EVROPSKA
KOMISIJA

Bruselj, 24.7.2019
COM(2019) 353 final

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, EVROPSKEMU SVETU IN SVETU

Devetnajsto poročilo o nadaljnjem napredku pri vzpostavljanju učinkovite in prave varnostne unije

I. UVOD

To je devetnajsto mesečno poročilo o nadaljnjem 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, ter krepitve naše zaščite in odpornosti proti tem grožnjam.

Evropejci od Unije pričakujejo, da jih bo zaščitila. Za Junckerjevo Komisijo je varnost že od prvega dne glavna prednostna naloga. V „Novi strateški agendi 2019–2024“ Evropskega sveta je cilj „zaščita državljanov in svoboščin“ na vrhu štirih poglavitnih prednostnih nalog za Unijo[1]. Evropski svet je nadalje napovedal, da bodo nadaljevali in krepili prizadevanja Unije v boju proti terorizmu in čezmejnim kaznivim dejanjem, vključno z izboljševanjem sodelovanja in izmenjave informacij ter nadaljnjim razvojem skupnih instrumentov.

EU je zaradi tesnega sodelovanja med Evropskim parlamentom, Svetom in Komisijo dosegla znaten napredek pri skupnih prizadevanjih za učinkovito in pravo varnostno unijo, pri čemer je vzpostavila več prednostnih zakonodajnih pobud in izvedla najrazličnejše nezakonodajne ukrepe za podporo njenim državam članicam in povečanje varnosti za vse državljane[2]. Unija je sprejela odločilne ukrepe za zaprtje prostora, v katerem delujejo teroristi in storilci kaznivih dejanj, saj je s prepovedjo nabave in uporabe določenega strelnega orožja in eksploziva ter omejevanjem dostopa do financiranja teroristom odvzela sredstva za izvajanje napadov. EU je tudi okrepila izmenjavo informacij med državami članicami ter odpravila informacijske vrzeli in pomanjkljivosti, ob tem pa sprejela ukrepe za boj proti radikalizaciji, za zaščito Evropejcev na spletu, reševanje kibernetskih groženj in groženj, ki jih omogoča kibernetski prostor, ter krepitev upravljanja zunanjih meja Unije in mednarodnega sodelovanja na področju varnosti.

Hkrati je na področju varnostne unije še vedno več prednostnih pobud, ki jih sozakonodajalca še nista sprejela. V tem poročilu, pripravljenem po sestavi 9. sklica Evropskega parlamenta 2. julija 2019:

- je navedeno, na katerih področjih sozakonodajalca zahtevata ukrepanje za odpravo neposrednih groženj. Zlasti je treba nujno sprejeti ukrepe za **boj proti teroristični propagandi in radikalizaciji na spletu**;
- so določene še nesprejete prednostne pobude na področju varnostne unije, v zvezi s katerimi je potrebno nadaljnje ukrepanje sozakonodajalcev, da bi se izboljšala **kibernetska varnost** in olajšal dostop do **elektronskih dokazov** ter dokončalo delo v zvezi s trdnejšimi in pametnejšimi informacijskimi sistemi za upravljanje varnosti, meja in migracij;
- so zajete najnovejše informacije o skupnih in nujnih prizadevanjih v zvezi z oceno in krepitvijo **varnosti omrežij pete generacije (5G)**, ki so se začela marca 2019, in sicer na podlagi nacionalnih ocen tveganja, ki so jih države članice predložile do 15. julija 2019;
- je obravnavan sveženj štirih poročil, povezanih s **preprečevanjem pranja denarja**, ki jih je Komisija sprejela 24. julija 2019 in v katerih so analizirana sedanja tveganja

[1] https://www.consilium.europa.eu/media/39935/a-new-strategic-agenda-2019-2024-sl.pdf.

[2] Za pregled glej informativni pregled „Varnostna unija: Evropa, ki varuje“ (https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-security-union_1.pdf) in „Osemnajsto poročilo o nadaljnjem napredku pri vzpostavljanju učinkovite in prave varnostne unije“ (COM(2019) 145 final z dne 20. marca 2019).

in ranljivosti na področju pranja denarja ter je ocenjeno, kako se ustrezni regulativni okvir EU uporablja v zasebnem in javnem sektorju;
- so zajete najnovejše informacije o napredku, ki je bil od marca 2019[3] dosežen pri izvajanju zakonodajnih ukrepov na področju varnostne unije, pri čemer je interoperabilnost informacijskih sistemov ena od glavnih prednostnih nalog držav članic za hitro in popolno izvajanje;
- so predstavljeni tekoče delo v zvezi z bojem proti dezinformacijam in zaščito volitev pred grožnjami, ki jih omogoča kibernetski prostor, prizadevanja za povečanje pripravljenosti in zaščite pred varnostnimi grožnjami ter sodelovanje z mednarodnimi partnerji pri varnostnih vprašanjih.

II. DOSEGANJE REZULTATOV PRI ZAKONODAJNIH PREDNOSTNIH NALOGAH

1. Preprečevanje radikalizacije na spletu in v skupnostih

Preprečevanje radikalizacije je v središču odziva EU na terorizem na spletu in v naših skupnostih.

Grozoviti napad v Christchurchu na Novi Zelandiji 15. marca 2019 je bil grozljiv opomin, kako je mogoče internet izkoristiti za teroristične namene, ne glede na to, ali jih spodbuja džihadizem, skrajno desničarski ekstremizem ali katera koli druga ekstremistična ideologija. Hitrost in obseg, s katerima se je video posnetek napada na Christchurch, ki se je prenašal v živo, razširil po internetnih platformah, sta poudarila ključni pomen tega, da imajo internetne platforme vzpostavljene ustrezne ukrepe za zaustavitev hitrega širjenja take vsebine.

Voditeljice in voditelji držav in vlad nekaterih držav članic in tretjih držav, predsednik Juncker in spletne platforme so v odziv 15. maja 2019 podprli „**poziv iz Christchurcha k ukrepanju**“[4], v katerem so določeni skupni ukrepi za odpravo terorističnih in nasilnih ekstremističnih spletnih vsebin. Skupini G7[5] in G20[6] sta v zvezi s tem sprejeli dodatne zaveze.

Komisija je jasno in prisotno nevarnost, ki jo predstavljajo teroristične spletne vsebine, že obravnavala z **zakonodajnim predlogom**, ki ga je predsednik Juncker napovedal v svojem govoru o stanju v Uniji iz leta 2018 in v katerem je predlagan jasen in usklajen pravni okvir za preprečevanje zlorabe ponudnikov storitev gostovanja za razširjanje terorističnih vsebin na spletu[7]. S predlaganimi ukrepi bi za internetne platforme postala obvezna odstranitev teroristične vsebine v eni uri po prejetju odredbe o odstranitvi od pristojnih organov v kateri koli državi članici. Poleg tega bi morala platforma, če bi bila zlorabljena za širjenje teroristične vsebine, za odkrivanje te vsebine uporabiti proaktivne ukrepe in preprečiti, da bi

---

3 Glej Osemnajsto poročilo o nadaljnjem napredku pri vzpostavljanju učinkovite in prave varnostne unije (COM(2019) 145 final z dne 20. marca 2019).

4 https://www.elysee.fr/emmanuel-macron/2019/05/15/the-christchurch-call-to-action-to-eliminate-terrorist-and-violent-extremist-content-online.en. Francoski predsednik Emmanuel Macron in novozelandska premierka Jacinda Ardern sta 15. maja 2019 voditelje in spletne platforme povabila v Pariz, da bi začeli izvajati to pobudo.

5 https://www.elysee.fr/en/g7/2019/04/06/g7-interior-ministers-meeting-what-are-the-outcomes.

6 Voditelji so na vrhu G20 v Osaki 28. in 29. junija 2019 znova potrdili svojo zavezanost ukrepanju za zaščito ljudi pred terorizmom in nasilnim ekstremizmom, ki spodbuja terorizem z izkoriščanjem interneta (https://g20.org/pdf/documents/en/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf).

7 COM(2018) 640 final z dne 12. septembra 2018.

se ponovno pojavila, in sicer z jasnimi pravili in zaščitnimi ukrepi. Organi držav članic bi morali zagotoviti namensko zmogljivost za kazenski pregon z viri za učinkovito odkrivanje teroristične vsebine in izdajo odredb o odstranitvi.

S tem se bo omogočila vzpostavitev hitrega in učinkovitega sistema v vsej Uniji in uvedli se bodo strogi zaščitni ukrepi, vključno z učinkovitimi pritožbenimi mehanizmi in zagotovitvijo pravnih sredstev.

Predlagani ukrepi bodo pomagali zagotoviti nemoteno delovanje enotnega digitalnega trga, hkrati pa bodo povečali varnost na spletu in zaupanje v spletno okolje ter okrepili ukrepe za zaščito svobode izražanja in obveščanja.

Ministri za pravosodje in notranje zadeve so se v Svetu decembra 2018 dogovorili o splošnem pristopu v zvezi s predlogom. Evropski parlament je svoje stališče sprejel v prvi obravnavi aprila 2019. **Komisija oba sozakonodajalca poziva, naj čim prej začneta medinstitucionalna pogajanja o tej prednostni pobudi o odstranitvi terorističnih spletnih vsebin**, da bi se dosegel hiter dogovor o regulativnem okviru EU z jasnimi pravili in zaščitnimi ukrepi.

