EVROPSKA
KOMISIJA

Bruselj, 30.10.2019
COM(2019) 552 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, EVROPSKEMU SVETU IN SVETU

Dvajseto poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije

I. UVOD

To je dvajseto poročilo o nadaljnjem napredku pri vzpostavljanju učinkovite in prave varnostne unije ter zajema razvoj v okviru dveh glavnih stebrov: boja proti terorizmu in organiziranemu kriminalu ter sredstvom, ki se uporabljajo v ta namen, ter krepitve naše zaščite in odpornosti proti tem grožnjam.

Za Junckerjevo Komisijo je varnost že od prvega dne glavna prednostna naloga. EU se je na podlagi evropske agende za varnost iz aprila 2015[1] in sporočila o utiranju poti k učinkoviti in pravi varnostni uniji iz aprila 2016,[2] z usklajenim pristopom odzvala na vrsto terorističnih napadov in druge vse resnejše varnostne izzive, pri čemer je dosegla pomemben napredek pri krepitvi naše skupne varnosti[3]. Vse bolj je jasno, da so današnji varnostni izzivi, ne glede na to, ali gre za terorizem, organizirani kriminal, kibernetske napade, dezinformacije ali druge nastajajoče grožnje, ki jih omogoča kibernetski prostor, grožnje, ki so skupne vsem. Samo s sodelovanjem lahko dosežemo raven kolektivne varnosti, ki jo državljani upravičeno zahtevajo in pričakujejo. Takšno skupno razumevanje je podlaga za napredek pri oblikovanju učinkovite in prave varnostne unije. Podpora na ravni EU se je zaradi potreb nacionalnih organov, ki si prizadevajo za varnost državljanov, osredotočila na zakonodajne in operativne ukrepe, pri katerih lahko skupno ukrepanje vpliva na varnost držav članic. To delo je potekalo v tesnem sodelovanju z Evropskim parlamentom in Svetom ter je bilo popolnoma pregledno za širšo javnost. V središču teh prizadevanj je polno spoštovanje temeljnih pravic, saj se lahko varnost Unije zagotovi le, če lahko državljani zaupajo, da se njihove temeljne pravice v celoti spoštujejo.

EU je v **boju proti terorizmu** zaprla prostor, v katerem delujejo teroristi, sprejela nova pravila, ki jim otežujejo dostop do eksplozivov, strelnega orožja in financiranja, ter omejila njihovo gibanje. EU je okrepila **izmenjavo informacij**, da bi osebam, ki so v prvi liniji boja proti terorizmu, policistom in mejnim uslužbencem, zagotovila učinkovit dostop do točnih in popolnih podatkov, pri čemer je kar najbolje izkoristila obstoječe informacije ter zapolnila vrzeli in slepe pege. Močno varovanje zunanjih meja je prvi pogoj za varnost na območju prostega gibanja brez nadzora na notranjih mejah. Marca 2019 sta Evropski parlament in Svet dosegla dogovor o dodatno okrepljeni in popolnoma opremljeni **evropski mejni in obalni straži**, nova uredba pa naj bi začela veljati v začetku decembra 2019. EU je zagotovila platformo in financiranje za tiste, ki delujejo v lokalnih skupnostih, da bi si izmenjevali najboljše prakse **v boju proti radikalizaciji in za preprečevanje nasilnega ekstremizma**, poleg tega je predlagala nova pravila za učinkovito odstranjevanje terorističnih spletnih vsebin. EU je z akcijskimi načrti za pomoč pri varovanju javnih prostorov in izboljšanje pripravljenosti na kemična, biološka, radiološka in jedrska varnostna tveganja pomagala **mestom, da so postala odpornejša** na napade. EU je **kibernetsko varnost in grožnje, ki jih omogoča kibernetski prostor**, obravnavala s pripravo nove strategije EU za kibernetsko varnost in sprejetjem ustrezne zakonodaje ter bojem proti **dezinformacijam**, da bi bolje zaščitila naše volitve. EU še naprej izboljšuje varnost naše **kritične digitalne infrastrukture**, vključno z okrepljenim sodelovanjem za **kibernetsko varnost omrežij 5G** po vsej Evropi.

Ostaja nam še veliko dela. Napad na sinagogo in uboj dveh oseb v nemškem mestu Halle 9. oktobra 2019, ki je bil predvajan v živo, je bil pretresljiv opomnik na grožnjo, ki jo predstavljata skrajno desničarski nasilni ekstremizem in antisemitizem. Poleg tega je znova opozoril na zlorabo interneta za teroristično propagando in s tem **potrebo po vseevropskih pravilih za izbris terorističnih spletnih vsebin**. Svet za pravosodje in notranje zadeve je na zasedanju 7. in 8. oktobra 2019 razpravljal o desničarskem nasilnem ekstremizmu in terorizmu ter poudaril, da so potrebna nadaljnja prizadevanja, tudi na področju preprečevanja širjenja nezakonitih desničarskih ekstremističnih vsebin na spletu in drugod. Istočasno uboj treh policistov in še enega uslužbenca na sedežu policije v Parizu 3. oktobra 2019 kaže, da je grožnja islamističnega terorizma še vedno resnična in da si je treba še naprej

[1] COM(2015) 185 final (28. 4. 2015).
[2] COM(2016) 230 final (20.4.2016).
[3] Prejšnja poročila o napredku pri vzpostavljanju učinkovite in prave varnostne unije so na voljo na strani: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

prizadevati za pomoč državam članicam pri obravnavanju te grožnje. Pobeg članov organizacije ISIS/Daiš iz zapora med nedavnimi dogodki v severni Siriji bi lahko imel resne posledice za varnost v Evropi. Pomembno je, da države članice v celoti izkoristijo obstoječe informacijske sisteme za odkrivanje in identifikacijo tujih terorističnih borcev pri prehodu zunanjih meja. Poleg tega potekajo priprave za uporabo informacij z bojišča za pregon tujih terorističnih borcev.

V tem poročilu je opisan nedavni napredek pri prizadevanjih za učinkovito in pravo varnostno unijo, v njem pa so izpostavljena področja, na katerih je potrebno nadaljnje ukrepanje. Vsebuje najnovejše informacije o izvajanju dogovorjenih ukrepov **za kibernetsko varnost omrežij 5G**, zlasti v zvezi s **poročilom EU o oceni tveganja**, ki je bilo objavljeno 9. oktobra 2019, ter **bojem proti dezinformacijam**.

To poročilo se osredotoča zlasti na **zunanjo razsežnost** sodelovanja v varnostni uniji s podpisom dveh dvostranskih **dogovorov o boju proti terorizmu** z Albanijo in Republiko Severno Makedonijo ter napredkom pri sodelovanju s partnerji iz tretjih držav na področju izmenjave podatkov iz **evidence podatkov o potnikih**. Poleg tega je Komisija skupaj s tem poročilom sprejela tudi zahtevo za odobritev začetka pogajanj o sporazumu med EU in **Novo Zelandijo** o izmenjavi osebnih podatkov v boju proti hudim kaznivim dejanjem in terorizmu.

II. DOSEGANJE REZULTATOV PRI ZAKONODAJNIH PREDNOSTNIH NALOGAH

1. Preprečevanje radikalizacije na spletu in v skupnostih

Preprečevanje radikalizacije je temelj odziva Unije na grožnje, ki jih predstavlja terorizem. Pri tem je internet najpomembnejše bojno polje za delovanje teroristov v 21. stoletju. Prostor, v katerem lahko radikalizirani posamezniki komunicirajo in si izmenjujejo vsebine, omogoča razvoj in širjenje mrež islamističnih in desničarskih nasilnih skrajnežev po vsem svetu. Zato Komisija nadaljuje svoj dvotirni pristop k boju proti spletni radikalizaciji, v okviru katerega bi morala predlagana pravila o odstranjevanju nezakonitih terorističnih spletnih vsebin okrepiti prostovoljno partnerstvo s spletnimi platformami.

Pri tem je bistven **zakonodajni predlog za preprečevanje razširjanja terorističnih spletnih vsebin** z jasnimi pravili in zaščitnimi ukrepi, na podlagi katerih bi bilo obvezno, da internetne platforme v eni uri po prejemu utemeljene zahteve pristojnih organov odstranijo teroristične vsebine ter sprejmejo proaktivne ukrepe, sorazmerne s stopnjo izpostavljenosti terorističnim vsebinam[4]. Med Evropskim parlamentom in Svetom potekajo medinstitucionalna pogajanja s prvim trialogom 17. oktobra 2019. Glede na grožnjo, ki jo predstavljajo teroristične spletne vsebine, Komisija poziva sozakonodajalca, naj do konca leta 2019 dosežeta dogovor o predlagani zakonodaji.

