poročilo o oceni napredka.

Komisija prav tako spodbuja in podpira tehnološke inovacije, med drugim z uporabo sredstev EU za raziskave za spodbujanje iskanja novih rešitev in ustvarjanje novih tehnologij, ki lahko prispevajo h krepitvi naše odpornosti na kibernetske napade (npr. projekti „vgrajene varnosti“). Lani poleti smo začeli izvajati 1,8 milijarde EUR vredno javno-zasebno partnerstvo z industrijo za kibernetsko varnost[7].

V prometu postaja digitalizacija pomemben dejavnik zelo potrebne preobrazbe današnjega prometnega sistema. Hitro napredovanje digitalizacije prinaša številne koristi, hkrati pa je zaradi tega promet bolj izpostavljen nevarnostim kibernetskega prostora z vidika zaščite strojne in programske opreme pred kibernetskimi napadi oziroma njihove varne uporabe. Izvaja se več ukrepov za omilitev grožnje na različnih ravneh, zlasti v letalstvu, vendar tudi v pomorskem, rečnem, železniškem in cestnem prometu[8]. Preostali izziv je še dodatno pojasniti, uskladiti in dopolniti dejavnosti različnih zainteresiranih strani, ki se ukvarjajo s krepitvijo različnih vidikov odpornosti sistemov kibernetske varnosti.

Širše, in glede na hitri razvoj grožnje, bosta Komisija in Visoki predstavnik EU v prihodnjih mesecih opredelila potrebne ukrepe za zagotovitev učinkovitega vseevropskega odziva na te grožnje, pri čemer se bosta oprla na strategijo EU za kibernetsko varnost iz leta 2013.

---

5 Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.

6 JOIN(2016) 18.

7 Napovedano v sporočilu o odpornosti sistema kibernetske varnosti iz leta 2016 (COM(2016) 410 final).

8 Primeri tega so mednarodne smernice, kot so smernice, ki jih je razvila Mednarodna pomorska organizacija, ali nedavno sprejeta resolucija Mednarodne organizacije civilnega letalstva s skupno pobudo EU in ZDA; poročanje o incidentih, na podlagi česar Evropska agencija za varnost v letalstvu trenutno razvija bolj odziven pristop, in kibernetska vgrajena varnost, ki se bo uporabljala v novih sistemih, ki se še razvijajo, kot je osrednji načrt za upravljanje zračnega prometa Skupnega podjetja SESAR.

V. VARSTVO OSEBNIH PODATKOV OB HKRATNI PODPORI UČINKOVITIH KAZENSKIH PREISKAV

Direktiva o varstvu osebnih podatkov za področji policije in kazenskega pravosodja[9] je temelj boja proti terorizmu in hudim kaznivim dejanjem. Organi kazenskega pregona držav članic bodo lahko na podlagi skupnega standarda za varstvo podatkov, opredeljenega v Direktivi, nemoteno izmenjevali relevantne podatke, medtem ko bo ustrezno zagotovljeno varstvo podatkov žrtev, prič in osumljencev kaznivih dejanj.

Poleg tega je Komisija za zagotovitev visoke ravni zaupnosti komunikacij za posameznike in podjetja ter enakih konkurenčnih pogojev za vse tržne udeležence, kot je določeno v strategiji za enotni digitalni trg iz aprila 2015, 11. januarja sprejela predlagano **uredbo o e-zasebnosti** (ki nadomešča Direktivo 2002/58/ES)[10]. Kot velja za veljavno direktivo, spremenjena uredba o e-zasebnosti natančno razlaga splošno uredbo o varstvu podatkov[11] in določa okvir, ki bo urejal varstvo zasebnosti in osebnih podatkov v sektorju elektronskih komunikacij.

Kot rezultat navedene spremembe se vsi podatki elektronskih komunikacij, tudi kar zadeva pomožno komunikacijo, štejejo za zaupne/tajne, ne glede na to, ali komunikacija poteka prek tradicionalnih telekomunikacijskih storitev ali drugih tako imenovanih storitev OTT („over-the-top services“), ki so jim enakovredne z vidika funkcionalnosti (npr. Skype in WhatsApp), ki so za številne uporabnike pogosto zamenljive z običajnimi telekomunikacijskimi operaterji[12]. Obveznosti za ponudnike storitev – poleg spoštovanja izbir njihovih strank glede zasebnosti pri uporabi, shranjevanju in obdelavi njihovih podatkov – vključujejo tudi obveznost za ponudnike storitev s sedežem zunaj EU, da imenujejo predstavnika v eni od držav članic. Tako bodo imele države članice tudi možnost, da pomagajo pri sodelovanju organov kazenskega pregona in pravosodnih organov s ponudniki storitev glede dostopa do elektronskih dokazov (glej v nadaljevanju).

Kot velja v skladu s trenutnimi pravili o e-zasebnosti, bo dostop organov kazenskega pregona in pravosodnih organov do relevantnih elektronskih informacij, ki so potrebne za preiskavo kaznivega dejanja, urejala izjema iz člena 11 predlagane uredbe o e-zasebnosti[13]. Ta določba v skladu s pravom EU ali nacionalnim pravom omogoča

---

9 Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ. Direktivo, ki velja od 5. maja 2016, morajo države članice do 6. maja 2018 prenesti v domačo zakonodajo. Komisija je oblikovala strokovno skupino z državami članicami za izmenjavo stališč glede prenosa policijske direktive.

