



V Bruseli 30. 10. 2019
COM(2019) 552 final

SPRÁVA KOMISIE EURÓPSKEMU PARLAMENTU, EURÓPSKEJ RADE A RADE

**Dvadsať správa o pokroku dosiahnutom pri budovaní účinnej a skutočnej
bezpečnostnej únie**

I. ÚVOD

Táto dvadsiata správa o ďalšom pokroku dosiahnutom pri budovaní účinnej a skutočnej bezpečnostnej únie sleduje vývoj v dvoch hlavných pilieroch: prvým je boj proti terorizmu a organizovanej trestnej činnosti, ako aj proti prostriedkom, ktorými sa podporujú, a druhým je posilňovanie našej obrany a budovanie odolnosti proti týmto hrozbám.

Junckerova Komisia považuje bezpečnosť za svoju najvyššiu prioritu už od prvého dňa svojho pôsobenia. EÚ v nadväznosti na Európsky program v oblasti bezpečnosti z apríla 2015¹ a oznámenie z apríla 2016 o pripravovaní pôdy pre účinnú a skutočnú bezpečnostnú úniu² reagovala na sériu teroristických útokov a ďalšie rastúce bezpečnostné výzvy koordinovaným prístupom a dosiahla v posilňovaní našej kolektívnej bezpečnosti významný pokrok³. Je čoraz jasnejšie, že dnešné bezpečnostné výzvy – či už ide o terorizmus, organizovanú trestnú činnosť, kybernetické útoky, dezinformácie alebo iné vznikajúce kybernetické hrozby – predstavujú spoločné hrozby. Iba spoločným úsilím môžeme dosiahnuť úroveň kolektívnej bezpečnosti, ktorú od nás občania oprávnené požadujú a očakávajú. Toto spoločné chápanie bolo základom pre pokrok dosiahnutý pri budovaní účinnej a skutočnej bezpečnostnej únie. Podpora na úrovni EÚ sa v dôsledku potrieb vnútroštátnych orgánov, ktoré sa usilujú o zaistenie bezpečnosti občanov, zamerala na legislatívne a operačné opatrenia v prípadoch, v ktorých spoločné opatrenia môžu mať vplyv na bezpečnosť členských štátov. Táto činnosť bola vykonaná v úzkej spolupráci s Európskym parlamentom a Radou, a to s úplnou transparentnosťou voči širšej verejnosti. Stredobodom úsilia vynakladaného v tejto súvislosti bolo plné rešpektovanie základných práv, keďže bezpečnosť Únie možno zaistiť len vtedy, ak sa občania budú môcť spoľahnúť na to, že sú ich základné práva plne rešpektované.

EÚ **bojovala proti terorizmu** tým, že obmedzila priestor, v ktorom teroristi pôsobia, pričom nové pravidlá im sťažujú prístup k výbušniam, k strelným zbraňam a financovaniu a obmedzujú ich pohyb. Zintenzívnila **výmenu informácií** s cieľom poskytnúť tým, ktorí sú v prvej línii, t. j. príslušníkom polície a pohraničnej strážne, účinný prístup k presným a úplným údajom, a tak čo najlepšie využívať existujúce informácie a odstraňovať medzery a slepé miesta. Predpokladom zaistenia bezpečnosti v priestore voľného pohybu bez kontroly vnútorných hraníc je dôsledná ochrana vonkajších hraníc. Európsky parlament a Rada dosiahli v marci 2019 dohodu o ďalšej posilnenej a plne vybavenej **európskej pohraničnej a pobrežnej strážne** a očakáva sa, že nové nariadenie nadobudne účinnosť začiatkom decembra 2019. EÚ poskytla platformu a finančné prostriedky pre tých, ktorí pôsobia v miestnych komunitách, aby si vymieňali najlepšie postupy v oblasti **boja proti radikalizácii a predchádzania násilnému extrémizmu**, a zároveň navrhla nové pravidlá na účinné odstraňovanie teroristického obsahu online. Vďaka podpore EÚ prostredníctvom akčných plánov na podporu ochrany verejných priestorov a zlepšenie pripravenosti na chemické, biologické, rádiologické a jadrové bezpečnostné riziká sa **mestá stali odolnejšími** voči útokom. EÚ riešila otázku **kybernetickej bezpečnosti a kybernetických hrozieb** tým, že zaviedla novú stratégiu kybernetickej bezpečnosti EÚ, prijala príslušné právne predpisy a odstraňuje **dezinformácie** s cieľom lepšie chrániť naše voľby. Ďalšie úsilie sa vynakladá na posilňovanie bezpečnosti našej **digitálnej kritickej infraštruktúry** vrátane posilnenej spolupráce v oblasti **kybernetickej bezpečnosti sietí 5G** v celej Európe.