Hkrati Komisija še naprej sodeluje s spletnimi platformami v okviru **internetnega foruma EU**[8]. Kot je predsednik Juncker napovedal na srečanju v Parizu 15. maja 2019 o „pozivu iz Christchurcha k ukrepanju“, je Komisija skupaj z Europolom začela delo v zvezi z razvojem **kriznega protokola EU**, da bi se lahko vlade in internetne platforme hitro in usklajeno odzvale na širjenje terorističnih spletnih vsebin, na primer takoj po terorističnem napadu. To delo je del prizadevanj na mednarodni ravni za izvajanje „poziva iz Christchurcha k ukrepanju“. Komisija bo poleg nadaljnjih razprav z državami članicami in industrijo ter zadnjim preverjanjem pred izvedbo, ki je načrtovana za september 2019 za simulacijo izrednih razmer, 7. oktobra 2019 sklicala srečanje ministrov v okviru internetnega foruma EU zaradi potrditve kriznega protokola EU.

Poleg tega si Komisija še naprej prizadeva za **podporo državam članicam in lokalnim akterjem pri preprečevanju radikalizacije in boju proti njej** na terenu v lokalnih skupnostih po vsej Evropi. Za to so potrebna dolgoročna in trajnostna prizadevanja, ki vključujejo vse pomembne akterje na lokalni in nacionalni ravni ter ravni EU. **Usmerjevalni odbor za ukrepe Unije na področju preprečevanja in zatiranja radikalizacije**, ustanovljen avgusta 2018 za svetovanje Komisiji o tem, kako okrepiti odziv politike EU na tem področju, se je 17. junija 2019 sestal drugič, da bi proučil nadaljnje ukrepe na prednostnih področjih, kot sta radikalizacija v zaporih in boj proti ekstremističnim ideologijam. Ker so strokovni delavci na terenu pogosto najprimernejši za opredelitev zgodnjih opozorilnih znakov radikalizacije in načinov za njihovo obravnavanje, **mreža za ozaveščanje o radikalizaciji**[9], ki jo je ustanovila EU, še naprej podpira službe za prvi odziv na terenu ter

---

[8] **Internetni forum EU**, vzpostavljen leta 2015, združuje ministre EU za notranje zadeve, internetno industrijo in druge deležnike, ki sodelujejo v prostovoljnem partnerstvu pri obravnavanju zlorabe interneta s strani terorističnih skupin in zaščiti državljanov.

[9] Komisija je leta 2011 vzpostavila **mrežo za ozaveščanje o radikalizaciji**, da bi združila strokovne delavce na terenu. Leta 2015 je mrežo okrepila z vzpostavitvijo centra odličnosti mreže za ozaveščanje o radikalizaciji za razvoj bolj usmerjenih služb za usmerjanje, podporo in svetovanje deležnikom v državah članicah ter povečanje strokovnega znanja in spretnosti različnih akterjev. Za več informacij o dejavnostih mreže za ozaveščanje o radikalizaciji glej: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en.

združuje približno 5 000 izvajalcev iz civilne družbe, šol in policije, pa tudi nacionalne koordinatorje in oblikovalce politike.

Zaradi nedavnega sodelovanja strokovnih delavcev na terenu v okviru mreže se je poglobilo razumevanje izzivov skrajnega desničarskega ekstremizma. Mreža za ozaveščanje o radikalizaciji bo letos objavila informativne liste, da bi oblikovalcem politike in strokovnim delavcem pomagala opredeliti glavne pojavne oblike in izraze skrajnega desničarskega in islamističnega ekstremizma, kot so ključne navedbe, jezik, oblike, simboli, tipologije in strategije. Nazadnje, lokalni akterji in **mesta** so v ospredju pri preprečevanju radikalizacije in boju proti njej, zato Komisija podpira pobude o boju proti radikalizaciji, ki jih vodijo mesta. Po konferenci z naslovom „Mesta v EU proti radikalizaciji“, ki je potekala 26. februarja 2019, je 8. julija 2019 potekalo prvo srečanje pilotne skupine približno 20 mest, ki ga je gostil župan Strasbourga, da bi se okrepili izmenjava dobrih praks in prizadevanja mest na tem področju.

Hkrati se izvajajo prizadevanja za podporo partnerskih držav pri obravnavanju radikalizacije, ki lahko vodi v terorizem, vključno v zaporih.

Da bi se preprečila grožnja, ki jo predstavljajo teroristične vsebine na spletu, Komisija Evropski parlament in Svet poziva, naj:

- čim prej začneta pogajanja o zakonodajnem predlogu za preprečevanje širjenja **terorističnih spletnih vsebin**, da bi se dosegel hiter dogovor o regulativnem okviru EU z jasnimi pravili in zaščitnimi ukrepi.

2. Krepitev kibernetske varnosti

Kibernetska varnost ostaja ključen varnostni izziv. EU je dosegla pomemben napredek[10] pri obravnavanju „klasičnih“ kibernetskih groženj, usmerjenih v sisteme in podatke, pri čemer je izvajala ukrepe iz skupnega sporočila[11] iz septembra 2017 z naslovom „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“. To vključuje uredbo EU o kibernetski varnosti[12], ki daje Agenciji Evropske unije za kibernetsko varnost trajni mandat, krepi njeno vlogo in vzpostavlja okvir EU za certificiranje na področju kibernetske varnosti. Komisija je obravnavala tudi sektorske zahteve, na primer prek Priporočila o kibernetski varnosti v energetskem sektorju, sprejetem 3. aprila 2019[13]. Vendar nadaljnje povečevanje dejavnosti zlonamernih akterjev proti različnim ciljem in žrtvam pomeni, da so prizadevanja za boj proti kibernetski kriminaliteti in izboljšanje kibernetske varnosti še vedno prednostna naloga EU.

Evropski parlament in Svet se morata dogovoriti še o prednostni pobudi Komisije o **Evropskem industrijskem, tehnološkem in raziskovalnem strokovnem centru za**

[10] Za več informacij glej brošuro „Okrepitev kibernetske varnosti v Evropski uniji: odpornost, odvračanje in obramba“: https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence.

[11] JOIN(2017) 450 final z dne 13. septembra 2017.

[12] Z aktom EU o kibernetski varnosti (Uredba (EU) 2019/881 z dne 17. aprila 2019) so bila prvič uvedena pravila za certificiranje proizvodov, procesov in storitev na področju kibernetske varnosti, ki bodo veljala za vso EU.Poleg tega zadevna uredba uvaja nov stalni mandat Agencije EU za kibernetsko varnost (ENISA) ter ji namenja več virov, da bo lahko dosegla svoje cilje. Za več informacij o razpisu za zbiranje predlogov glej: https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross.

[13] C(2019) 2400 final in SWD(2019) 1240 final z dne 3. aprila 2019.

kibernetsko varnost ter mreži nacionalnih koordinacijskih centrov[14]. Cilj predloga je podpreti tehnološke in industrijske zmogljivosti na področju kibernetske varnosti ter povečati konkurenčnost industrije Unije na tem področju. Oba sozakonodajalca sta svoja pogajalska mandata sprejela marca 2019. Ker medinstitucionalnih pogajanj ni bilo mogoče zaključiti pred koncem prejšnjega mandata Evropskega parlamenta, je ta formalno sprejel stališče na prvi obravnavi. Medtem se nadaljujejo razprave med državami članicami in Svetom, poseben poudarek pa je namenjen medsebojnemu vplivu predlagane uredbe o strokovnem centru in strokovni mreži za kibernetsko varnost na eni strani ter programoma Obzorje Evropa in Digitalna Evropa na drugi strani. **Komisija oba sozakonodajalca poziva, naj nadaljujeta in hitro zaključita medinstitucionalna pogajanja o tej prednostni pobudi za izboljšanje kibernetske varnosti.**

Medtem Komisija še naprej **podpira raziskave in inovacije**, povezane s kibernetsko varnostjo, in sicer je v sedanjem večletnem finančnem okviru namenila 135 milijonov EUR za projekte na področjih, kot so kibernetska varnost v kritični infrastrukturi, inteligentno upravljanje varnosti in zasebnosti ter orodja, namenjena zlasti državljanom ter malim in srednjim podjetjem[15]. Komisija je julija 2019 objavila nov razpis za zbiranje predlogov v okviru programa Instrument za povezovanje Evrope, in sicer je ključnim akterjem, opredeljenim v direktivi o varnosti omrežij in informacijskih sistemov (direktivi NIS)[16], kot so evropske skupine za odzivanje na incidente na področju računalniške varnosti, izvajalci bistvenih storitev (npr. banke, bolnišnice, ponudniki komunalnih storitev, železnice, letalske družbe, ponudniki domenskih imen) in različni javni organi, zagotovila sredstva EU v višini 10 milijonov EUR. Poleg tega so evropski organi za certificiranje na področju kibernetske varnosti prvič upravičeni do vloge za vključitev v ta program, da bi se jim omogočilo izvajanje uredbe EU o kibernetski varnosti.

Svet je 17. maja 2019 sprejel **režim sankcij**, s katerim lahko EU naloži ciljno usmerjene omejevalne ukrepe za odvračanje kibernetskih napadov, ki pomenijo zunanjo grožnjo EU ali njenim državam članicam, in odziv nanje. Nov režim sankcij je del **zbirke orodij EU za kibernetsko diplomacijo**[17], okvira za skupni diplomatski odziv EU na zlonamerne kibernetske dejavnosti[18], ki EU omogoča, da ukrepe v okviru skupne zunanje in varnostne politike v celoti izkoristi za odvračanje od zlonamernih kibernetskih dejavnosti in v odziv nanje.