Predlagana zakonodaja dopolnjuje prostovoljno partnerstvo z internetno industrijo in drugimi zainteresiranimi stranmi na **internetnem forumu EU**. Forum vse od ustanovitve leta 2015 spodbuja internetna podjetja, da proaktivno prepoznavajo in odstranjujejo teroristične spletne vsebine, pri čemer je utiral pot pobudi industrije za „skupno podatkovno zbirko ključnikov“[5] in ustanovitvi svetovnega internetnega foruma za boj proti terorizmu. Enota EU za prijavljanje internetnih vsebin, ki je del agencije Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Europol), je imela ključno vlogo pri krepitvi sodelovanja z internetnimi podjetji in prispevanju k splošnim ciljem internetnega foruma EU. Na zadnjem ministrskem srečanju internetnega foruma EU 7. oktobra 2019 so se države članice EU in visoki predstavniki internetnih podjetij zavezali k sodelovanju v okviru t. i. **kriznega protokola EU**. Krizni protokol EU določa prage za okrepljeno

[4] COM(2018) 640 final (12. 9. 2018).

[5] Orodje, ki ga je vzpostavil konzorcij podjetij za olajšanje sodelovanja, da se prepreči razširjanje terorističnih vsebin prek platform.

sodelovanje in uvaja nove načine za izboljšanje odzivanja na krize. To je del prizadevanj na mednarodni ravni za izvajanje „poziva iz Christchurcha za ukrepanje“[6], da bi se zagotovilo usklajeno in hitro odzivanje za zajezitev širjenja terorističnih ali nasilnih ekstremističnih spletnih vsebin.

Poleg ukrepov proti radikalizaciji na spletu Komisija še naprej podpira prizadevanja na nacionalni in lokalni ravni tako za **preprečevanje radikalizacije kot za boj proti njej na terenu**. Na podlagi bogatih izkušenj in strokovnega znanja, pridobljenih v okviru mreže za ozaveščanje o radikalizaciji, ponuja EU lokalnim akterjem[7], vključno z mesti, ciljno usmerjeno podporo ter zagotavlja priložnosti za izmenjavo izkušenj in znanja med strokovnimi delavci, raziskovalci in oblikovalci politik. Mreža je na primer izdala posebne smernice in organizirala delavnice za podporo pristojnim organom pri delu z otroki, ki so prišli s konfliktnih območij.[8] Za zagotovitev neprekinjenega opravljanja dejavnosti v okviru mreže za ozaveščanje o radikalizaciji je Komisija začela postopek za novo okvirno pogodbo v ocenjeni vrednosti 61 milijonov EUR za obdobje štirih let, z začetkom leta 2020[9].

Za preprečevanje grožnje, ki jo predstavljajo teroristične spletne vsebine, Komisija poziva Evropski parlament in Svet, naj:

- pred koncem leta zaključita pogajanja o zakonodajnem predlogu za preprečevanje širjenja **terorističnih spletnih vsebin**.

2. Trdnejši in pametnejši informacijski sistemi za upravljanje varnosti, meja in migracij

EU je pospešila izmenjavo informacij, s čimer je olajšala boj proti identitetnim prevaram[10], okrepila mejne kontrole[11], posodobila vseevropske podatkovne baze organov kazenskega pregona[12], zapolnila

6 Francoski predsednik Emmanuel Macron in predsednica vlade Nove Zelandije Jacinda Ardern sta v odziv na napade v Christchurchu na Novi Zelandiji 15. marca 2019 povabila voditelje in spletne platforme v Pariz, 15. maja 2019, da bi začela „poziv iz Christchurcha za ukrepanje“. Predsednik Juncker je podprl poziv in napovedal pripravo kriznega protokola EU.

7 Za sodelovanje z mesti na področju varnosti glej tudi oddelek V.2 o pripravljenosti in varovanju ter zlasti o varovanju javnih prostorov.

8 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_en.pdf.

9 Okvirna pogodba je razdeljena v dva sklopa: 29 000 000 EUR za podporo dejavnostim mreže za ozaveščanje o radikalizaciji za naslednja štiri leta in 32 000 000 EUR za izboljšanje zmogljivosti držav članic, nacionalnih, regionalnih in lokalnih organov ter prednostnih tretjih držav za učinkovit boj proti radikalizaciji, zlasti z zagotavljanjem priložnosti za mreženje, usmerjenih storitev na podlagi potreb ter raziskav in analiz.

10 Uredba (EU) 2019/1157 z dne 20. junija 2019 o okrepitvi varnosti osebnih izkaznic državljanov Unije in dokumentov za prebivanje, izdanih državljanom Unije in njihovim družinskim članom, ki uresničujejo svojo pravico do prostega gibanja.

11 Uvedba sistematičnih kontrol na zunanjih mejah za vse državljane, ki uporabljajo schengenski informacijski sistem. Vse schengenske države ter Romunija, Bolgarija, Hrvaška in Ciper uporabljajo pravila o sistematičnih preverjanjih v ustreznih podatkovnih zbirkah na zunanjih mejah, ki so bila uvedena aprila 2017. Ta pravila dopuščajo začasna odstopanja na kopenskih ali morskih mejah, vendar le v zvezi z državljani EU, saj imajo nesorazmeren vpliv na pretok prometa. Trenutno je takšna odstopanja priglasilo šest držav članic/pridruženih schengenskih držav (Hrvaška, Finska, Madžarska, Latvija, Norveška in Slovenija). Za zračne meje je možnost odstopanja od pravil o sistematičnih preverjanjih prenehala veljati aprila 2019.

12 Okrepljeni schengenski informacijski sistem (Uredba (EU) 2018/1860 z dne 28. 11. 2018, Uredba (EU) 2018/1861 z dne 28. 11. 2018, Uredba (EU) 2018/1862 z dne 28. 11. 2018 in evropski informacijski sistem kazenskih evidenc, razširjen na državljane tretjih držav (Uredba (EU) 2019/816 z dne 17. 4. 2019. Krepitev schengenskega informacijskega sistema vključuje splošno obveznost, da se v sistem vnesejo razpisi ukrepov, povezanih s terorizmom.

informacijske vrzeli[13] in okrepila agencijo Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Europol)[14]. V središču tega je **interoperabilnost informacijskih sistemov EU**[15], kar pomeni, da je treba kar najbolje izkoristiti obstoječe informacije in odpraviti slepe pege. Interoperabilnost se odziva na potrebe tistih, ki delajo na prvi liniji, saj uslužbencem organov kazenskega pregona, mejnim uradnikom in uradnikom za migracije omogoča hitrejši in bolj sistematičen dostop do informacij, s čimer prispeva k izboljšanju notranje varnosti in upravljanja meja.

Vendar pa bodo interoperabilnost in vse inovacije, ki jih prinaša, pustile svoj pečat pri upravljanju varnosti, meja in migracij na terenu le, če vsaka država članica v celoti sprejme s tem povezano zakonodajo. Zato je **izvajanje** interoperabilnosti glavna prednostna naloga varnostne unije, tako na politični kot na tehnični ravni. Komisija in Agencija Evropske unije za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice (eu-LISA) podpirata države članice s strokovnim znanjem in izmenjavo najboljših praks, pri čemer uporabljata mrežo nacionalnih koordinatorjev ter razvijata pregled stanja za učinkovito spremljanje in usklajevanje. Tesno sodelovanje med agencijami EU, vsemi državami članicami in pridruženimi schengenskimi državami bo ključnega pomena, da bi dosegli ambiciozen cilj popolne interoperabilnosti informacijskih sistemov EU za upravljanje varnosti, meja in migracij do leta 2020.