¹ COM(2015) 185 final z 28. 4. 2015.

² COM(2016) 230 final z 20. 4. 2016.

³ Predchádzajúce správy o pokroku dosiahnutom pri budovaní účinnej a skutočnej bezpečnostnej únie: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

Je však potrebné vykonať ešte veľa práce. Útok na synagógu naživo vysielaný na internete 9. októbra 2019 v nemeckom meste Halle, pri ktorom boli zabití dvaja občania, šokujúcim spôsobom pripomenul hrozbu, ktorú predstavuje pravicový násilný extrémizmus a antisemitizmus. Tento útok takisto opätovne upozornil na zneužívanie internetu na teroristickú propagandu a poukázal teda na potrebu zaviesť v celej EÚ **pravidlá pre odstraňovanie teroristického obsahu online**. Rada pre spravodlivosť a vnútorné veci 7. – 8. októbra 2019 diskutovala o pravicovom násilnom extrémizme a terorizme, pričom zdôraznila, že je potrebné vyvíjať ďalšie úsilie, a to aj v oblasti boja proti šíreniu nezákonného obsahu pravicového extrémizmu online a offline. Zabitie troch príslušníkov polície a ďalšej zamestnankyne policajného ústredia v Paríži 3. októbra 2019 zároveň svedčí o tom, že hrozba terorizmu inšpirovaného džihádcom je naďalej reálna a že je potrebné pokračovať v podpore členských štátov pri riešení tejto hrozby. Únik uväznených členov organizácie ISIS/Dá'iš, ku ktorému došlo počas nedávnych udalostí v severnej Sýrii, by mohol mať na bezpečnosť v Európe vážny vplyv. Je dôležité, aby členské štáty plne využívali existujúce informačné systémy na odhaľovanie a identifikáciu zahraničných teroristických bojovníkov pri prekračovaní vonkajších hraníc. Naďalej sa pracuje aj na využívaní informácií z bojísk na účely trestného stíhania zahraničných teroristických bojovníkov.

V tejto správe sa uvádza nedávny pokrok dosiahnutý v úsilí o vytvorenie účinnej a skutočnej bezpečnostnej únie, pričom sa zdôrazňujú oblasti, v ktorých sú potrebné ďalšie opatrenia. Poskytujú sa v nej aktuálne informácie o vykonávaní dohodnutých opatrení v oblasti **kybernetickej bezpečnosti sietí 5G**, najmä o **správe EÚ o hodnotení rizika** uverejnenej 9. októbra 2019 a o **odstraňovaní dezinformácií**.

Táto správa sa zameriava najmä na **vonkajší rozmer** spolupráce v bezpečnostnej únii so zreteľom na podpísanie dvoch dvojstranných **dohôd o boji proti terorizmu s Albánskom a Severomacedónskou republikou** a pokrok, ktorý bol dosiahnutý v spolupráci s partnermi z tretích krajín pri výmene **údajov zo záznamov o cestujúcich**. Okrem toho Komisia spolu s touto správou prijala žiadosť o povolenie začať rokovania o dohode medzi EÚ a **Novým Zélandom** o výmene osobných údajov na účely boja proti závažnej trestnej činnosti a terorizmu.

II. PLNENIE LEGISLATÍVNYCH PRIORÍT

1. *Predchádzanie radikalizácii online a v komunitách*

Základom reakcie Únie na hrozby, ktoré predstavuje terorizmus, je **predchádzanie radikalizácii**. Internet je v tejto súvislosti najvýznamnejším bojiskom, na ktorom pôsobia teroristi v 21. storočí. Priestor, v ktorom môžu radikalizovaní jednotlivci komunikovať a zdieľať obsah, umožňuje rozvoj svetových, rozširujúcich sa sietí džihádistov a pravicových násilných extrémistov. Komisia preto proti radikalizácii online i naďalej uplatňuje dvojúrovňový prístup, v rámci ktorého by navrhované pravidlá pre odstraňovanie nezákonného teroristického obsahu online mali posilniť dobrovoľné partnerstvo s online platformami.