EU poleg ukrepov proti kibernetskim grožnjam, usmerjenim v sisteme in podatke, sprejema tudi ukrepe za obravnavanje zapletenih in večstranskih izzivov, ki jih predstavljajo **hibridne grožnje**[19]. Evropski svet je v svojih sklepih z dne 21. junija 2019[20] poudaril, da mora EU „poskrbeti za usklajeno odzivanje na hibridne in kibernetske grožnje ter okrepiti sodelovanje

---

14 COM(2018) 630 final z dne 12. septembra 2018.

15 https://ec.europa.eu/programmes/horizon2020/en/h2020-section/cross-cutting-activities-focus-areas.

16 Direktiva (EU) 2016/1148 z dne 6. julija 2016.

17 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/sl/pdf.

18 To vključuje kibernetske napade, pa tudi poskuse kibernetskih napadov s potencialno pomembnim učinkom, ki vključujejo na primer dostop do informacijskih sistemov ali prestrezanje podatkov prek digitalne infrastrukture, kot so omrežja 5G (glej tudi oddelek III o krepitvi varnosti digitalnih infrastruktur).

19 Glej poročilo o izvajanju skupnega okvira o preprečevanju hibridnih groženj iz leta 2016 ter skupno poročilo o povečanju odpornosti in krepitvi zmogljivosti za obravnavanje hibridnih groženj (SWD(2019) 200 final z dne 28. maja 2019).Glej tudi zakonodajni predlog uredbe Evropskega parlamenta in Sveta o vzpostavitvi režima Unije za nadzor izvoza, prenosa, posredovanja, tehnične pomoči in tranzita blaga z dvojno rabo (prenovitev) iz septembra 2016 (COM(2016) 616 final z dne 28. septembra 2016).

20 https://www.consilium.europa.eu/media/39960/20-21-euco-final-conclusions-sl.pdf.

z ustreznimi mednarodnimi akterji“. Komisija se strinja z dejstvom, da je boj proti hibridnim grožnjam tudi prednostna naloga finskega predsedstva Sveta ter da je na neformalnem srečanju ministrov za pravosodje in notranje zadeve v Helsinkih 18. in 19. julija 2019 potekala politična razprava na podlagi scenarijev. Podobne razprave o hibridnih grožnjah na podlagi scenarijev so potekale med direktorji za obrambno politiko EU 7. in 8. julija 2019 ter med direktorji za politiko EU 9. in 10. julija 2019, ministri za zunanjo politiko in obrambo pa bodo z izidi teh razprav seznanjeni na skupnem neformalnem sestanku 29. in 30. avgusta 2019.

Da bi se izboljšala kibernetska varnost, Komisija Evropski parlament in Svet poziva, naj:

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

3. Izboljšanje dostopa organov kazenskega pregona do elektronskih dokazov

EU je sprejela nadaljnje ukrepe, da bi teroristom in storilcem kaznivih dejanj preprečila uporabo sredstev za njihovo delovanje, kar bi jim otežilo dostop do predhodnih sestavin za eksplozive[21], financiranje njihovega delovanja[22] in potovanje brez odkrivanja[23].

Pogajanja o predlogih Komisije iz aprila 2018 o izboljšanju **dostopa do elektronskih dokazov** za organe kazenskega pregona bi bilo treba čim prej zaključiti, glede na to, da več kot polovica vseh kazenskih preiskav danes vključuje čezmejno zahtevo za dostop do elektronskih dokazov[24]. Svet je sprejel pogajalsko izhodišče za predlog uredbe[25] za izboljšanje čezmejnega dostopa do elektronskih dokazov v kazenskih preiskavah in predlog direktive[26] o določitvi harmoniziranih pravil o imenovanju pravnih zastopnikov za namene zbiranja dokazov v kazenskih postopkih. Glede na odločilni pomen učinkovitega dostopa do elektronskih dokazov za preiskovanje in pregon čezmejnih kaznivih dejanj, kot je terorizem ali kibernetska kriminaliteta, Komisija Evropski parlament poziva, naj pospeši obravnavanje tega predloga, da si lahko zakonodajalca prizadevata za hitro sprejetje.

Hkrati si Komisija prizadeva za izboljšanje in zagotovitev potrebnih zaščitnih ukrepov na področju **mednarodne izmenjave elektronskih dokazov**, in sicer v okviru tekočih pogajanj o Drugem dodatnem protokolu h Konvenciji Sveta Evrope o kibernetski kriminaliteti iz Budimpešte, pa tudi z Združenimi državami Amerike v skladu s pogajalskimi mandati, ki jih

[21] Uredba (EU) 2019/1148 z dne 20. junija 2019 o trženju in uporabi predhodnih sestavin za eksplozive.

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

[23] 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.

[24] Elektronski dokazi so potrebni v približno 85 % kazenskih preiskav in pri dveh tretjinah teh preiskav je treba dokaze zahtevati od ponudnikov spletnih storitev s sedežem v drugi jurisdikciji. Glej oceno učinka, priloženo zakonodajnemu predlogu (SWD(2018) 118 final z dne 17. aprila 2018).

[25] COM(2018) 225 final z dne 17. aprila 2018. Svet je svoj pogajalski mandat o predlagani uredbi sprejel na zasedanju Sveta za pravosodje in notranje zadeve 7. decembra 2018.

[26] COM(2018) 226 final z dne 17. aprila 2018. Svet je svoj pogajalski mandat o predlagani direktivi sprejel na zasedanju Sveta za pravosodje in notranje zadeve 8. marca 2019.

je Svet podelil na seji Sveta za pravosodje in notranje zadeve 6. in 7. junija 2019[27]. Komisija je sodelovala v najnovejšem krogu pogajanj o Drugem dodatnem protokolu h Konvenciji Sveta Evrope o kibernetski kriminaliteti iz Budimpešte 9. in 11. julija 2019. Komisija in organi Združenih držav Amerike se trenutno na tehnični ravni pripravljajo na uradni začetek pogajanj za sporazum med EU in ZDA o čezmejnem dostopu do elektronskih dokazov.

Da bi se izboljšal dostop organov kazenskega pregona do elektronskih dokazov, Komisija Evropski parlament poziva, naj:
• sprejme svoj pogajalski mandat v zvezi z zakonodajnima predlogoma o **elektronskih dokazih** in hitro začne tristranske razprave s Svetom *(prednostna naloga iz skupne izjave).*

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

Komisija je po sprejetju pravil o **interoperabilnosti informacijskih sistemov**[28], s katerimi se bodo odpravile informacijske vrzeli in pomanjkljivosti pri odkrivanju več identitet in boju proti identitetnim prevaram, hitro začela izvajati vrsto pobud za podporo državam članicam v postopku izvajanja, po potrebi vključno s financiranjem, pa tudi z delavnicami za lažjo izmenjavo strokovnega znanja in dobrih praks. Tesno sodelovanje med agencijami EU, vsemi državami članicami in pridruženimi schengenskimi državami bo ključnega pomena, da bi dosegli ambiciozen cilj doseganja popolne interoperabilnosti informacijskih sistemov EU za upravljanje varnosti, meja in migracij do leta 2020.

Za dosego tega cilja je potrebno tudi hitro in celovito izvajanje nedavno sprejete zakonodaje za vzpostavitev novih informacijskih sistemov – sistema vstopa/izstopa EU[29] in Evropskega sistema za potovalne informacije in odobritve[30] – ter okrepitev schengenskega informacijskega sistema[31] in razširitev evropskega informacijskega sistema kazenskih evidenc[32] na državljane tretjih držav. Nova arhitektura za trdnejše in pametnejše informacijske sisteme za upravljanje varnosti, meja in migracij bo dejanske spremembe na terenu prinesla le, če se bodo vse komponente v celoti izvedle na ravni Unije in v vsaki državi članici v skladu z dogovorjenim časovnim razporedom.

Hkrati morata sozakonodajalca sprejeti nadalje ukrepe za dokončanje dela v zvezi s trdnejšimi in pametnejšimi informacijskimi sistemi za upravljanje varnosti, meja in migracij.

Komisija je v okviru tehničnega izvajanja **Evropskega sistema za potovalne informacije in odobritve** 7. januarja 2019 predstavila dva predloga, ki določata tehnične spremembe zadevne uredbe[33], potrebne za popolno vzpostavitev sistema. Komisija sozakonodajalca poziva, naj si prizadevata za te tehnične spremembe, da bi se čim prej sprejel dogovor, ter tako omogočita hitro in pravočasno izvajanje Evropskega sistema za potovalne informacije in odobritve, da bi ta začel delovati v začetku leta 2021.

---

27 https://www.consilium.europa.eu/sl/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/.

28 Uredba (EU) 2019/817 in Uredba (EU) 2019/818 z dne 20. maja 2019.

29 Uredba (EU) 2017/2226 z dne 30. novembra 2017.

30 Uredba (EU) 2018/1240 in Uredba (EU) 2018/1241 z dne 12. septembra 2018.

31 Uredba (EU) 2018/1860, Uredba (EU) 2018/1861 in Uredba (EU) 2018/1862 z dne 28. novembra 2018.

32 Uredba (EU) 2019/816 z dne 17. aprila 2019.

33 COM(2019) 3 final in COM(2019) 4 final z dne 7. januarja 2019.

Komisija je maja 2018 predstavila predlog za **okrepitev obstoječega vizumskega informacijskega sistema**[34], v katerem so določeni temeljitejši pregledi ozadja prosilcev za vizum in odprava informacijskih vrzeli z boljšo izmenjavo informacij med državami članicami.

Svet je svoj pogajalski mandat sprejel 19. decembra 2018, Evropski parlament pa je 13. marca 2019 na plenarnem zasedanju glasoval o svojem poročilu o predlogu in zaključil prvo obravnavo. Komisija poziva k hitremu začetku pogajanj med sozakonodajalcema v okviru Evropskega parlamenta v novi sestavi.