Medtem morata Evropski parlament in Svet še **dokončati zakonodajno delo** na tem področju. Hiter dogovor o vseh odprtih zakonodajnih predlogih je bistven za zagotovitev popolne in pravočasne uvedbe interoperabilnosti. Prvič, pri tehničnem izvajanju **Evropskega sistema za potovalne informacije in odobritve** obstaja potreba po tehničnih spremembah povezanih uredb[16], da se sistem vzpostavi v celoti. Komisija poziva Evropski parlament, naj pospeši svoje delo v zvezi s temi tehničnimi spremembami, da bi se čim prej začela medinstitucionalna pogajanja. Drugič, medinstitucionalna pogajanja v zvezi s predlogom iz maja 2018 za okrepitev in nadgradnjo obstoječega **vizumskega informacijskega sistema**[17] še vedno potekajo. Komisija na podlagi prvega trialoga, ki je potekal 22. oktobra 2019, poziva oba sozakonodajalca, naj čim prej zaključita pogajanja. Tretjič, še vedno ni bil dosežen dogovor o predlogu Komisije iz maja 2016 o razširitvi področja uporabe sistema **Eurodac**[18], da se v njem ne bodo shranjevali le prstni odtisi in ustrezni podatki prosilcev za azil in oseb, prijetih zaradi nezakonitega vstopa na zunanji meji, ampak tudi državljanov tretjih držav, ki nezakonito prebivajo v EU. Predlagane spremembe bi tudi podaljšale obdobje hrambe prstnih odtisov in ustreznih podatkov o osebah, ki nezakonito vstopajo v EU. Komisija poziva sozakonodajalca, naj sprejmeta predlog.

Komisija za okrepitev informacijskih sistemov EU za upravljanje varnosti, meja in migracij poziva Evropski parlament in Svet, naj:

- pospešita prizadevanja za hiter dogovor o predlaganih tehničnih spremembah, ki so potrebne za vzpostavitev **Evropskega sistema za potovalne informacije in odobritve**;
- hitro izvedeta in zaključita pogajanja o predlogu za okrepitev obstoječega **vizumskega**

[13] Sistem vstopa/izstopa EU (Uredba (EU) 2017/2226 (30. 11. 2017) in Evropski sistem za potovalne informacije in odobritve (Uredba (EU) 2018/1240 (12. 9. 2018) ter Uredba (EU) 2018/1241 (12. 9. 2018)).

[14] Vloga Europola se je v zadnjih letih znatno okrepila, tako glede področij pristojnosti kot glede globine. Agencija je bila leta 2016 okrepljena s sprejetjem uredbe o Europolu (Uredba (EU) 2016/794 (11. 5. 2016)). Države članice so znatno povečale količino informacij, ki jih izmenjujejo z Europolom in prek njega. Ustanovitev Evropskega centra za boj proti terorizmu (ECTC) je okrepila analitične zmogljivosti Europola v zadevah, povezanih s terorizmom. Proračun Europola se je v zadnjih letih dosledno povečeval, in sicer z 82 milijonov EUR leta 2014 na 138 milijonov EUR leta 2019. Pogajanja o proračunu za leto 2020 še potekajo.

[15] Uredba (EU) 2019/817 (20. 5. 2019) in Uredba (EU) 2019/818 (20. 5. 2019).

[16] Uredba (EU) 2018/1240 in Uredba (EU) 2018/1241 z dne 12. 9. 2018.

[17] COM (2018) 302 final (16. 5. 2018).

[18] COM (2016) 272 final (4. 5. 2016).

informacijskega sistema;

- sprejmeta zakonodajni predlog o sistemu **Eurodac** *(prednostna naloga iz skupne izjave*);

3. Omejitev možnosti delovanja teroristov

EU je sprejela odločne ukrepe za zaprtje prostora, v katerem delujejo teroristi, z novimi pravili, ki teroristom in drugim storilcem kaznivih dejanj otežujejo dostop do eksplozivov[19], strelnega orožja in financiranja[20] ter omejujejo njihovo gibanje[21].

Za okrepitev pravosodnega odziva na terorizem je Agencija EU za pravosodno sodelovanje v kazenskih zadevah (Eurojust) 1. septembra 2019 ustanovila **evropski sodni register za boj proti terorizmu**. V registru se bodo zbirale sodne informacije za vzpostavitev povezav v postopkih proti osumljencem terorističnih kaznivih dejanj, s čimer se bo okrepilo usklajevanje med tožilci pri protiterorističnih preiskavah z morebitnimi čezmejnimi posledicami.

Vendar so potrebna nadaljnja prizadevanja za podporo in olajšanje preiskav v čezmejnih primerih, zlasti kar zadeva **dostop** organov kazenskega pregona **do elektronskih dokazov**. Kar zadeva zakonodajne predloge iz aprila 2018 za izboljšanje čezmejnega dostopa do elektronskih dokazov v kazenskih preiskavah[22], mora Evropski parlament še sprejeti svoja pogajalskega stališča, preden lahko sozakonodajalca začneta pogajanja. Komisija poziva Evropski parlament, naj nadaljuje ta zakonodajni predlog, da ga bosta sozakonodajalca lahko hitro sprejela. Komisija na podlagi svojega predloga za notranja pravila EU sodeluje tudi pri **mednarodnih pogajanjih** za izboljšanje čezmejnega dostopa do elektronskih dokazov. Komisija in organi Združenih držav Amerike so 25. septembra 2019 izvedli prvi krog uradnih pogajanj o sporazumu med **EU in ZDA o čezmejnem dostopu do elektronskih dokazov**. Drugi krog je predviden za 6. november 2019. Komisija je v okviru tekočih pogajanj o **Drugem dodatnem protokolu h Konvenciji Sveta Evrope o kibernetski kriminaliteti iz Budimpešte** v imenu Unije sodelovala na treh pogajalskih zasedanjih julija, septembra in oktobra 2019. Čeprav je bil na teh pogajanjih dosežen precejšen napredek, ostajajo odprta številna vprašanja, ki so pomembna za Unijo, kot so zaščitni ukrepi za varstvo podatkov. Pogajanja o drugem dodatnem protokolu se bodo nadaljevala novembra 2019 in tekom leta 2020. Pomembno je, da se pogajanja hitro nadaljujejo, da se pospeši mednarodno sodelovanje pri izmenjavi elektronskih dokazov, hkrati pa se zagotovi skladnost z zakonodajo EU in obveznostmi držav članic iz nje, pri čemer je treba upoštevati tudi prihodnji razvoj prava EU.

Evropski parlament je 19. septembra 2019 sprejel **resolucijo o stanju glede izvajanja zakonodaje Unije za preprečevanje pranja denarja**[23], s katero odgovarja na sveženj štirih poročil o preprečevanju pranja denarja, ki jih je Komisija sprejela 24. julija 2019[24]. Evropski parlament je pozval države članice, naj zagotovijo ustrezno in hitro izvajanje direktiv o preprečevanju pranja denarja. Evropski parlament je tudi pozval Komisijo, naj oceni, ali bi bila uredba o preprečevanju

---

19 Uredba (EU) 2019/1148 z dne 20. junija 2019 o trženju in uporabi predhodnih sestavin za eksplozive. Uredba je začela veljati 31. julija 2019 in se začne uporabljati 18 mesecev po začetku veljavnosti.

20 Direktiva (EU) 2019/1153 z dne 11. 7. 2019 o določitvi pravil za lažjo uporabo finančnih in drugih informacij za namene preprečevanja, odkrivanja, preiskovanja ali pregona nekaterih kaznivih dejanj.

21 Uvedba sistematičnih kontrol na zunanjih mejah za vse državljane, ki uporabljajo schengenski informacijski sistem.

22 COM(2018) 225 final (17. 4. 2018) in COM(2018) 226 final (17. 4. 2018).

23 http://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_SL.html.

24 Poročilo o oceni tveganja pranja denarja in financiranja terorizma, ki vpliva na notranji trg in je povezano s čezmejnimi dejavnostmi (COM(2019) 370 (24. 7. 2019)), Poročilo o medsebojnem povezovanju nacionalnih centraliziranih avtomatiziranih mehanizmov (osrednji registri ali osrednji elektronski sistemi za pridobivanje podatkov) (COM(2019) 372 final (24. 7. 2019)), Poročilo o oceni nedavnih domnevnih primerov pranja denarja, v katere so bile vpletene kreditne institucije EU (COM(2019) 373 final (24.7. 2019)), Poročilo o oceni okvira za sodelovanje med finančnoobveščevalnimi enotami (COM(2019) 371 final (24. 7. 2019)).

pranja denarja primernejša od direktive, ter potrebo po mehanizmu usklajevanja in podpore za finančnoobveščevalne enote.

Da bi se izboljšal dostop organov kazenskega pregona do elektronskih dokazov, Komisija poziva Evropski parlament Svet, naj:
• hitro dosežeta dogovor o zakonodajnih predlogih o **elektronskih dokazih** (*prednostna naloga iz skupne izjave*) .