V tejto súvislosti má zásadný význam **legislatívny návrh na zabránenie šíreniu teroristického obsahu online** s jasnými pravidlami a zárukami, vďaka ktorým by internetové platformy boli povinné odstrániť teroristický obsah do jednej hodiny od prijatia odôvodnenej žiadosti príslušných orgánov, a prijať proaktívne opatrenia primerané úrovni vystavenia teroristickému obsahu⁴. Momentálne prebiehajú medziinštitucionálne rokovania medzi Európskym parlamentom a Radou, v rámci ktorých sa 17. októbra 2019 konalo prvé zasadnutie trialógu. Vzhľadom na

⁴ COM(2018) 640 final z 12. 9. 2018.

hrozbu, ktorú predstavuje teroristický obsah online, Komisia vyzýva spoluzákonodarcov, aby dohodu o navrhovaných právnych predpisoch dosiahli do konca roka 2019.

Navrhované právne predpisy dopĺňajú dobrovoľné partnerstvo s internetovým odvetvím a inými zainteresovanými stranami v rámci **internetového fóra EÚ**. Fórum už od svojho vzniku v roku 2015 podnecuje internetové spoločnosti k tomu, aby aktívne podnikali kroky na identifikáciu a odstraňovanie teroristického obsahu online, čím pripravilo pôdu pre iniciatívu pod vedením priemyselného odvetvia s názvom „spoločná databáza hashov“⁵ a zriadenie Globálneho internetového fóra na boj proti terorizmu. Jednotka EÚ pre nahlasovanie internetového obsahu, ktorá je súčasťou Europolu, agentúry EÚ pre presadzovanie práva, zohrala kľúčovú úlohu pri posilňovaní spolupráce s internetovými spoločnosťami a prispievala k celkovým cieľom internetového fóra EÚ. Na poslednom zasadnutí internetového fóra EÚ na úrovni ministrov, ktoré sa konalo 7. októbra 2019, sa členské štáty EÚ a vysokí predstavitelia internetových spoločností zaviazali spolupracovať v rámci tzv. **krízového protokolu EÚ**. V krízovom protokole EÚ sa stanovujú kritériá pre posilnenú spoluprácu a zavádzajú sa nové spôsoby zlepšenia reakcie na krízy. Je to súčasť medzinárodného úsilia o realizáciu „Výzvy na činnosť z Christchurch“⁶ s cieľom zabezpečiť koordinovanú a rýchlu reakciu v záujme zabránenia šíreniu virálneho teroristického alebo násilného extrémistického obsahu online.

Okrem opatrení na riešenie radikalizácie online Komisia pokračuje v podpore úsilia, ktoré sa na vnútroštátnej a miestnej úrovni **vynakladá v snahe predchádzať radikalizácii a bojovať proti nej na mieste**. Na základe bohatých skúseností a odborných poznatkov získaných v rámci siete na zvyšovanie povedomia o radikalizácii EÚ poskytuje cieleňú podporu miestnym aktérom vrátane miest⁷ a poskytuje príležitosti na výmenu skúseností medzi odborníkmi z praxe, výskumníkmi a tvorcami politík. Táto sieť napríklad vydala osobitné usmernenia a zorganizovala semináre na podporu príslušných orgánov pri zaobchádzaní s deťmi, ktoré pochádzajú z konfliktných oblastí⁸. S cieľom zabezpečiť kontinuitu činností vykonávaných v rámci siete na zvyšovanie povedomia o radikalizácii začala Komisia postup pre novú rámcovú zmluvu v odhadovanej hodnote 61 miliónov eur na obdobie štyroch rokov počnúc rokom 2020⁹.