Komisija je maja 2016 predlagala razširitev področja uporabe **sistema Eurodac**[35], tako da bi poleg identifikacije prosilcev za azil vključeval tudi identifikacijo nezakonito prebivajočih državljanov tretjih držav in oseb, ki nedovoljeno vstopijo v EU. Komisija v skladu s sklepi Evropskega sveta[36] iz decembra 2018 in sporočilom Komisije z dne 6. marca 2019 o napredku pri izvajanju evropske agende o migracijah[37] sozakonodajalca poziva, naj nemudoma sprejmeta predlog. Ta zakonodajni predlog je treba sprejeti, da bo lahko sistem Eurodac postal del prihodnje arhitekture interoperabilnih informacijskih sistemov EU, s čimer se bodo povezali ključni podatki nezakonito prebivajočih državljanov tretjih držav in oseb, ki nedovoljeno vstopijo v EU.

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

- sprejmeta zakonodajni predlog o **sistemu Eurodac** *(prednostna naloga iz skupne izjave)*;
- pospešita prizadevanja za hiter dogovor o predlaganih tehničnih spremembah, ki so potrebne za vzpostavitev **Evropskega sistema za potovalne informacije in odobritve.**

III. KREPITEV VARNOSTI DIGITALNIH INFRASTRUKTUR

Odpornost naše digitalne infrastrukture je ključnega pomena za vlade, podjetja, varnost naših osebnih podatkov in delovanje naših demokratičnih institucij. **Omrežja pete generacije (5G)**, ki bodo uvedena v naslednjih letih, bodo digitalna hrbtenica naših družb in gospodarstev, ki bo povezovala milijarde državljanov, objektov in sistemov, tudi v kritičnih sektorjih, kot so energija, promet, bančništvo in zdravstvo, ter sisteme za industrijsko kontrolo, ki bodo prenašali občutljive informacije in podpirali varnostne sisteme.

S prihodki od omrežij 5G, ki naj bi po oceni leta 2025 na svetovni ravni znašali 225 milijard EUR, je 5G ključ do konkurenčnosti Evrope na svetovnem trgu, **varnost omrežij 5G pa je bistvena za zagotavljanje strateške avtonomije Unije**. Za zagotovitev visoke ravni kibernetske varnosti so potrebni usklajeni ukrepi na nacionalni in evropski ravni, saj bi vsaka šibka točka v omrežjih 5G v eni državi članici prizadela Unijo kot celoto.

Komisija je po podpori, ki so jo voditeljice in voditelji držav in vlad izrazili na zasedanju Evropskega sveta marca 2019[38], 26. marca 2019 predložila **Priporočilo o kibernetski**

[34] COM(2018) 302 final z dne 16. maja 2018.
[35] COM(2016) 272 final z dne 4. maja 2016.
[36] https://www.consilium.europa.eu/sl/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/.
[37] COM(2019) 126 final z dne 6. marca 2019.
[38] https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/sl/pdf.

varnosti omrežij 5G[39], v katerem so določeni ukrepi za oceno tveganj za kibernetsko varnost omrežij 5G in okrepitev preventivnih ukrepov. Priporočila temeljijo na usklajeni oceni tveganja na ravni EU in ukrepih za obvladovanje tveganja, učinkovitem okviru za sodelovanje in izmenjavo informacij, ter skupnem situacijskem okviru za spremljanje razmer v EU.

V **prvi fazi** postopka, ki se je začel s priporočilom, so do 15. julija 2019 vse države članice zaključile svoje **nacionalne ocene tveganja**, svoje ugotovitve pa predložile Komisiji in Agenciji EU za kibernetsko varnost ali napovedale, da bodo to storile v kratkem. Nacionalne ocene tveganja so bile pripravljene v skladu s sklopom smernic in na podlagi skupne predloge za poročanje o ugotovitvah, o katerih so se dogovorile države članice in Komisija, da bi spodbudili skladnost in olajšali izmenjavo informacij o nacionalnih rezultatih na ravni EU. Parametri, ocenjeni v vseh državah članicah, so vključevali:

- glavne grožnje in akterje, ki predstavljajo nevarnost in vplivajo na omrežja 5G;
- stopnje občutljivosti komponent in funkcij omrežja 5G ter drugih sredstev in
- različne vrste šibkih točk, vključno s tehničnimi in drugimi vrstami šibkih točk, na primer takimi, ki bi lahko izhajale iz dobavne verige 5G.

Poleg tega je delo v zvezi z nacionalnimi ocenami tveganja vključevalo številne odgovorne akterje v državah članicah, kot so, odvisno od nacionalnih pristojnosti, organi za kibernetsko varnost, telekomunikacijski organi ter varnostne in obveščevalne službe, ter tako okrepilo njihovo medsebojno sodelovanje in usklajevanje. Številne države članice so hkrati in glede na svoje nacionalne časovne razporede za uvedbo 5G že izvedle ukrepe za okrepitev veljavnih varnostnih zahtev na tem področju, več drugih pa je izrazilo namero, da bodo v bližnji prihodnosti razmislile o novih ukrepih.

Organi držav članic za kibernetsko varnost v skupini za sodelovanje na področju varnosti omrežij in informacijskih sistemov[40] bodo na podlagi rezultatov nacionalne ocene tveganj do 1. oktobra 2019 pripravili **skupni pregled tveganj na ravni EU**, kar bo druga faza postopka, ki se je začel na podlagi priporočila. Skupna za sodelovanje bo na podlagi tega v tretji fazi do 31. decembra 2019 pripravila **skupno zbirko blažilnih ukrepov Unije** za obravnavanje opredeljenih tveganj. Komisija in Agencija EU za kibernetsko varnost bosta še naprej podpirali izvajanje priporočila.

Delo v skupini za sodelovanje na področju varnosti omrežij in informacijskih sistemov podpira več drugih forumov. Organ evropskih regulatorjev za elektronske komunikacije pripravlja pregled vseh obstoječih varnostnih ukrepov, ki bi lahko bili pomembni za 5G. Nova namenska strokovna skupina v Agenciji EU za kibernetsko varnost je začela pripravljati pregled okolja groženj za omrežja 5G. Poleg tega bosta Komisija in Agencija EU za kibernetsko varnost po začetku veljavnosti uredbe o kibernetski varnosti 27. junija 2019 izvedli vse potrebne ukrepe za vzpostavitev okvira za certificiranje na ravni EU. Države članice so se junija 2019 tudi sestale v okviru odbora za standarde, da bi razpravljale o kibernetski varnosti in standardizaciji v odziv na priporočilo, naj se proučijo prihodnji izzivi

[39] C(2019) 2335 final z dne 26. marca 2019.

[40] Skupina za sodelovanje na področju varnosti omrežij in informacijskih sistemov je vzpostavljena na podlagi Direktive (EU) 2016/1148 z dne 6. julija 2016 o varnosti omrežij in informacijskih sistemov. Kot je predvideno v priporočilu, je bil vzpostavljen namenski delovni postopek v okviru skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov, ki ga vodi več držav članic. Skupina se je srečala že trikrat – aprila, maja in julija 2019 – da bi izmenjala informacije o nacionalnih pristopih in razpravljala o tem, kako olajšati pripravo ocene tveganja, usklajene na ravni EU.

na področju standardizacije kibernetske varnosti, vključno z omrežji 5G, in ustrezne pobude politike na ravni EU.

Nazadnje, varnost omrežij 5G je strateškega pomena za Unijo. Tveganje za varnost Unije lahko predstavljajo tudi tuje naložbe v strateške sektorje, pridobitev kritičnih sredstev, tehnologij in infrastrukture v Uniji ter dobava kritične opreme.

Dne 10. aprila 2019 je uradno začel veljati nov **okvir EU za pregled neposrednih tujih naložb**[41]. Komisija in države članice bodo v naslednjih 18 mesecih izvedle potrebne ukrepe, s katerimi bodo zagotovile, da bo lahko EU od 11. oktobra 2020 v celoti uporabljala uredbo o pregledu naložb.

IV. PREPREČEVANJE PRANJA DENARJA

Storilcem kaznivih dejanj in teroristom daje možnost, da v nekaj urah prenesejo sredstva med različnimi bančnimi računi, omogoča lažjo pripravo terorističnih dejanj ali nezakonito pranje premoženjske koristi, pridobljene s kaznivim dejanjem, v različnih državah članicah. Unija je za reševanje tega izziva razvila trden **regulativni okvir za boj proti pranju denarja in financiranju terorizma** v skladu z mednarodnimi standardi, ki jih je sprejela Projektna skupina za finančno ukrepanje.

Komisija je zaradi potrebe po sledenju razvijajočim se trendom, tehnološkemu razvoju in prilagodljivi iznajdljivosti storilcev kaznivih dejanj pri izkoriščanju morebitnih vrzeli ali šibkih točk v sistemu 24. julija 2019 sprejela **sveženj štirih poročil**, v katerih so analizirana sedanja tveganja in ranljivosti na področju pranja denarja ter je ocenjeno, kako okvir uporabljajo ustrezni akterji v zasebnem in javnem sektorju[42].