4. Krepitev kibernetske varnosti

Krepitev kibernetske varnosti ostaja ključni vidik prizadevanj za resnično in učinkovito varnostno unijo. Unija je z izvajanjem strategije EU za kibernetsko varnost iz leta 2017[25] okrepila svojo odpornost tako, da je napadalcem otežila možnosti za napade in omogočila hitrejše okrevanje, poleg tega je tudi poskrbela za odvračanje od napadov, saj je povečala verjetnost, da bodo napadalci ujeti in kaznovani, med drugim prek okvira za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti. Unija poleg tega podpira države članice pri kibernetski obrambi z izvajanjem okvira politike EU za kibernetsko obrambo[26].

Z začetkom veljavnosti uredbe o kibernetski varnosti[27] junija 2019 se oblikuje **certifikacijski okvir EU za kibernetsko varnost**. Certificiranje ima ključno vlogo pri povečanju zaupanja in varnosti izdelkov in storitev, ki so ključnega pomena za enotni digitalni trg. Certifikacijski okvir bo zagotovil vseevropske sheme certificiranja kot celovit sklop pravil, tehničnih zahtev, standardov in postopkov. Vključuje dve strokovni skupini, in sicer evropsko certifikacijsko skupino za kibernetsko varnost, ki zastopa organe držav članic, in certifikacijsko skupino deležnikov za kibernetsko varnost, ki zastopa industrijo. Slednja združuje tako strani, ki povprašujejo po izdelkih in storitvah informacijske in komunikacijske tehnologije, kot strani, ki jih ponujajo, vključno z malimi in srednjimi podjetji, ponudniki digitalnih storitev, evropskimi in mednarodnimi organi za standardizacijo, nacionalnimi akreditacijskimi organi, nadzornimi organi za varstvo podatkov in organi za ugotavljanje skladnosti.

Evropski parlament in Svet morata v tem času še doseči dogovor o zakonodajni pobudi[28] za **Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost ter mrežo nacionalnih koordinacijskih centrov**. Cilj predloga je okrepiti zmogljivosti Unije na področju kibernetske varnosti s spodbujanjem evropskega tehnološkega in industrijskega ekosistema kibernetske varnosti ter z usklajevanjem in združevanjem povezanih virov. Komisija oba sozakonodajalca poziva, naj nadaljujeta in hitro zaključita medinstitucionalna pogajanja o tej prednostni pobudi za izboljšanje kibernetske varnosti.

Prizadevanja za izboljšanje kibernetske varnosti vključujejo podporo tako na nacionalni kot na regionalni ravni[29].

EU poleg ukrepov proti kibernetskim grožnjam, usmerjenim v sisteme in podatke, še naprej obravnava zapletene in večstranske izzive, ki jih predstavljajo **hibridne grožnje**. V Svetu je bila ustanovljena horizontalna delovna skupina za preprečevanje hibridnih groženj, da bi se izboljšala odpornost EU in njenih držav članic na hibridne grožnje ter podprli ukrepi za krepitev odpornosti družb na krize. Komisija in Evropska služba za zunanje delovanje podpirata ta prizadevanja v okviru skupnega okvira

[25] JOIN(2017) 450 final (13. 9. 2017).

[26] Okvir politike EU za kibernetsko obrambo (posodobitev iz leta 2018), ki ga je Svet sprejel 19. novembra 2018 (14413/18).

[27] Uredba (EU) 2019/881 (17. 4. 2019).

[28] COM(2018) 630 final (12.9.2018).

[29] Komisija na primer podpira medregionalno partnerstvo za inovacije na področju kibernetske varnosti, ki vključuje Bretanjo, Kastiljo in Leon, Severno Porenje-Vestfalijo, osrednjo Finsko in Estonijo, da bi razvila evropsko vrednostno verigo na področju kibernetske varnosti, s poudarkom na komercializaciji in širitvi.

o preprečevanju hibridnih groženj iz leta 2016[30] ter skupnega sporočila iz leta 2018[31] o povečanju odpornosti in krepitvi zmogljivosti za obravnavanje hibridnih groženj. Poleg tega Skupno raziskovalno središče pripravlja okvir „konceptualnega modela“ za opredelitev hibridnih groženj, katerega cilj je državam članicam in njihovim pristojnim organom pomagati opredeliti vrsto hibridnega napada, ki bi se lahko zgodil. Model obravnava način, kako akter (državni ali nedržavni) uporablja vrsto orodij (od dezinformacij do vohunjenja ali fizičnih operacij) na različnih področjih (gospodarskem, vojaškem, socialnem, političnem), s katerimi vpliva na tarčo, da bi dosegel različne cilje.

Za izboljšanje kibernetske varnosti Komisija poziva Evropski parlament in Svet, naj:

- hitro dosežeta dogovor glede zakonodajnega predloga o **Evropskem industrijskem, tehnološkem in raziskovalnem strokovnem centru za kibernetsko varnost ter mreži nacionalnih koordinacijskih centrov**.

III. KREPITEV VARNOSTI DIGITALNIH INFRASTRUKTUR

Omrežja pete generacije (5G) bodo prihodnja hrbtenica vedno bolj digitaliziranih gospodarstev in družb. Zadevajo milijarde predmetov in sistemov, tudi v ključnih sektorjih, kot so energetika, promet, bančništvo in zdravje, ter sisteme za industrijsko kontrolo, ki prenašajo občutljive informacije in podpirajo varnostne sisteme. Zagotavljanje kibernetske varnosti in odpornosti omrežij 5G je zato bistvenega pomena.

Države članice so ob podpori Komisije in Evropske agencije za kibernetsko varnost 9. oktobra 2019 v okviru usklajenega pristopa objavile poročilo o **usklajeni oceni tveganja za kibernetsko varnost v omrežjih 5G v EU**[32]. Ta pomembni korak je del izvajanja priporočila Komisije iz marca 2019 za zagotovitev visoke ravni kibernetske varnosti omrežij 5G po vsej EU[33]. Poročilo temelji na rezultatih nacionalnih ocen tveganja za kibernetsko varnost, ki so jih opravile vse države članice. Opredeljuje glavne grožnje in akterje, ki predstavljajo nevarnost, najobčutljivejša sredstva, glavne šibke točke (vključno s tehničnimi in drugimi vrstami šibkih točk) ter več strateških tveganj. Ta ocena je podlago za opredelitev ukrepov za zmanjšanje tveganj, ki se lahko uporabijo na nacionalni in evropski ravni.

V poročilu so opredeljeni številni pomembni **izzivi na področju kibernetske varnosti**, ki se bodo verjetno pojavili ali postali pomembnejši v omrežjih 5G. Ti varnostni izzivi so večinoma povezani s ključnimi *inovacijami* na področju tehnologije 5G, zlasti s pomenom programske opreme in široko paleto storitev in aplikacij, ki jih omogoča 5G, ter vlogo *dobaviteljev* pri izgradnji in delovanju omrežij 5G in stopnji odvisnosti od posameznih dobaviteljev. To pomeni, da so izdelki, storitve in dejavnosti dobaviteljev vse bolj del „površine za napade“ omrežij 5G. Poleg tega bo profil tveganja posameznih dobaviteljev postal še posebej pomemben, vključno z verjetnostjo, da je dobavitelj predmet interference iz države, ki ni članica EU.

V skladu s postopkom iz priporočila Komisije iz marca 2019 bi se morale države članice do 31. decembra 2019 dogovoriti o **naboru ukrepov za zmanjšanje tveganj**, namenjenem obravnavi opredeljenih tveganj za kibernetsko varnost na nacionalni ravni in ravni Unije. Komisija in Evropska služba za zunanje delovanje bosta s podobno mislečimi partnerji še naprej izmenjevali mnenja o kibernetski varnosti in odpornosti omrežij 5G. V zvezi s tem je Komisija v stiku z Natom za usklajeno oceno tveganja za kibernetsko varnost omrežij 5G.