V snahe eliminovať hrozbu, ktorú predstavuje teroristický obsah online, Komisia vyzýva Európsky parlament a Radu, aby:

- **do konca roka ukončili rokovania o legislatívnom návrhu na predchádzanie šíreniu teroristického obsahu online.**

⁵ Nástroj vytvorený konzorciom spoločností na uľahčenie spolupráce s cieľom zabrániť šíreniu teroristického obsahu v rámci platforiem.

⁶ V reakcii na útoky v novozélandskom meste Christchurch, ku ktorým došlo 15. marca 2019, pozval francúzsky prezident Emmanuel Macron a novozélandská predsedníčka vlády Jacinda Ardernová 15. mája 2019 vedúcich predstaviteľov a online platformy do Paríža, aby spustili „Výzvu na činnosť z Christchurch“. Predseda Juncker výzvu podporil a oznámil vypracovanie krízového protokolu EÚ.

⁷ Pokiaľ ide o spoluprácu s mestami v oblasti bezpečnosti, pozri aj oddiel V.2 o pripravenosti a ochrane, a najmä o ochrane verejných priestorov.

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 Rámcová zmluva je rozdelená na dve časti: 29 000 000 eur na podporu činností siete na zvyšovanie povedomia o radikalizácii na nasledujúce štyri roky a 32 000 000 eur na posilnenie kapacít členských štátov, vnútroštátnych, regionálnych a miestnych orgánov a prioritných tretích krajín na účinné odstraňovanie radikalizácie, a to najmä poskytovaním príležitostí na nadväzovanie kontaktov, cieleňých služieb vychádzajúcich z potrieb a výskumu a analýz.

2. *Silnejšie a inteligentnejšie informačné systémy v oblasti bezpečnosti, riadenia hraníc a migrácie*

EÚ zintenzívnila výmenu informácií s cieľom uľahčiť boj proti podvodom s osobnými údajmi¹⁰, posilniť hraničné kontroly¹¹, modernizovať celoeurópske databázy presadzovania práva¹², odstrániť informačné medzery¹³ a posilniť agentúru EÚ pre presadzovanie práva Europol¹⁴. Kľúčom k tomu je **interoperabilita informačných systémov EÚ**¹⁵, ktorá zabezpečuje čo najlepšie využitie existujúcich informácií a odstránenie slepých miest. Interoperabilita, ktorá reaguje na potreby tých, ktorí pracujú v prvej línii, povedie k rýchlejšiemu, systematickejšiemu prístupu k informáciám pre príslušníkov orgánov presadzovania práva, príslušníkov pohraničnej stráže a migračných úradníkov, čím prispeje k zlepšeniu vnútornej bezpečnosti a riadenia hraníc.

Vďaka interoperabilite a všetkým inováciám, ktoré so sebou prináša, sa situácia v oblasti bezpečnosti, riadenia hraníc a migrácie v praxi zmení len vtedy, ak každý členský štát bude vykonávať príslušné právne predpisy v plnej miere. Preto je **zavádzanie** interoperability v bezpečnostnej únii najvyššou prioritou, a to na politickej aj technickej úrovni. Komisia a Agentúra EÚ na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti (eu-LISA) podporujú členské štáty na základe odborných znalostí a výmeny najlepších postupov, pričom využívajú sieť vnútroštátnych koordinátorov a vypracúvajú tabuľku výsledkov s cieľom umožniť účinné monitorovanie a koordináciu. Úzka spolupráca medzi agentúrami EÚ, všetkými členskými štátmi a krajinami pridruženými k schengenskému priestoru bude mať prvoradý význam z hľadiska splnenia ambiciózneho cieľa, ktorým je dosiahnuť do roku 2020 úplnú interoperabilitu informačných systémov EÚ pre oblasť bezpečnosti, riadenia hraníc a riadenia migrácie.

¹⁰ Nariadenie (EÚ) 2019/1157 z 20. júna 2019 o posilnení zabezpečenia preukazov totožnosti občanov Únie a dokladov o pobyte vydávaných občanom Únie a ich rodinným príslušníkom vykonávajúcim svoje právo na voľný pohyb.