Sveženj vključuje **oceno morebitnega povezovanja nacionalnih centraliziranih registrov bančnih računov** in **sistemov za pridobivanje podatkov** v EU. Taki nacionalni centralizirani sistemi omogočajo identifikacijo vsake fizične ali pravne osebe, ki ima ali nadzoruje plačilne račune, bančne račune in sefe. To so informacije, ki so pogosto ključne za pristojne organe v boju proti pranju denarja in financiranju terorizma. Države članice morajo v skladu s peto direktivo o preprečevanju pranja denarja[43] vzpostaviti take nacionalne centralizirane sisteme ter svojim finančnim obveščevalnim enotam zagotoviti neposreden dostop. Nedavno sprejeta pravila za olajšanje uporabe finančnih informacij za boj proti hudim kaznivim dejanjem[44] pristojnim organom kazenskega pregona in uradom za odvzem premoženjske koristi zagotavljajo neposreden dostop do njihovih ustreznih nacionalnih

[41] Uredba (EU) 2019/452 z dne 19. marca 2019 o vzpostavitvi okvira za pregled neposrednih tujih naložb v Uniji. Novi okvir vzpostavlja mehanizem sodelovanja, znotraj katerega si bodo države članice in Komisija lahko izmenjevale informacije in izražale pomisleke v zvezi s posameznimi naložbami. Komisiji bo tudi omogočil, da izdaja mnenja v primerih, kadar naložba ogroža varnost ali javni red več držav članic ali kadar bi naložba lahko vplivala na projekt ali program, ki je v interesu celotne EU. Država članica, v kateri se naložba izvaja, odloča glede tega, kako se naložba obravnava.

[42] Poročilo o oceni tveganja pranja denarja in financiranja terorizma, ki vpliva na notranji trg in je povezano s čezmejnimi dejavnostmi (COM(2019) 370 final z dne 24. julija 2019), Poročilo o medsebojni povezavi nacionalnih centraliziranih avtomatiziranih mehanizmov (osrednjih registrov ali osrednjih elektronskih sistemov za pridobivanje podatkov) (COM(2019) 372 final z dne 24. julija 2019), Poročilo o oceni nedavnih domnevnih primerov pranja denarja, ki vključujejo kreditne institucije EU (COM(2019) 373 final z dne 24. julija 2019), Poročilo o oceni okvira za sodelovanje med finančnimi obveščevalnimi enotami (COM(2019) 371 final z dne 24. julija 2019).

[43] Direktiva (EU) 2015/849 z dne 20. maja 2015.

[44] Direktiva (EU) 2019/1153 z dne 20. junija 2019.

centraliziranih registrov bančnih računov. V poročilu so na podlagi tega in v skladu z direktivo o preprečevanju pranja denarja ocenjene različne informacijske rešitve na ravni EU, ki že delujejo ali so v pripravi in so lahko model za morebitno medsebojno povezovanje nacionalnih centraliziranih sistemov. Ker bi prihodnja medsebojna povezava centraliziranih mehanizmov na ravni EU pospešila dostop do finančnih informacij in olajšala čezmejno sodelovanje pristojnih organov, se namerava Komisija nadalje posvetovati z ustreznimi deležniki, vladami, pa tudi finančnimi obveščevalnimi enotami, organi kazenskega pregona in uradi za odvzem premoženjske koristi kot morebitnimi „končnimi uporabniki“ morebitnega sistema povezovanja.

V poročilu o oceni **sodelovanja med finančnimi obveščevalnimi enotami** je kot del razmisleka o delu finančnih obveščevalnih enot proučeno sodelovanje z Unijo in s tretjimi državami[45]. Opredeljene so nekatere pomanjkljivosti, ki bodo verjetno še obstajale, dokler naloge in obveznosti finančnih obveščevalnih enot glede čezmejnega sodelovanja ne bodo jasneje določene v pravnem okviru EU za preprečevanje pranja denarja in financiranju terorizma. Ocena kaže tudi na potrebo po močnejšem mehanizmu za usklajevanje in podpiranje čezmejnega sodelovanja in potrebo po analizi.

Komisija bo poleg obstoječega dela na področju pranja denarja in financiranja terorizma ter v odgovor na poziv Evropskega parlamenta[46] še naprej ocenjevala nujnost, tehnično izvedljivost in sorazmernost dodatnih ukrepov za spremljanje financiranja terorizma v EU[47].

V. IZVAJANJE DRUGIH PREDNOSTNIH DOSJEJEV O VARNOSTI

1. Izvajanje zakonodajnih ukrepov na področju varnostne unije

S sklenitvijo dogovora o ukrepih v okviru varnostne unije se proces ne zaključi – ključno je, da države članice naknadno zagotovijo njihovo hitro in popolno izvajanje, da se lahko izkoristijo vse prednosti. Komisija države članice pri tem dejavno podpira, med drugim s financiranjem in lajšanjem izmenjave dobrih praks.

Vendar je po potrebi pripravljena tudi v celoti uporabiti svoja pooblastila za izvrševanje zakonodaje EU na podlagi Pogodb, vključno z ukrepi za ugotavljanje kršitev, kadar je to ustrezno.

Rok za izvedbo **direktive EU o evidenci podatkov o potnikih**[48] se je iztekel 25. maja 2018. Do danes je Komisijo o popolnem prenosu uradno obvestilo 25 držav članic.[49]. Dve državi članici Direktive še vedno nista v celoti prenesli kljub postopkoma za ugotavljanje kršitev,

---

45 Ta ocena se zahteva s členom 65(2) pete direktive o pranju denarja (Direktive (EU) 2018/843 z dne 30. maja 2018).

46 Posebni odbor Evropskega parlamenta o terorizmu je v svojem končnem poročilu, sprejetem decembra 2018, pozval k ustanovitvi sistema Evropske unije za sledenje financiranja terorističnih dejavnosti, ki bi bil usmerjen v transakcije posameznikov, ki so povezani s terorizmom, in njihovo financiranje v enotnem območju plačil v eurih.

47 Glej Osemnajsto poročilo o nadaljnjem napredku pri vzpostavljanju učinkovite in prave varnostne unije (COM(2019) 145 final z dne 20. marca 2019).

48 Direktiva (EU) 2016/681 z dne 27. aprila 2016.

49 Sklici na uradna obvestila o popolnem prenosu upoštevajo izjave držav članic in ne posegajo v preverjanje prenosa, ki ga izvajajo službe Komisije.

uvedenima 19. julija 2018[50]. Hkrati Komisija vse države članice še naprej podpira pri prizadevanjih za dokončanje razvoja njihovih sistemov evidenc podatkov o potnikih, vključno s spodbujanjem izmenjave informacij in dobrih praks.

Rok za prenos **direktive o boju proti terorizmu**[51] se je iztekel 8. septembra 2018. Do danes je Komisijo o popolnem prenosu uradno obvestilo 22 držav članic. Tri države članice kljub uvedbi postopkov za ugotavljanje kršitev 22. novembra 2018 še vedno niso sporočile sprejetja nacionalne zakonodaje, s katero bi v celoti prenesle navedeno direktivo.[52]

Rok za prenos **direktive o nadzoru nabave in posedovanja orožja**[53] se je iztekel 14. septembra 2018. Do danes je Komisijo o popolnem prenosu uradno obvestilo osem držav članic. Dvajset držav članic kljub uvedbi postopkov za ugotavljanje kršitev 22. novembra 2018 še vedno ni sporočilo sprejetja nacionalnih ukrepov, s katerimi bi v celoti prenesle Direktivo[54].

Kar zadeva prenos **direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj**[55] v nacionalno pravo, se je rok za prenos iztekel 6. maja 2018. Do danes je Komisijo o popolnem prenosu uradno obvestilo 20 držav članic.[56]. Sedem držav članic kljub postopkom za ugotavljanje kršitev, ki jih je Komisija uvedla 19. julija 2018, še vedno ni sporočilo sprejetja nacionalnih ukrepov, s katerimi bi v celoti prenesle Direktivo[57].

Države članice so morale **direktivo o varnosti omrežij in informacijskih sistemov**[58] v nacionalno zakonodajo prenesti do 9. maja 2018. Do danes je Komisijo o popolnem prenosu uradno obvestilo 26 držav članic, dve državi članici pa sta Direktivo prenesli delno[59]. Poleg tega so morale države članice v skladu z Direktivo do 9. novembra 2018 določiti izvajalce bistvenih storitev. Komisija bi morala do 9. maja 2019 Evropskemu parlamentu in Svetu predložiti poročilo, v katerem oceni skladnost pristopa držav članic pri določanju izvajalcev bistvenih storitev, določenih na njihovem ozemlju. Vendar je morala pripravo poročila preložiti, ker več držav članic še ni predložilo popolnih informacij o postopku določitve.

Komisija ocenjuje prenos četrte **direktive o preprečevanju pranja denarja**[60], hkrati pa tudi preverja, ali države članice izvajajo ta pravila. Komisija je začela postopke za ugotavljanje kršitev zoper 24 držav članic, saj je ocenila, da sporočila, prejeta od držav članic, ne pomenijo

---

50 Slovenija je poslala uradno obvestilo o delnem prenosu. Španija ni poslala uradnega obvestila o prenosu (stanje na dan 24. julija 2019).

51 Direktiva (EU) 2017/541 z dne 15. marca 2017.

52 Poljska je poslala uradno obvestilo o delnem prenosu. Grčija in Luksemburg nista poslali uradnega obvestila o prenosu (stanje na dan 24. julija 2019).

53 Direktiva (EU) 2017/853 z dne 17. maja 2017.

54 Belgija, Češka, Estonija, Litva, Poljska, Portugalska, Švedska in Združeno kraljestvo so poslali uradno obvestilo o delnem prenosu. Nemčija, Irska, Grčija, Španija, Ciper, Luksemburg, Madžarska, Nizozemska, Romunija, Slovenija, Slovaška in Finska niso poslali uradnega obvestila o prenosu (stanje na dan 24. julija 2019).