---

30 JOIN(2016) 18 final (6. 4. 2016).

31 JOIN(2018) 16 final (13. 6. 2018).

32 Skupina pristojnih organov za sodelovanje je s pomočjo Komisije in Evropske agencije za kibernetsko varnost pripravila usklajeno oceno tveganja za kibernetsko varnost v omrežjih 5G v EU, kot je določeno v direktivi o varnosti omrežij in informacijskih sistemov (Direktiva (EU) 2016/1148 (6. 7. 2016)): https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

33 C(2019)2355 final (26. 3. 2019).

IV. BOJ PROTI DEZINFORMACIJAM IN ZAŠČITA VOLITEV PRED DRUGIMI GROŽNJAMI, KI JIH OMOGOČA KIBERNETSKI PROSTOR

EU je vzpostavila **okvir za usklajeno ukrepanje proti dezinformacijam**, ki v celoti spoštuje evropske vrednote in temeljne pravice[34]. V okviru akcijskega načrta proti dezinformacijam[35] še naprej potekajo prizadevanja za zaprtje prostora za dezinformacije, tudi za zaščito integritete volitev.

Za to je ključno sodelovanje z industrijo prek samoregulativnega **kodeksa ravnanja glede dezinformacij** za spletne platforme in oglaševalski sektor, ki se je začel uporabljati oktobra 2018[36]. Komisija je ocenila učinkovitost kodeksa po prvem letu njegove uporabe na podlagi letnih samoocenjevalnih poročil, ki so jih predložile spletne platforme in druge podpisnice kodeksa ter so bila objavljena 29. oktobra 2019 skupaj z izjavo Komisije[37]. Na splošno poročila kažejo odločna prizadevanja podpisnic, da bi izpolnile svoje zaveze.

Ukrepi, ki so jih sprejele platforme, ki so podpisale kodeks, se razlikujejo glede hitrosti in obsega v vseh petih stebrih zavez v okviru kodeksa. Na splošno je bil dosežen večji napredek pri zavezah, povezanih z evropskimi volitvami leta 2019, zlasti z onemogočanjem spodbud za oglaševanje in monetizacijo dezinformacij (steber 1), zagotavljanjem preglednosti političnega in tematskega oglaševanja (steber 2) ter zagotavljanjem integritete storitev boja proti lažnim računom in neavtentičnemu ravnanju (steber 3). Nasprotno pa je napredek pri zavezah za opolnomočenje potrošnikov (steber 4) in zavezah za krepitev vloge raziskovalne skupnosti, tudi prek ustreznega, z zasebnostjo skladnega dostopa do podatkovnih nizov, ki ga omogočijo platforme za raziskovalne namene (steber 5), omejen ali ga ni. Obstajajo tudi razlike v področju uporabe ukrepov, ki jih izvajajo posamezne platforme za uresničevanje svojih zavez, pa tudi razlike med državami članicami glede uporabe posameznih politik. Komisija še naprej sodeluje s podpisnicami kodeksa in drugimi zainteresiranimi stranmi, da bi pospešila ukrepe proti dezinformacijam.

Komisija in visoka predstavnica sta v okviru akcijskega načrta proti dezinformacijam v sodelovanju z državami članicami vzpostavili **sistem hitrega obveščanja** za boj proti dezinformacijam. Sistem hitrega obveščanja je institucijam EU in državam članicam omogočil izmenjavo informacij in analiz pred volitvami v Evropski parlament leta 2019 ter usklajevanje odzivov. To delo se je še okrepilo po volitvah, pri čemer se vsakodnevno odvijajo izmenjave na delovni ravni, različne države članice pa so organizirale tudi tri srečanja kontaktnih točk za hitro opozarjanje.

Še en praktičen korak za prepoznavanje dezinformacij je bilo delo **ekipe za strateško komuniciranje** (v nadaljnjem besedilu: ekipa StratComms), zlasti njene projektne skupine East Stratcom, ki vodi projekt „EUvsDisinfo“ za spremljanje in analizo proruskih dezinformacij ter odzivanje nanje[38]. Od začetka leta 2019 je prvi namenski proračun v višini 3 milijonov EUR omogočil pospešitev in razširitev tega dela, da vključuje spremljanje in analizo proruskih dezinformacij na spletu, v oddajah in družbenih medijih v 19 jezikih, od angleščine do srbščine in arabščine. Količina razkritih dejavnosti

---

34 Glej akcijski načrt proti dezinformacijam (JOIN(2018) 36 final (5. 12. 2018)).

35 JOIN(2019) 12 final (14. 6. 2019).

36 V skladu s kodeksom so se spletne platforme Google, Facebook, Twitter in Microsoft zavezale, da bodo preprečevale manipulativno uporabo svojih storitev s strani slabih akterjev, zagotavljale preglednost in javno razkritje političnega oglaševanja ter sprejele druge ukrepe za izboljšanje preglednosti, odgovornosti in zanesljivosti spletnega ekosistema. Poklicna združenja iz oglaševalskega sektorja so se prav tako zavezala k sodelovanju s platformami, da bi izboljšali nadzor nad prikazovanjem oglasov in razvili orodja za varnost blagovnih znamk, katerih namen je omejiti oglaševanje na spletnih mestih, ki širijo dezinformacije.

37 https://ec.europa.eu/commission/presscorner/detail/sl/statement_19_6166. Poleg Googla, Facebooka, Twitterja in Microsofta so podpisnice kodeksa tudi Mozilla, sedem združenj na evropski ravni ali nacionalni ravni, ki zastopajo oglaševalski sektor, ter EDiMA, evropsko združenje, ki zastopa platforme in druga tehnološka podjetja, dejavna v spletnem sektorju.

38 www.euvsdisinfo.eu.

dezinformiranja se je več kot podvojila zaradi izboljšanega spremljanja, pri čemer je bilo leta 2019 do zdaj odkritih približno 2 000 primerov dezinformacij v primerjavi s 765 primeri v istem obdobju leta 2018. Projektna skupina East Stratcom je imela ključno vlogo pri spremljanju in razkrivanju proruskih dezinformacij, usmerjenih v volitve v Evropski parlament leta 2019. Raziskave so bile povezane s kampanjo ozaveščanja o poskusih vmešavanja v volilne procese po svetu. V okviru ozaveščanja v tesnem sodelovanju z Evropskim parlamentom in Komisijo je bilo opravljenih več kot 20 medijskih intervjujev, v kampanji pa je sodelovalo več kot 300 novinarjev.

Komisija je sprejela tudi ukrepe za **zmanjšanje širjenja dezinformacij in mitov o institucijah in politikah EU**. Vzpostavila je mrežo strokovnjakov za komuniciranje s spletnim portalom, ki zagotavlja interaktivno informativno gradivo o politikah EU ter izzivu dezinformacij in njihovega vpliva na družbo. V sodelovanju z Evropskim parlamentom in Evropsko službo za zunanje delovanje je začela tudi vrsto kampanj v družbenih medijih, ki se osredotočajo na boj proti dezinformacijam[39].

V. IZVAJANJE DRUGIH PREDNOSTNIH DOSJEJEV NA PODROČJU VARNOSTI

1. Izvajanje zakonodajnih ukrepov na področju varnostne unije

Dogovorjeni ukrepi na področju varnostne unije bodo v celoti koristili varnosti le, če bodo vse države članice zagotovile njihovo hitro in popolno izvajanje. Zato Komisija dejavno podpira države članice pri izvajanju zakonodaje EU, vključno s financiranjem in omogočanjem izmenjave najboljših praks. Komisija v celoti uporablja svoja pooblastila v skladu s Pogodbama za izvrševanje prava EU, vključno z ustreznimi ukrepi za ugotavljanje kršitev.

Rok za prenos **direktive EU o evidenci podatkov o potnikih**[40] je potekel 25. maja 2018. Do danes je uradno obvestilo o popolnem prenosu poslalo 25 držav članic[41], kar je pomemben napredek od julija 2018, ko je Komisija začela postopke za ugotavljanje kršitev proti 14 državam članicam[42]. Dve državi članici kljub tekočim postopkom za ugotavljanje kršitev, ki so se začeli 19. julija 2018, še nista poslali uradnega obvestila o popolnem prenosu[43]. Hkrati Komisija vse države članice še naprej podpira pri prizadevanjih za dokončanje njihovih sistemov evidenc podatkov o potnikih, vključno s spodbujanjem izmenjave informacij in najboljših praks.

Rok za prenos **direktive o boju proti terorizmu**[44] se je iztekel 8. septembra 2018. Do danes je uradno obvestilo o popolnem prenosu poslalo 22 držav članic, kar je precejšen napredek od novembra 2018, ko je Komisija začela postopke za ugotavljanje kršitev proti 16 državam članicam[45]. Tri države članice kljub tekočim postopkom za ugotavljanje kršitev še niso poslale uradnega obvestila o popolnem prenosu[46]. Komisija je 25. julija 2019 poslala obrazloženo mnenje dvema državama članicama, ker nista poslali uradnega obvestila o popolnem prenosu direktive[47]. V odgovor sta obe državi članici

---

39 https://europa.eu/euprotects/.