¹¹ Zavedenie systematických kontrol všetkých občanov na vonkajších hraniciach pri využití Schengenského informačného systému. Všetky schengenské štáty, ako aj Rumunsko, Bulharsko, Chorvátsko a Cyprus uplatňujú pravidlá systematických kontrol na vonkajších hraniciach s použitím príslušných databáz, ktoré boli zavedené v apríli 2017. Vzhľadom na neúmerný vplyv na plynulosť premávky sú na pozemných alebo námorných hraniciach v súlade s týmito pravidlami možné dočasné odchýlky, avšak iba pokiaľ ide o občanov EÚ. V súčasnosti takéto odchýlky oznámilo šesť členských štátov/krajín pridružených k schengenskému priestoru (Chorvátsko, Fínsko, Maďarsko, Lotyšsko, Nórsko a Slovinsko). Pokiaľ ide o vzdušné hranice, možnosť odchýliť sa od pravidiel systematických kontrol uplynula v apríli 2019.

¹² Posilnený Schengenský informačný systém [nariadenie (EÚ) 2018/1860 z 28. novembra 2018, nariadenie (EÚ) 2018/1861 z 28. novembra 2018, nariadenie (EÚ) 2018/1862 z 28. novembra 2018] a Európsky informačný systém registrov trestov rozšírený na štátnych príslušníkov tretích krajín [nariadenie (EÚ) 2019/816 zo 17. apríla 2019]. Posilnenie Schengenského informačného systému zahŕňa všeobecnú povinnosť vkladať do systému zápisy súvisiace s terorizmom.

¹³ Systém EÚ vstup/výstup [nariadenie (EÚ) 2017/2226 z 30. novembra 2017] a európsky systém pre cestovné informácie a povolenia [nariadenie (EÚ) 2018/1240 z 12. septembra 2018 a nariadenie (EÚ) 2018/1241 z 12. septembra 2018].

¹⁴ V posledných rokoch sa úloha Europolu výrazne posilnila z hľadiska rozsahu aj hĺbky. Agentúra bola posilnená prijatím nariadenia o Europole v roku 2016 [nariadenie (EÚ) 2016/794 z 11. mája 2016]. Členské štáty výrazne zvýšili objem informácií poskytovaných Europolu a prostredníctvom neho. Zriadením Centra Europolu pre boj proti terorizmu (ECTC) sa posilnili analytické spôsobilosti Europolu v prípadoch terorizmu. Rozpočet Europolu sa za posledné roky neustále zvyšoval, a to z 82 miliónov eur v roku 2014 na 138 miliónov eur v roku 2019. Prebiehajú rokovania o rozpočte na rok 2020.

¹⁵ Nariadenie (EÚ) 2019/817 z 20. mája 2019) a nariadenie (EÚ) 2019/818 z 20. mája 2019).

Európsky parlament a Rada medzitým ešte musia v tejto súvislosti **dokončiť legislatívny proces**. Na zabezpečenie úplného a včasného zavádzania interoperability je nevyhnutná rýchla dohoda o všetkých prerokovaných legislatívnych návrhoch. Po prvé, v rámci technickej realizácie **európskeho systému pre cestovné informácie a povolenia** sú potrebné technické zmeny súvisiacich nariadení¹⁶, aby bol systém plne zavedený. Komisia vyzýva Európsky parlament, aby prácu na týchto technických zmenách urýchlil s cieľom začať medziinštitucionálne rokovania čo najskôr. Po druhé, stále prebiehajú medziinštitucionálne rokovania o návrhu z mája 2018 na posilnenie a modernizáciu existujúceho **vízového informačného systému**¹⁷. Na základe prvého zasadnutia trialógu, ktoré sa konalo 22. októbra 2019, Komisia vyzýva oboch spoluzákonodarcov, aby rokovania urýchlene uzavreli. Po tretie, ešte nebola dosiahnutá dohoda o návrhu Komisie z mája 2016 na rozšírenie rozsahu pôsobnosti systému **Eurodac**¹⁸ tak, aby sa uchovávali odtlačky prstov a príslušné údaje nielen v prípade žiadateľov o azyl a osôb zadržaných v súvislosti s neoprávneným prekročením vonkajších hraníc, ale aj v prípade neoprávnene sa zdržiavajúcich štátnych príslušníkov tretích krajín. Navrhovanými zmenami by sa takisto predĺžilo obdobie uchovávania odtlačkov prstov a príslušných údajov osôb, ktoré neoprávnene vstúpili na územie EÚ. Komisia vyzýva spoluzákonodarcov, aby pristúpili k prijatiu návrhu.