55 Direktiva (EU) 2016/680 z dne 27. aprila 2016.

56 Dvajset držav članic je zaključilo prenos (stanje na dan 24. julija 2019).

57 Latvija, Portugalska, Slovenija in Finska so poslale uradno obvestilo o delnem prenosu. Grčija in Španija nista poslali uradnega obvestila o prenosu. Čeprav je Nemčija poslala uradno obvestilo o popolnem prenosu, Komisija meni, da ta prenos ni zaključen (stanje na dan 24. julija 2019).

58 Direktiva (EU) 2016/1148 z dne 27. aprila 2016.

59 Belgija in Madžarska sta delno prenesli Direktivo (stanje na dan 24. julija 2019).

60 Direktiva (EU) 2015/849 z dne 20. maja 2015.

popolnega prenosa te direktive[61].

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 uradno obvestila o prenosu v nacionalno zakonodajo, ena država članica pa še ni dopolnila uradnega obvestila o prenosu[62];
- **direktiva o boju proti terorizmu**, v zvezi s katero dve državi članici Komisije še nista uradno obvestili o prenosu v nacionalno zakonodajo, ena država članica pa še ni dopolnila uradnega obvestila o prenosu[63];
- **direktiva o nadzoru nabave in posedovanja orožja**, v zvezi s katero 12 držav članic Komisije še ni uradno obvestilo o prenosu v nacionalno zakonodajo, osem držav članic pa še ni dopolnilo uradnega obvestila o prenosu[64];
- **direktiva o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj**, v zvezi s katero dve državi članici Komisije še nista uradno obvestili o prenosu v nacionalno zakonodajo, pet držav članic pa še ni dopolnilo uradnega obvestila o prenosu[65];
- **direktiva o varnosti omrežij in informacijskih sistemov**, v zvezi s katero dve državi članici še nista dopolnili uradnega obvestila o prenosu[66] in
- **četrta direktiva o preprečevanju pranja denarja**, v zvezi s katero 24 držav članic še ni dopolnilo uradnega obvestila o prenosu[67].

2. Boj proti dezinformacijam in zaščita volitev pred drugimi grožnjami, ki jih omogoča kibernetski prostor

Zaščita demokratičnih procesov in institucij pred dezinformacijami in povezanim vmešavanjem je velik izziv za družbe po vsem svetu. EU je za reševanje tega izziva vzpostavila **trden okvir za usklajeno ukrepanje proti dezinformacijam** ob polnem spoštovanju evropskih vrednot in temeljnih pravic[68]. Kot je določeno v Skupnem sporočilu z dne 14. junija 2019 o izvajanju akcijskega načrta proti dezinformacijam[69], je delo na več

[61] Belgija, Bolgarija, Češka, Danska, Nemčija, Estonija, Irska, Španija, Francija, Italija, Ciper, Latvija, Litva, Madžarska, Nizozemska, Avstrija, Poljska, Portugalska, Romunija, Slovenija, Slovaška, Finska, Švedska in Združeno kraljestvo (stanje na dan 24. julija 2019).

[62] Slovenija je poslala uradno obvestilo o delnem prenosu. Španija ni poslala uradnega obvestila o prenosu (stanje na dan 24. julija 2019).

[63] Poljska je poslala uradno obvestilo o delnem prenosu. Grčija in Luksemburg nista poslala uradnega obvestila o prenosu (stanje na dan 24. julija 2019).

[64] Belgija, Češka, Estonija, Litva, Poljska, Portugalska, Švedska in Združeno kraljestvo so poslali uradno obvestilo o delnem prenosu. Nemčija, Irska, Grčija, Španija, Ciper, Luksemburg, Madžarska, Nizozemska, Romunija, Slovenija, Slovaška in Finska niso poslali uradnega obvestila o prenosu (stanje na dan 24. julija 2019).

[65] Latvija, Portugalska, Slovenija in Finska so poslale uradno obvestilo o delnem prenosu. Grčija in Španija nista poslali uradnega obvestila o prenosu. Čeprav je Nemčija poslala uradno obvestilo o popolnem prenosu, Komisija meni, da ta prenos ni zaključen (stanje na dan 24. julija 2019).

[66] Belgija in Madžarska sta delno prenesli Direktivo (stanje na dan 24. julija 2019).

[67] Belgija, Bolgarija, Češka, Danska, Nemčija, Estonija, Irska, Španija, Francija, Italija, Ciper, Latvija, Litva, Madžarska, Nizozemska, Avstrija, Poljska, Portugalska, Romunija, Slovenija, Slovaška, Finska, Švedska in Združeno kraljestvo (stanje na dan 24. julija 2019).

[68] Glej akcijski načrt proti dezinformacijam (JOIN(2018) 36 final z dne 5. decembra 2018).

[69] JOIN (2019) 12 final z dne 14. junija 2019.

področjih, ki se medsebojno dopolnjujejo, pripomoglo k zaprtju prostora za dezinformacije in ohranjanju integritete volitev v Evropski parlament.

Evropski svet je v svojih sklepih z dne 21. junija 2019[70] pozdravil namero Komisije, da natančno oceni izvajanje zavez, ki so jih v skladu s **kodeksom ravnanja proti dezinformacijam**[71] sprejele spletne platforme in drugi podpisniki ter Komisijo in visoko predstavnico Unije za zunanje zadeve in varnostno politiko pozval, naj stalno ocenjujeta in se ustrezno odzoveta na „spreminjajoče se narave groženj in vse večje nevarnosti zlonamernih motenj in spletnih manipulacij, povezanih z razvojem umetne inteligence in tehnik zbiranja podatkov“.

Komisija in visoka predstavnica bosta svoje delo na tem področju nadaljevali v skladu s sklepi Evropskega sveta. Komisija in visoka predstavnica sta marca 2019 vzpostavili **sistem hitrega obveščanja** med institucijami EU in državami članicami, da bi se olajšala izmenjava spoznanj v zvezi z dezinformacijskimi kampanjami in usklajevanje odzivov. Prvo srečanje kontaktnih točk držav članic po volitvah v Evropski parlament je potekalo 3. in 4. junija 2019 v Talinu. Za nadaljnjo krepitev sistema hitrega obveščanja bosta visoka predstavnica in Komisija v tesnem sodelovanju z državami članicami jeseni 2019 pregledali delovanje sistema hitrega opozarjanja. Razvili bodo tudi skupno metodologijo za analizo in razkrivanje dezinformacijskih kampanj ter tesnejša partnerstva z mednarodnimi partnerji, kot sta skupina G7 in NATO.

Delo se nadaljuje tudi v **evropski mreži za sodelovanje na volitvah**[72], ki je na prvem srečanju 7. junija 2019 ocenila volitve v Evropski parlament. Ti razmisleki in nadaljnji prispevki ustreznih nacionalnih organov, političnih strank in spletnih platform bodo prispevali k celovitemu poročilu o volitvah v Evropski parlament, ki ga bo Komisija sprejela oktobra 2019. Države članice so mrežo uporabile v zvezi z volitvami, ki niso volitve v Evropski parlament, kar poudarja njeno širšo uporabnost za zagotavljanje integritete demokracije v EU.

Komisija bo tudi nadalje spremljala in spodbujala izvajanje zavez, ki so jih platforme sprejele v **kodeksu ravnanja proti dezinformacijam**.

Iz poročil, ki so jih Google, Twitter in Facebook predložili na podlagi kodeksa ravnanja, je

---

70 https://www.consilium.europa.eu/media/39960/20-21-euco-final-conclusions-sl.pdf. Poziv Evropskega sveta temelji na prispevku romunskega predsedstva Sveta ter Komisije in visokega predstavnika za zunanje zadeve in varnostno politiko k pridobljenim izkušnjam v zvezi z dezinformacijami ter zagotavljanjem svobodnih in poštenih volitev, vključno s skupnim sporočilom o izvajanju akcijskega načrta proti dezinformacijam.

71 Kodeks ravnanja so oktobra 2018 podpisale spletne platforme Facebook, Google in Twitter, Mozilla, pa tudi oglaševalci in oglaševalska industrija, določa pa samoregulativne standarde za boj proti dezinformacijam. Namen kodeksa je izpolniti cilje iz sporočila Komisije o boju proti dezinformacijam na spletu iz aprila 2018 (COM(2018) 236 final z dne 26. aprila 2018) z določitvijo najrazličnejših zavez, in sicer od preglednosti v političnem oglaševanju do zaprtja lažnih računov in demonetizacije glavnih virov dezinformacij.

72 Evropska mreža za sodelovanje na volitvah združuje kontaktne točke nacionalnih mrež za volilno sodelovanje organov, pristojnih za volilne zadeve, ter organov, pristojnih za spremljanje in izvrševanje pravil v zvezi s spletnimi dejavnostmi, pomembnimi za volilni kontekst. Evropska mreža za sodelovanje na volitvah se uporablja za opozarjanje o grožnjah, izmenjavo dobre prakse med nacionalnimi mrežami, razpravo o skupnih rešitvah za opredeljene izzive ter spodbujanje skupnih projektov in vaj med nacionalnimi mrežami.

razvidno, da so vse platforme ukrepale pred volitvami v Evropski parlament z označevanjem političnih oglasov in njihovo javno dostopnostjo prek knjižnic oglasov, ki omogočajo iskanje. Hkrati obstajajo možnosti za izboljšave, kot je opredelila skupina evropskih regulatorjev za avdiovizualne medijske storitve[73]. Zlasti še vedno ni dostopa do podrobnih neobdelanih podatkov, potrebnih za celovito spremljanje. Nazadnje, platforme bi morale v skladu s pravili o varstvu osebnih podatkov raziskovalni skupnosti zagotoviti ustrezen dostop do podatkov. Komisija bo še letos izvedla celovito oceno izvajanja vseh zavez na podlagi kodeksa ravnanja v njegovem prvem 12-mesečnem obdobju. Na podlagi tega lahko prouči nadaljnje ukrepe, tudi regulativne narave, za izboljšanje dolgoročnega odziva EU na dezinformacije.