40 Direktiva (EU) 2016/681 (27. 4. 2016). Danska ni sodelovala pri sprejetju te direktive, ki zato zanjo ni zavezujoča in ji je ni treba uporabljati.

41 Sklici na uradna obvestila o popolnem prenosu upoštevajo izjave držav članic in ne posegajo v preverjanje prenosa, ki ga izvajajo službe Komisije (stanje z dne 17. oktobra 2019).

42 Glej Šestnajsto poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije (COM(2018) 690 final (10. 10. 2018)).

43 Slovenija je poslala uradno obvestilo o delnem prenosu. Španija ni poslala uradnega obvestila o prenosu (stanje z dne 17. oktobra 2019).

44 Direktiva (EU) 2017/541 (15. 3. 2017). Direktiva se ne uporablja v Združenem kraljestvu, na Irskem in Danskem.

45 Glej Sedemnajsto poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije (COM(2018) 845 final (11. 12. 2018)).

46 Grčija in Luksemburg nista poslala uradnega obvestila o nacionalnih izvedbenih ukrepih. Poljska je poslala uradno obvestilo o nacionalnih ukrepih, ki so pomenili delni prenos (stanje z dne 17. oktobra 2019).

47 Grčija in Luksemburg.

napovedali, da bo zakonodajno delo zaključeno pred koncem tega leta.

Rok za prenos **direktive o nadzoru nabave in posedovanja orožja**[48] se je iztekel 14. septembra 2018. Do danes je uradno obvestilo o popolnem prenosu poslalo 13 držav članic. 15 držav članic kljub tekočim postopkom za ugotavljanje kršitev, ki so se začeli 22. novembra 2018, še ni poslalo uradnega obvestila o popolnem prenosu[49]. Komisija je 25. julija 2019 poslala obrazloženo mnenje 20 državam članicam, ker ji niso poslale uradnega obvestila o popolnem prenosu direktive. Pet držav članic je v odgovor poslalo uradno obvestilo o popolnem prenosu direktive[50].

Rok za prenos **direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj**[51] je potekel 6. maja 2018. Do danes je uradno obvestilo o popolnem prenosu poslalo 25 držav članic, kar je pomemben napredek od julija 2018, ko je Komisija začela postopke za ugotavljanje kršitev proti 19 državam članicam[52]. Tri države članice kljub tekočim postopkom za ugotavljanje kršitev še niso poslale uradnega obvestila o popolnem prenosu[53]. Komisija se je 25. julija 2019 odločila, da proti dvema državama članicama[54] sproži postopek pred Sodiščem Evropske unije zaradi neizvršitve prenosa direktive, in poslala uradni opomin eni državi članici,[55] ker ni v celoti prenesla direktive[56].

Komisija ocenjuje prenos **četrte direktive o preprečevanju pranja denarja**[57], hkrati pa tudi preverja, ali države članice izvajajo ta pravila. Direktivo so morale prenesti v nacionalno zakonodajo do 26. junija 2018. Komisija ohranja postopke za ugotavljanje kršitev zoper 21 držav članic, saj je ocenila, da obvestila, prejeta od držav članic, ne pomenijo popolnega prenosa te direktive[58].

Komisija je ocenila skladnost prenosa **direktiv v zvezi s kibernetsko kriminaliteto**. Julija in oktobra 2019 je začela postopke za ugotavljanje kršitev zoper 23 držav članic,[59] saj je ocenila, da nacionalna izvedbena zakonodaja, o kateri so uradno obvestilo poslale te države članice, ne pomeni pravilnega prenosa **direktive o boju proti spolni zlorabi otrok**[60]. Komisija je julija in oktobra 2019 začela tudi postopke za ugotavljanje kršitev proti štirim državam članicam,[61] saj je ocenila, da nacionalna izvedbena zakonodaja, o kateri so uradno obvestilo poslale te države članice, ne pomeni

48 Direktiva (EU) 2017/853 (17. 10. 2019).

49 Belgija, Češka, Estonija, Poljska, Švedska, Slovaška in Združeno kraljestvo so poslali uradno obvestilo o ukrepih za prenos dela novih določb. Ciper, Nemčija, Grčija, Španija, Luksemburg, Madžarska, Romunija in Slovenija niso poslali uradnega obvestila o kakršnih koli ukrepih za prenos (stanje z dne 17. oktobra 2019).

50 Finska, Irska, Litva, Nizozemska, Portugalska (stanje z dne 17. oktobra 2019).

51 Direktiva (EU) 2016/680 (27. 4. 2016).

52 Glej Šestnajsto poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije (COM(2018) 690 final (10. 10. 2018)).

53 Slovenija je poslala uradno obvestilo o delnem prenosu. Španija ni poslala uradnega obvestila o prenosu. Čeprav je Nemčija poslala uradno obvestilo o popolnem prenosu, Komisija meni, da ta prenos ni zaključen (stanje z dne 17. oktobra 2019).

54 Grčija in Španija.

55 Nemčija.

56 Grčija je poslala uradno obvestilo o popolnem prenosu, ki ga Komisija ocenjuje.

57 Direktiva (EU) 2015/849 (20. 5. 2015).

58 Belgija, Bolgarija, Češka, Danska, Nemčija, Estonija, Irska, Francija, Italija, Ciper, Latvija, Litva, Madžarska, Nizozemska, Avstrija, Poljska, Romunija, Slovaška, Finska, Švedska in Združeno kraljestvo (stanje z dne 17. oktobra 2019). Pred tem je bilo zaključenih 7 postopkov za ugotavljanje kršitev, povezanih z direktivo.

59 Belgija, Bolgarija, Češka, Nemčija, Estonija, Grčija, Španija, Francija, Hrvaška, Italija, Latvija, Litva, Luksemburg, Madžarska, Malta, Avstrija, Poljska, Portugalska, Romunija, Slovenija, Slovaška, Finska in Švedska.

60 Direktiva 2011/93/EU (13. 12. 2011).

61 Bolgarija, Italija, Portugalska in Slovenija.

pravilnega prenosa **direktive o napadih na informacijske sisteme**[62].

Komisija države članice poziva, naj nemudoma sprejmejo potrebne ukrepe za popoln prenos naslednjih direktiv v nacionalno zakonodajo in o tem obvestijo Komisijo:

- **direktiva EU o evidenci podatkov o potnikih**, v zvezi s katero ena država članica Komisije še ni poslala uradnega obvestila o prenosu v nacionalno zakonodajo, ena država članica pa še ni dopolnila priglasitve o prenosu[63];
- **direktiva o boju proti terorizmu**, v zvezi s katero dve državi članici še nista poslali uradnega obvestila o prenosu v nacionalno zakonodajo, ena država članica pa še ni dopolnila uradnega obvestila o prenosu[64];
- **direktiva o nadzoru nabave in posedovanja orožja**, v zvezi s katero osem držav članic še ni poslalo uradnega obvestila o prenosu v nacionalno zakonodajo, sedem držav članic pa še ni dopolnilo uradnega obvestila o prenosu[65];
- **direktiva o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj**, v zvezi s katero ena država članica še ni poslala uradnega obvestila o prenosu v nacionalno zakonodajo, dve državi članici pa še nista dopolnili uradnega obvestila o prenosu[66];
- **četrta direktiva o preprečevanju pranja denarja**, v zvezi s katero 21 držav članic še ni dopolnilo uradnega obvestila o prenosu[67];
- **direktiva o boju proti spolni zlorabi otrok**, v zvezi s katero so bili začeti postopki za ugotavljanje kršitev zaradi nepravilnega prenosa zoper 23 držav članic[68];
- **direktiva o napadih na informacijske sisteme**, v zvezi s katero so bili začeti postopki za ugotavljanje kršitev zaradi nepravilnega prenosa zoper štiri države članice[69].

2. Pripravljenost in varovanje

Krepitev odpornosti na varnostne grožnje je bistven del prizadevanj za učinkovito in pravo varnostno unijo. Komisija podpira države članice in lokalne organe pri krepitvi varovanja javnih prostorov, izvajanju akcijskega načrta iz oktobra 2017 in partnerstvu za varnost javnih prostorov iz januarja 2019 v okviru agende EU za mesta. To delo vključuje mesta, ki so se obrnila na Komisijo in zaprosila za podporo pri reševanju izzivov, s katerimi se spoprijemajo pri varovanju javnih prostorov.