10 Uredba o zasebnosti in elektronskih komunikacijah (COM(2017) 10).

11 Uredba (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), ki se bo začela uporabljati 25. maja 2018.

12 To sledi pristopu v predlagani direktivi o Evropskem zakoniku o elektronskih komunikacijah, ki ga je Komisija predložila 14. septembra 2016 (telekomunikacijski sveženj) (COM(2016) 590 final).

13 Glej člen 11(1), tj. določbo o hrambi podatkov, ki ostaja enaka členu 15 direktive o e-zasebnosti in je skladna z zahtevami splošne uredbe o varstvu podatkov. Pri takšnih omejitvah je treba zagotoviti spoštovanje temeljnih pravic, prav tako pa morajo biti omejitve nujne, primerne in sorazmerne.

omejitev zaupnosti komunikacij, kadar je to potrebno in sorazmerno, da se zaščitijo nacionalna varnost, obramba, javna varnost in preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij. Ta določba je še zlasti pomembna za nacionalna pravila za **hrambo podatkov**, tj. obveznost ponudnikov telekomunikacijskih storitev, da za določeno obdobje hranijo podatke komunikacij zaradi morebitnega dostopa organov kazenskega pregona, potem ko je Sodišče Evropske unije leta 2014 za neveljavno razglasilo direktivo o hrambi podatkov[14]. Od takrat ni bilo instrumenta EU v zvezi s hrambo podatkov in nekatere države članice so sprejele lastne nacionalne zakone o hrambi podatkov. Švedski in britanski zakon o hrambi podatkov sta bila izpodbijana pred Sodiščem, ki je svojo sodbo Tele2 izreklo 21. decembra[15]. Sodišče je za nezdružljivo s pravom EU razglasilo nacionalno zakonodajo, ki za namen boja proti kriminalu določa splošno in neselektivno hranjenje vseh podatkov o prometu in lokaciji naročnikov in uporabnikov v zvezi z vsemi sredstvi elektronskih komunikacij. Analiza posledic sodbe poteka in Komisija bo pripravila navodila za pripravo nacionalnih zakonov o hrambi podatkov, da bodo skladni s sodbo.

Kazniva dejanja puščajo digitalne sledi, ki se lahko uporabijo kot dokazi v sodnem postopku. Elektronske komunikacije med osumljenci so pogosto edini indici, ki jih lahko zberejo organi kazenskega pregona in tožilstvo. Vendar je pridobitev dostopa do **elektronskih dokazov** – zlasti če so shranjeni v tujini ali v oblaku – lahko tehnično in pravno kompleksen postopek, pogosto pa pomeni veliko breme z vidika postopka, kar ovira potrebo preiskovalcev po hitrem delovanju. Da bi obravnavala ta izziv, Komisija trenutno ocenjuje rešitve, ki bi preiskovalcem omogočile pridobivanje čezmejnih elektronskih dokazov, vključno s povečanjem učinkovitosti medsebojne pravne pomoči ter iskanjem načinov neposrednega sodelovanja s ponudniki internetnih storitev, in ki bi predlagale merila za določitev in uveljavitev jurisdikcije v kibernetskem prostoru, ob polnem spoštovanju veljavnih pravil o varstvu podatkov.[16] Komisija je 9. decembra 2016 Svetu za pravosodje in notranje zadeve poročala o napredku na tem področju[17].

Celovit (in še ne zaključen) postopek posvetovanja s strokovnjaki je Komisiji omogočil, da je opredelila različne, pogosto kompleksne probleme v zvezi z dostopom do elektronskih dokazov, pridobila boljše razumevanje veljavnih pravil in praks v državah članicah ter identificirala različne možne politike. Poročilo o napredku zagotavlja pregled zamisli, ki so se doslej porajale v postopku zbiranja informacij in strokovnem procesu. V prihodnjih mesecih bo Komisija v posvetovanju z zainteresiranimi stranmi te zamisli podrobneje proučila. Kot je bilo napovedano v delovnem programu Komisije, bo Komisija pobudo na tem področju predstavila v letu 2017.

---

[14] Sodba Sodišča z dne 8. aprila 2014 v združenih zadevah Digital Rights Ireland (C-293/12 in C-594/12).

[15] Sodba Sodišča z dne 21. decembra 2016 v združenih zadevah Tele2 (C-203/15 in C-698/15).

[16] Kakor se je zavezala v evropski agendi za varnost (COM(2015) 185 final) in v sporočilu Komisije z naslovom „Izvajanje evropske agende za varnost z namenom boja proti terorizmu ter utiranja poti k učinkoviti in pravi varnostni uniji“ (COM(2016) 230 final).

[17] Svet je v svojih Sklepih o izboljšanju kazenskega pravosodja v kibernetskem prostoru z dne 9. junija 2016 Komisijo pozval, naj sprejme konkretne ukrepe, razvije skupen pristop EU in do junija 2017 predstavi dosežene rezultate.

VI. ZAKLJUČEK

Naslednje poročilo, ki mora biti pripravljeno do 1. marca, bo priložnost za pregled napredka pri izvajanju teh in drugih ključnih delovnih področij.