3. Pripravljenost in varovanje

Krepitev obrambe in odpornosti pred varnostnimi grožnjami je pomemben vidik prizadevanj za učinkovito in pravo varnostno unijo. To vključuje podporo, ki jo Komisija zagotavlja državam članicam in njihovim lokalnim organom pri krepitvi **varovanja javnih prostorov**[74], pa tudi podporo državam članicam pri izboljšanju pripravljenosti na **kemična, biološka, radiološka in jedrska varnostna tveganja**[75], izvajanju obeh akcijskih načrtov na tem področju, pa tudi analizo potreb po povezanih odzivnih zmogljivostih, ki jih je treba razviti v okviru sistema rescEU[76]. Kar zadeva vse večje kemijske grožnje[77], je Komisija v sodelovanju z državami članicami in posvetovanju z mednarodnimi partnerji pripravila seznam kemikalij, ki vzbujajo največjo skrb glede zlorabe v teroristične namene. Seznam EU je podlaga za nadaljnje delo za zmanjšanje dostopa do teh kemikalij in sodelovanje s proizvajalci pri izboljšanju zmogljivosti odkrivanja.

S tehnologijami za brezpilotne zrakoplove je mogoče izvajati najrazličnejše operacije. **Brezpilotni zrakoplovi** zaradi hitre širitve v zadnjih letih na trgu sistemov brezpilotnih zrakoplovov za vojaške, civilne komercialne in prostočasne namene predstavljajo priložnost, pa tudi vse večjo varnostno grožnjo za kritično infrastrukturo (vključno z letalstvom), javne prostore in dogodke ter občutljiva mesta in posameznike. V Evropi so bili brezpilotni zrakoplovi uporabljeni za motenje letalskih operacij in operacij organov kazenskega pregona, nadzor nad kritično infrastrukturo ter tihotapljenje tihotapskega blaga v zapore in čez meje.

---

[73] Skupina evropskih regulatorjev za avdiovizualne medijske storitve združuje vodje ali predstavnike nacionalnih neodvisnih regulativnih organov na področju avdiovizualnih storitev na visoki ravni, ki Komisiji svetujejo pri izvajanju direktive EU o avdiovizualnih medijskih storitvah (Direktiva 2010/13/EU z dne 10. marca 2010). Skupina je na svojem zadnjem srečanju 20. in 21. junija 2019 v Bratislavi predstavila rezultate dosedanjega dela na področju dezinformacij s poudarkom na volitvah v Evropski parlament leta 2019 ter povezanih področjih političnega in tematskega oglaševanja.

[74] Glej „Dobre prakse za javne organe in zasebne upravljavce za krepitev varnosti javnih prostorov“ iz Osemnajstega poročila o nadaljnjem napredku pri vzpostavljanju učinkovite in prave varnostne unije (COM(2019) 145 final z dne 20. marca 2019). To temelji na akcijskem načrtu za podporo pri varovanju javnih prostorov iz oktobra 2017 (COM(2017) 612 final z dne 18. oktobra 2017). Dne 5. junija 2019 je potekalo tretje srečanje foruma za upravljavce v okviru foruma EU o varovanju javnih prostorov. Združilo je predstavnike držav članic EU in zasebne izvajalce javnih prostorov, zastopane prek 14 evropskih združenj, ki zajemajo gostinski sektor, izvedbe v živo, glasbo in zabavo, zabaviščne parke in atrakcije, letalstvo, železniški promet, trgovske centre, telekomunikacije, pa tudi zasebne varnostne službe in proizvajalce varnostne opreme.

[75] Zlasti z izvajanjem akcijskega načrta za okrepitev pripravljenosti na kemična, biološka, radiološka in jedrska varnostna tveganja iz oktobra 2017 (COM(2017) 610 final z dne 18. oktobra 2017).

[76] Glej člen 12(2) Sklepa št. 1313/2013/EU z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite, kakor je bil spremenjen s Sklepom (EU) 2019/420 z dne 13. marca 2019.

[77] Glej „Okrepljeni ukrepi proti kemičnim grožnjam“ iz Petnajstega poročila o napredku pri vzpostavljanju učinkovite in prave varnostne unije (COM(2018) 470 final z dne 13. junija 2018).

Komisija podpira države članice pri preprečevanju vse večje grožnje, ki jo brezpilotni zrakoplovi predstavljajo državljanom in kritičnim družbenim funkcijam, ne da bi zavrgli njihovo koristno uporabo, na primer pri operacijah odzivanja v izrednih razmerah. Pred kratkim je sprejela **skupna pravila o varnem delovanju brezpilotnih zrakoplovov na ravni EU**[78] za zmanjšanje tveganja njihove zlonamerne uporabe, ki vključujejo določbe, s katerimi se zahteva registracija operatorja in ki omogočajo identifikacijo na daljavo. Poleg tega Komisija podpira države članice s spremljanjem trendov razvoja grožnje, ki jo predstavljajo brezpilotni zrakoplovi, financiranjem ustreznih raziskovalnih projektov in ukrepov za krepitev zmogljivosti ter olajšanjem izmenjave med državami članicami in drugimi deležniki. Za okrepitev te podpore bo 17. oktobra 2019 organizirala mednarodno konferenco na visoki ravni za preprečevanje tveganj, ki jih predstavljajo brezpilotni zrakoplovi.

Komisija je v odziv na potrebo po širokem pregledu politike EU o **zaščiti kritične infrastrukture**[79] 23. julija 2019 predložila vrednotenje direktive o evropski kritični infrastrukturi[80] kot pravnem okviru za ugotavljanje in določanje evropske kritične infrastrukture ter oceno potrebe za izboljšanje njene zaščite. V vrednotenju je bilo ugotovljeno, da se je od začetka veljavnosti Direktive bistveno spremenil okvir, v katerem delujejo kritične infrastrukture v Evropi, vključno z zakonodajnimi spremembami v sektorjih, zajetih v Direktivi, kot je energetika[81], in da so določbe Direktive zaradi razvitega področja le delno upoštevne. Hkrati države članice še naprej podpirajo politiko EU o zaščiti kritične infrastrukture, ki spoštuje subsidiarnost in zagotavlja dodano vrednost.

4. Zunanja razsežnost

Zaradi čezmejne in globalne narave večine varnostnih groženj, s katerimi se spopada Unija, je sodelovanje z mednarodnimi organizacijami in partnerskimi državami zunaj EU sestavni del prizadevanj za učinkovito in pravo varnostno unijo.

Izkoriščanje prednosti večstranskega sodelovanja je sestavni del tega prizadevanja ter vključuje sodelovanje med EU in OZN, ki je bilo pred kratkim okrepljeno s podpisom **okvira o boju proti terorizmu med OZN in EU** 24. aprila 2019 v New Yorku ob drugem političnem dialogu OZN-EU o boju proti terorizmu na visoki ravni[82]. Okvir spodbuja sodelovanje pri krepitvi zmogljivosti za boj proti terorizmu ter za preprečevanje in boj proti nasilnemu ekstremizmu v Afriki, na Bližnjem vzhodu in v Aziji. V njem so opredeljena področja za sodelovanje med OZN in EU ter prednostne naloge do leta 2020.

Varnostno sodelovanje z Zahodnim Balkanom je posebna regionalna prednostna naloga, v okviru katerega se izvaja več varnostnih prednostnih ukrepov, opredeljenih v strategiji za Zahodni Balkan iz leta 2018[83]. Komisija je v ta namen 4. aprila 2019 organizirala prvo

78 Izvedbena uredba Komisije (EU) 2019/947 z dne 24. maja 2019 o pravilih in postopkih za upravljanje brezpilotnih zrakoplovov (UL L 152, 11.6.2019, str. 45).

79 V celoviti oceni varnostne politike EU iz leta 2017 (SWD(2017) 278 final z dne 26. julija 2017) je bila poudarjena potreba po širokem pregledu politike EU za zaščito kritične infrastrukture.

80 Direktiva Sveta 2008/114/ES z dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe po izboljšanju njene zaščite je namenjena izboljšanju zaščite kritične infrastrukture v Evropski uniji.

81 Zlasti Uredba (EU) 2017/1938 z dne 25. oktobra 2017 o ukrepih za zagotavljanje zanesljivosti oskrbe s plinom in Uredba (EU) 2019/941 z dne 5. junija 2019 o pripravljenosti na tveganja v sektorju električne energije.

82 https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf.

83 COM(2018) 65 final z dne 6. februarja 2018.

srečanje medagencijske projektne skupine za Zahodni Balkan, na katerem so predstavniki sedmih agencij EU izmenjali izkušnje in okrepili operativno sodelovanje s partnerji v regiji, tudi v boju proti organiziranemu kriminalu, terorizmu, strelnemu orožju, drogam, tihotapljenju migrantov in trgovini z ljudmi. V vseh šestih državah Zahodnega Balkana so se začele izvajati raziskave o hibridnih grožnjah. Drugi oprijemljivi primer sodelovanja z regijo je sporazum o statusu evropske mejne in obalne straže med EU in Albanijo, ki je začel veljati 1. maja 2019, čemur je takoj sledila napotitev skupin Evropske agencije za mejno in obalno stražo na mejo z Grčijo. To sta prvi tovrstni sporazum s tretjo državo in napotitev vanjo. Podobni sporazumi bi se morali kmalu podpisati z drugimi državami v regiji.