Izmenjava najboljših praks med lokalnimi organi in z zasebnimi operaterji je ključnega pomena za krepitev varnosti javnih prostorov. To je bila osrednja tema **evropskega tedna varnosti** v Nici (Francija) med 14. in 18. oktobrom 2019, organiziranega v okviru projekta „Protect Allied Cities against Terrorism in Securing Urban Areas“ (Varovanje povezanih mest pred terorizmom z

62 Direktiva 2013/40/EU (12. 8. 2013).

63 Slovenija je poslala uradno obvestilo o delnem prenosu. Španija ni poslala uradnega obvestila o prenosu (stanje z dne 17. oktobra 2019).

64 Grčija in Luksemburg nista poslala uradnega obvestila o prenosu. Poljska je poslala uradno obvestilo o delnem prenosu (stanje z dne 17. oktobra 2019).

65 Belgija, Češka, Estonija, Poljska, Švedska, Slovaška in Združeno kraljestvo so poslali uradno obvestilo o ukrepih za prenos dela novih določb. Ciper, Nemčija, Grčija, Španija, Luksemburg, Madžarska, Romunija in Slovenija niso poslali uradnega obvestila o nobenih ukrepih za prenos (stanje z dne 17. oktobra 2019).

66 Slovenija je poslala uradno obvestilo o delnem prenosu. Španija ni poslala uradnega obvestila o prenosu. Čeprav je Nemčija poslala uradno obvestilo o popolnem prenosu, Komisija meni, da ta prenos ni zaključen (stanje z dne 17. oktobra 2019).

67 Belgija, Bolgarija, Češka, Danska, Nemčija, Estonija, Irska, Francija, Italija, Ciper, Latvija, Litva, Madžarska, Nizozemska, Avstrija, Poljska, Romunija, Slovaška, Finska, Švedska in Združeno kraljestvo (stanje z dne 17. oktobra 2019).

68 Belgija, Bolgarija, Češka, Nemčija, Estonija, Grčija, Španija, Francija, Hrvaška, Italija, Latvija, Litva, Luksemburg, Madžarska, Malta, Avstrija, Poljska, Portugalska, Romunija, Slovenija, Slovaška, Finska in Švedska.

69 Bolgarija, Italija, Portugalska in Slovenija.

izboljšanjem varnosti na mestnih območjih), ki ga financira EU. Na dogodku, na katerem se je zbralo 500 udeležencev iz mest iz vse Evrope, nacionalnih organov in raziskovalnih ustanov, sta bila poudarjena pomen tesnega sodelovanja med vsemi zainteresiranimi stranmi, tako javnimi kot zasebnimi, ter vloga novih tehnologij pri boljšem varovanju mest. Varovanje javnih prostorov je bilo poleg tega tema **evropskega tedna regij in mest** v Bruslju med 7. in 10. oktobrom 2019, na katerem je potekala tudi delavnica o agendi za mesta za partnerstvo EU za varnost javnih prostorov. Osredotočena je bila na vlogo lokalnih organov na področju varnostne politike, ureditve EU in financiranja pri reševanju glavnih varnostnih izzivov na mestnih javnih prostorih ter ključne teme, kot so inovacije prek pametnih rešitev in tehnologij, vključno z načelom vgrajene varnosti, preprečevanja in socialne vključenosti. Komisija k spodbujanju inovativnosti mest na teh področij prispeva tudi s svojim zadnjim razpisom za zbiranje predlogov v okviru pobude Inovativni ukrepi v mestih, rezultati katerega so bili objavljeni avgusta 2019. Med izbranimi projekti bodo nove rešitve za vprašanja varnosti v mestih preizkusila tri mesta (Pirej v Grčiji, Tampere na Finskem in Torino v Italiji)[70].

Za boljšo **zaščito verskih objektov** in preučitev potreb različnih verskih skupnosti je Komisija 7. oktobra 2019 organizirala sestanek s predstavniki judovskih, muslimanskih, krščanskih in budističnih skupnosti. V okviru izvajanja akcijskega načrta EU za podporo pri varovanju javnih prostorov iz leta 2017 je bilo na srečanju poudarjeno, da se ozaveščenost in pripravljenost na področju varnosti zelo razlikujeta med različnimi verskimi skupnostmi, kar kaže na pomen nadaljnje izmenjave dobrih praks. Srečanje je pokazalo tudi, da uvedba osnovnih varnostnih ukrepov in boljša ozaveščenost na področju varnosti nista nezdružljiva z ohranjanjem odprtega in dostopnega značaja verskih objektov. Komisija bo zbirala dobre prakse in gradivo za ozaveščanje na svoji elektronski platformi strokovnjakov ter z zadevo seznanila varnostne organe držav članic v okviru javno-zasebnega foruma za varovanje javnih prostorov.

Eno od posebnih področij, ki zahtevajo nadaljnjo pozornost, je vse večja varnostna grožnja za kritično infrastrukturo in javne prostore, ki jo predstavljajo **droni**. Komisija z dopolnitvijo nedavne zakonodaje EU[71] o varnem upravljanju dronov v zračnem prostoru, v katerem letijo zrakoplovi s posadko, podpira države članice pri sledenju trendom zlonamerne uporabe dronov, financiranju ustreznih raziskav in omogočanju testiranja protiukrepov, pri tem pa ne ogroža priložnosti za koristno uporabo dronov. Izmenjava izkušenj in najboljših praks je bistvenega pomena, kot je pokazala mednarodna konferenca na visoki ravni o boju proti grožnjam, ki jih predstavljajo sistemi brezpilotnih zrakoplovov, 17. oktobra 2019 v Bruslju. Na tem dogodku, ki ga je organizirala Komisija, se je zbralo 250 udeležencev iz držav članic, mednarodnih organizacij, partnerjev iz tretjih držav, industrije, akademskih krogov in civilne družbe, da bi razpravljali o varnostnih izzivih, ki jih predstavljajo droni, in načinih za njihovo reševanje. Na srečanju se je pokazala potreba po rednih ocenah tveganja, povezanega z droni, ter tesnem sodelovanju med letalskimi organi in organi kazenskega pregona pri nadaljnjem razvoju evropske zakonodaje o varnem upravljanju dronov. Obstaja tudi potreba po nadaljnjem preskušanju protiukrepov proti dronom z usklajenim evropskim pristopom. Poleg tega je bilo doseženo soglasje, da je za varno in operativno zanesljivo uporabo dronov, ki jih je težko uporabljati zlonamerno, nujno tesno sodelovanje med organi in industrijo.

3. Zunanja razsežnost

Ker večina varnostnih tveganj, s katerimi se spoprijema Unija, presega meje EU in predstavlja svetovne grožnje, ima sodelovanje s partnerskimi državami, organizacijami in ustreznimi zainteresiranimi stranmi ključno vlogo pri vzpostavljanju učinkovite in prave varnostne unije.

[70] Pobuda Inovativni ukrepi v mestih je instrument, ki ga sofinancira Evropski sklad za regionalni razvoj. Več informacij je na voljo na spletišču: https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals.

[71] Izvedbena uredba Komisije (EU) 2019/947 z dne 24. maja 2019 o pravilih in postopkih za upravljanje brezpilotnih zrakoplovov.

To sodelovanje temelji na izmenjavi informacij. Komisija je skupaj s tem poročilom sprejela priporočilo Svetu za odobritev začetka pogajanj o **sporazumu med EU in Novo Zelandijo o izmenjavi osebnih podatkov za boj proti hudim kaznivim dejanjem in terorizmu** med Europolom in pristojnimi organi Nove Zelandije. S takšnim sporazumom se bodo dodatno okrepile zmogljivosti Europola za sodelovanje z Novo Zelandijo pri preprečevanju kaznivih dejanj, ki spadajo v okvir ciljev Europola, in boju proti njim. Delovni dogovor med Europolom in novozelandsko policijo iz aprila 2019 sicer zagotavlja okvir za strukturirano sodelovanje na strateški ravni, ne pa tudi pravne podlage za izmenjavo osebnih podatkov. Izmenjava osebnih podatkov ob polnem spoštovanju prava in temeljnih pravic EU je bistvenega pomena za učinkovito operativno policijsko sodelovanje. Pred tem je Komisija opredelila osem prednostnih držav na Bližnjem vzhodu/v severni Afriki na podlagi teroristične grožnje, izzivov, povezanih z migracijami, in operativnih potreb Europola za začetek pogajanj[72]. Ob upoštevanju operativnih potreb organov kazenskega pregona po vsej EU in možnih koristi tesnejšega sodelovanja na tem področju, kar je razvidno tudi iz ukrepov po napadu v Christchurchu marca 2019, Komisija meni, da je treba Novo Zelandijo dodati kot prednostno državo, s katero je treba čim prej začeti pogajanja.

Še en temelj varnostnega sodelovanja Unije s partnerji iz tretjih držav je prenos **podatkov iz evidence podatkov o potnikih**. Komisija je 27. septembra 2019 sprejela priporočilo Svetu o odobritvi začetka pogajanj o sporazumu **med EU in Japonsko** o prenosu podatkov iz evidence podatkov o potnikih za preprečevanje terorizma in hudih mednarodnih kaznivih dejanj ter boj proti njim, pri čemer bodo v celoti spoštovani zaščitni ukrepi za varstvo podatkov in temeljne pravice[73]. Priporočilo se preučuje v delovni skupini Sveta in Komisija poziva Svet, naj čim prej sprejme mandat za pogajanja z Japonsko. Dogovor bi bilo z vidika varnosti dobro doseči do olimpijskih iger leta 2020.

Na svetovni ravni Komisija podpira delo, ki ga **Mednarodna organizacija civilnega letalstva** opravlja pri pripravi standarda za obdelavo podatkov iz evidence podatkov o potnikih. To je odgovor na poziv iz Resolucije Varnostnega sveta Združenih narodov št. 2396, naj vse države članice Združenih narodov razvijejo zmogljivosti za zbiranje, obdelavo in analizo podatkov iz evidence podatkov o potnikih. Komisija je 13. septembra 2019 predstavila predlog[74] sklepa Sveta o stališču, ki naj se v imenu EU zastopa v Mednarodni organizaciji civilnega letalstva glede standardov in priporočenih praks v zvezi s podatki iz evidence podatkov o potnikih. Predlog se preučuje v delovni skupini Sveta in Komisija poziva k hitremu sprejetju sklepa Sveta. Stališče Unije in njenih držav članic je bilo predstavljeno tudi v informativnem dokumentu o standardih in načelih za zbiranje, uporabo, obdelavo in varstvo podatkov iz evidence podatkov o potnikih, ki je bil predložen na 40. zasedanju skupščine Mednarodne organizacije civilnega letalstva.

Komisija si prizadeva za hitro sklenitev sporazuma o evidenci podatkov o potnikih s **Kanado**. Medtem sta se poleti začela izvajati skupni pregled in skupna ocena sporazuma o evidenci podatkov o potnikih z **Avstralijo**, pa tudi skupna ocena sporazuma o evidenci podatkov o potnikih z **Združenimi državami**, začenši z obiski v Canberri in Washingtonu avgusta oziroma septembra 2019. Komisija je 14. oktobra 2019 na zaprti seji obvestila Odbor za državljanske svoboščine, pravosodje in notranje zadeve Evropskega parlamenta o stanju sodelovanja z Japonsko, Avstralijo in Kanado v zvezi s podatki iz evidence podatkov o potnikih.

Prav tako je bil z izvajanjem skupnega akcijskega načrta o boju proti terorizmu na Zahodnem Balkanu iz oktobra 2018 dosežen napredek pri varnostnem sodelovanju s partnericami z **Zahodnega Balkana**. Komisija je 9. oktobra podpisala dva nezavezujoča dvostranska sporazuma o boju proti terorizmu z

[72] Glej Enajsto poročilo o napredku pri vzpostavljanju učinkovite in prave varnostne unije (COM(2017) 608 final (18. 10. 2017)). Prednostne države so Alžirija, Egipt, Izrael, Jordanija, Libanon, Maroko, Tunizija in Turčija.

[73] COM(2019) 420 final (27. 9. 2019).

[74] COM(2019) 416 final (13. 9. 2019).

Albanijo in Republiko Severno Makedonijo[75]. V teh dogovorih so določeni prilagojeni prednostni ukrepi, ki naj bi jih sprejeli organi posamezne partnerske države in ki zajemajo pet ciljev skupnega akcijskega načrta[76] ter kažejo podporo, ki jo namerava zagotoviti Komisija. Podobne ureditve s preostalimi partnericami z Zahodnega Balkana bodo predvidoma podpisane v prihodnjih tednih. Poleg tega je Komisija 7. oktobra 2019 s Črno goro podpisala sporazum o sodelovanju med Črno goro in Evropsko agencijo za mejno in obalno stražo (Frontex) pri upravljanju meja. Ta sporazum agenciji omogoča, da Črni gori pomaga pri upravljanju meja ter posledično pri spopadanju z nezakonitimi migracijami in čezmejnimi kaznivimi dejanji, s čimer se krepi varnost na zunanjih mejah EU.

Za okrepitev sodelovanja s partnerskimi državami pri obvladovanju skupnih varnostnih groženj Komisija poziva Svet, naj:

- sprejme pooblastilo za začetek pogajanj o sporazumu med EU in **Novo Zelandijo** o izmenjavi osebnih podatkov za boj proti hudim kaznivim dejanjem in terorizmu;
- sprejme pooblastilo za začetek pogajanj o sporazumu med EU in **Japonsko** o prenosu podatkov iz evidence podatkov o potnikih;
- sprejme predlagani **sklep Sveta o stališču, ki naj se v imenu EU zastopa v Mednarodni organizaciji civilnega letalstva** glede standardov in priporočenih praks v zvezi s podatki iz evidence podatkov o potnikih.

VI. SKLEP

To poročilo navaja širok nabor ukrepov, ki jih je EU sprejela za obravnavanje skupnih groženj v Evropi in krepitev naše kolektivne varnosti. Napredek pri vzpostavljanju učinkovite in prave varnostne unije, ki temelji na skupnem razumevanju, da je današnje varnostne izzive najbolje reševati skupaj in v sodelovanju s tretjimi državami, je rezultat tesnega sodelovanja med različnimi akterji, krepitve zaupanja, delitve virov in skupnega spopadanja z grožnjami: na vseh ravneh upravljanja, od mest in drugih lokalnih akterjev, regij in nacionalnih organov do EU z Evropskim parlamentom in Svetom; z vključevanjem javnih organov, agencij EU, zasebnih akterjev in civilne družbe ter uporabo strokovnega znanja, orodij in virov na različnih področjih politike, kot so prometna politika, enotni digitalni trg in kohezijska politika. Pri tem je delo na področju varnostne unije del varstva temeljnih pravic ter varovanja in spodbujanja naših vrednot.

Nadaljevati moramo delo v smeri učinkovite in prave varnostne unije. Čim prej je treba doseči dogovor o še ne sprejetih pomembnih pobudah, zlasti o: (1) zakonodajnem predlogu o odstranjevanju terorističnih vsebin na spletu, (2) zakonodajnem predlogu o izboljšanju dostopa do elektronskih dokazov za organe kazenskega pregona, (3) zakonodajnem predlogu o ustanovitvi Evropskega industrijskega, tehnološkega in raziskovalnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov ter (4) odprtih zakonodajnih predlogih o trdnejših in pametnejših informacijskih sistemih za upravljanje varnosti, meja in migracij. Dogovorjene ukrepe in instrumente je treba dejansko uporabiti na terenu s pravočasnim in doslednim izvajanjem zakonodaje EU v vseh državah članicah, da bi izkoristili vse njihove koristi za varnost. Zlasti je bistveno, da vse države članice izvajajo nedavno sprejeto zakonodajo o interoperabilnosti informacijskih sistemov EU za upravljanje varnosti, meja in migracij, da bi dosegli ambiciozen cilj polne interoperabilnosti do leta 2020. Poleg tega mora biti Evropa ostati pozorna na nastajajoče in spreminjajoče se grožnje ter si še naprej skupaj prizadevati za večjo varnost vseh državljanov in državljank.

[75] https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en.

[76] Skupni akcijski načrt predvideva ukrepe v okviru naslednjih petih ciljev: trdnega okvira za boj proti terorizmu, učinkovitega preprečevanja nasilnega ekstremizma in boja proti njemu, učinkovite izmenjave informacij in operativnega sodelovanja, krepitve zmogljivosti za boj proti pranju denarja in financiranju terorizma, krepitve zaščite državljanov in državljank ter infrastrukture.