Poleg tega je bil julija 2019 v Albanijo napoten uradnik za zvezo Europola, da bi še naprej pomagal albanskim organom pri njihovih prizadevanjih za preprečevanje organiziranega kriminala in boj proti njemu. Za okrepitev boja proti trgovini s strelnim orožjem je Komisija 27. junija 2019 predložila vrednotenje akcijskega načrta o **boju proti trgovini s strelnim orožjem** med EU in regijo jugovzhodne Evrope za obdobje 2015–2019[84]. Vrednotenje je pokazalo, da ima sodelovanje dodano vrednost, vendar je bilo v njem poudarjeno, da so potrebna nadaljnja prizadevanja, na primer z vzpostavitvijo učinkovitih nacionalnih koordinacijskih centrov za strelno orožje ali uskladitvijo zbiranja informacij in poročanja o zasegih orožja.

EU enako prednost daje razvoju **sodelovanja z državami Bližnjega vzhoda in Severne Afrike** na področju varnosti. EU je začela varnostni dialog s Tunizijo in Alžirijo. Tretji dialog med EU in Tunizijo o varnosti in boju proti terorizmu je potekal 12. junija v Tunisu, drugi dialog med EU in Alžirijo o varnosti in boju proti terorizmu pa 12. novembra 2018 v Alžiru. Po nedavnem srečanju pridružitvenega sveta 27. junija, na katerem sta EU in Maroko priznala pomen poglobljenega sodelovanja na področju varnosti, da bi se spopadla s skupnimi izzivi, potekajo pogovori za začetek strukturiranega varnostnega dialoga z Marokom. Hkrati potekajo razprave o razvoju strukturiranega varnostnega dialoga z Egiptom, kar je bilo potrjeno tudi na zadnjem uradnem srečanju višjih uradnikov EU in Egipta 10. julija v Kairu.

Komisija je na podlagi mandata Sveta začela neformalne pogovore z večino držav **Bližnjega vzhoda in Severne Afrike**, da bi začela formalna pogajanja o mednarodnem sporazumu o izmenjavi osebnih podatkov med Agencijo Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (**Europol**) ter ustreznimi pristojnimi organi v državah **Bližnjega vzhoda in Severne Afrike** za boj proti hudim kaznivim dejanjem in terorizmu. Komisija v zvezi s tem spodbuja tudi sklenitev neposrednih delovnih dogovorov med Europolom in partnerskimi organi v državah **Bližnjega vzhoda in Severne Afrike**, da se zagotovi formalni okvir za redno sodelovanje na strateški ravni.

EU in **Združene države Amerike** sta tesni in strateški partnerici pri reševanju skupnih groženj in povečanju varnosti. Na srečanju ministrov za pravosodje in notranje zadeve 19. junija 2019 sta ponovno potrdili, da je boj proti terorizmu med njunimi glavnimi prednostnimi nalogami. Kar zadeva sporazum med EU in ZDA o evidenci podatkov o potnikih[85], sta obe strani potrdili pomen sporazuma in se zavezali, da bosta septembra 2019 začeli skupno vrednotenje za oceno njegovega izvajanja v skladu z določbami sporazuma. Obe strani sta se tudi zavezali, da bosta okrepili svoja skupna prizadevanja v boju proti

[84] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190627_com-2019-293-commission-report_sl.pdf.

[85] UL L 215, 11.8.2012, str. 5.

terorizmu, tudi z razširitvijo izmenjave informacij, zbranih na območjih boja, za uporabo v preiskavah in kazenskem pregonu.

Komisija je za okrepitev tega sodelovanja skupaj z Evropskim koordinatorjem za boj proti terorizmu 10. julija 2019 v Bruslju organizirala delavnico o informacijah z bojišča na visoki ravni. Združila je visoke uradnike ministrstev držav članic za obrambo, notranje zadeve in pravosodje, visoke uradnike ZDA, Europola in Eurojusta ter predstavnike mednarodnih organizacij, da so izmenjali mnenja o uporabi informacij z bojišča in skupaj razmislili o postopkovnih, pravnih in operativnih izzivih, s katerimi se trenutno srečujejo pri prizadevanjih, da identificirajo teroriste in jih privedejo pred sodišče. EU in Združene države Amerike so 14. in 15. maja 2019 v Bruslju izvedle tudi dialog o krepitvi zmogljivosti v zvezi s

kemičnimi, biološkimi, radiološkimi in jedrskimi snovmi, da bi uskladile prizadevanja za zmanjšanje groženj z orožjem za množično uničevanje in okrepitev varnosti KBRJ na svetovni ravni.

Sporazum o programu za sledenje financiranja terorističnih dejavnosti med EU in ZDA[86] velja od leta 2010 ter ureja prenos in obdelavo podatkov za namene identifikacije, sledenja in zasledovanja teroristov in njihovih mrež. Sporazum vsebuje jamstva, ki zagotavljajo varstvo podatkov državljanov EU, v njem pa je predviden redni pregled „zaščitnih ukrepov, nadzora in določb o vzajemnosti“. Komisija je v rednem poročilu o vrednotenju[87], objavljenem 22. julija 2019, ugotovila, da se sporazum, vključno z njegovimi bistvenimi zaščitnimi ukrepi in nadzorom, v njeno zadovoljstvo ustrezno izvaja. Pozdravlja stalno preglednost organov Združenih držav Amerike pri izmenjavi informacij, iz česar je razvidna vrednost programa za sledenje financiranju terorističnih dejavnosti v skupnih protiterorističnih prizadevanjih. Informacije, predložene na podlagi sporazuma, so bile ključnega pomena za izvedbo posebnih preiskav v zvezi s terorističnimi napadi na evropskih tleh, vključno z napadi v Stockholmu, Barceloni in Turkuju leta 2017. Države članice in Europol so povečali uporabo mehanizma, zaradi podatkov programa za sledenje financiranju terorističnih dejavnosti pa se je število preiskovalnih sledi v primerjavi s prejšnjim obdobjem poročanja povečalo za sedemkrat. Naslednji skupni pregled sporazuma naj bi se izvedel leta 2021.

Kar zadeva mednarodno sodelovanje pri izmenjavi **evidenc podatkov o potnikih za boj proti terorizmu in hudim kaznivim dejanjem**, sta EU in Kanada na 17. vrhu EU-Kanada v Montrealu 17. in 18. julija 2019 pozdravili zaključek pogajanj o novem sporazumu o evidenci podatkov o potnikih. Potem ko je Kanada opozorila na svojo zahtevo po pravnem pregledu, sta se pogodbenici zavezali, da bosta po navedenem pregledu čim prej dokončali sporazum ter pri tem priznali ključno vlogo sporazuma pri krepitvi varnosti ter zagotavljanju zasebnosti in varstva osebnih podatkov. Kar zadeva veljavni sporazum o evidenci podatkov o potnikih med EU in Avstralijo[88], bo skupina EU obiskala Canberro avgusta 2019 v okviru skupnega pregleda in skupne ocene sporazuma.

Komisija prav tako sodeluje z državami članicami v Svetu v zvezi s stališčem EU za prihodnje 40. zasedanje skupščine **Mednarodne organizacije civilnega letalstva**, ki bo

[86] UL L 195, 27.7.2010, str. 5.
[87] COM(2019) 342 final z dne 22. julija 2019.
[88] UL L 186, 14.7.2012, str. 4.

potekalo od 24 septembra do 4. oktobra 2019. Skupščina bo določila politično usmeritev in Svetu Mednarodne organizacije civilnega letalstva dala navodila o tehničnem delu v zvezi s standardi Mednarodne organizacije civilnega letalstva za obdelavo evidenc podatkov o potnikih. Svet je potrdil informativni dokument, ki ga je Komisija pripravila, da bi opisala stališče Unije v zvezi s temeljnimi načeli, na katerih bi moral temeljiti vsak prihodnji standard glede evidenc podatkov o potnikih. Informativni dokument bo predložen organu v zvezi z njegovimi člani, ki niso države članice EU.

VI. SKLEPNE UGOTOVITVE

EU je zaradi tesnega sodelovanja med Evropskim parlamentom, Svetom, državami članicami in Komisijo v zadnjih letih dosegla znaten napredek pri skupnih prizadevanjih za učinkovito in pravo varnostno unijo, pri čemer se je dogovorila o več prednostnih zakonodajnih pobudah. Države članice ob podpori Komisije izvajajo tudi različne nezakonodajne operativne ukrepe za izboljšanje varnosti za vse državljane. Hkrati je na področju varnostne unije še vedno več prednostnih pobud, ki še niso bile sprejete in v zvezi s katerimi je potrebno nadaljnje ukrepanje sozakonodajalcev za odpravo neposrednih groženj. Komisija Evropski parlament in Svet poziva, naj izvedeta potrebne ukrepe za dosego hitrega dogovora o zakonodajnih predlogih za boj proti teroristični propagandi in radikalizaciji na spletu, izboljšanje kibernetske varnosti, olajšanje dostopa do elektronskih dokazov ter dokončanje dela v zvezi s trdnejšimi in pametnejšimi informacijskimi sistemi za upravljanje varnosti, meja in migracij.

Komisija države članice poziva, naj hitro in v celoti izvajajo vso zakonodajo, sprejeto na področju varnostne unije, in s tem zagotovijo vse njene koristi. Poleg tega jih poziva, naj nadaljujejo in okrepijo ključno delo v zvezi s praktičnimi ukrepi za povečanje varnosti digitalne infrastrukture, boj proti dezinformacijam in drugim grožnjam, ki jih omogoča kibernetski prostor, povečanje pripravljenosti in zaščite ter krepitev sodelovanje z partnerji zunaj Unije pred skupnimi grožnjami. Vsi ti ukrepi skupaj povečujejo varnost vseh državljanov.