V záujme posilnenia informačných systémov EÚ v oblasti bezpečnosti, riadenia hraníc a migrácie Komisia vyzýva Európsky parlament a Radu, aby:

- pokračili v úsilí o rýchle dosiahnutie dohody o navrhovaných technických zmenách, ktoré sú potrebné na zriadenie **Európskeho systému pre cestovné informácie a povolenia**,
- urýchlene uskutočnili a uzavreli rokovania o návrhu na posilnenie existujúceho **vízového informačného systému**,
- prijali legislatívny návrh týkajúci sa systému **Eurodac** (*Priorita uvedená v rámci spoločného vyhlásenia*).

3. Obmedzenie priestoru, v ktorom pôsobia teroristi

EÚ prijala prísne opatrenia na obmedzenie priestoru, v ktorom pôsobia teroristi, a to zavedením nových pravidiel, ktoré teroristom a iným páchatelom trestnej činnosti sťažujú prístup k výbušniam¹⁹, k strelným zbraňam a financovaniu²⁰, a na obmedzenie ich pohybu²¹.

V záujme posilnenia súdnej reakcie na terorizmus zriadila Agentúra EÚ pre justičnú spoluprácu v trestných veciach (Eurojust) 1. septembra 2019 **Európsky súdny protiteroristický register**. Register bude zhromažďovať súdne informácie v snahe vytvárať prepojenia v konaniach proti osobám podozrivým z teroristických trestných činov, čím sa posilní koordinácia medzi prokurátormi pri vyšetrovaní terorizmu s možnými cezhraničnými dôsledkami.

Na podporu a uľahčenie vyšetrovania v cezhraničných prípadoch je však potrebné ďalšie úsilie, najmä v súvislosti s **prístupom** orgánov presadzovania práva k **elektronickým dôkazom**. Pokiaľ ide o legislatívne návrhy z apríla 2018, ktorých cieľom je zlepšiť cezhraničný prístup k elektronickým

¹⁶ Nariadenie (EÚ) 2018/1240 z 12. septembra 2018 a nariadenie (EÚ) 2018/1241 z 12. septembra 2018).

¹⁷ COM(2018) 302 final zo 16. 5. 2018.

¹⁸ COM(2016) 272 final zo 4. 5. 2016.

¹⁹ Nariadenie (EÚ) 2019/1148 z 20. júna 2019 o uvádzaní prekurzorov výbušnín na trh a ich používaní. Nariadenie nadobudlo účinnosť 31. júla 2019 a uplatňuje sa 18 mesiacov po nadobudnutí jeho účinnosti.

²⁰ Smernica (EÚ) 2019/1153 z 11. júla 2019), ktorou sa stanovujú pravidlá uľahčovania využívania finančných a iných informácií na predchádzanie určitým trestným činom, ich odhaľovanie, vyšetrovanie alebo stíhanie.

²¹ Zavedenie systematických kontrol všetkých občanov na vonkajších hraniciach pri využití Schengenského informačného systému.

dôkazom pri vyšetrowaní trestných činov²², Európsky parlament ešte musí prijať svoju rokovaciu pozíciu predtým, ako spoluzákonodarcovia začnú rokovania. Komisia vyzýva Európsky parlament, aby v súvislosti s týmto legislatívnym návrhom pokročil tak, aby spoluzákonodarcovia mohli pracovať na jeho rýchlom prijatí. V záujme zlepšenia cezhraničného prístupu k elektronickým dôkazom sa Komisia na základe svojho návrhu vnútorných pravidiel EÚ takisto zapája do **medzinárodných rokovaní**. Komisia a orgány Spojených štátov uskutočnili 25. septembra 2019 prvé formálne kolo rokovaní o **dohode medzi EÚ a USA o cezhraničnom prístupe k elektronickým dôkazom**. Ďalšie kolo je naplánované na 6. novembra 2019. Komisia sa v kontexte prebiehajúcich rokovaní o **Druhom dodatkovom protokole k budapeštianskemu dohovoru Rady Európy o počítačovej kriminalite** zúčastnila v mene Únie na troch rokovaníach, a to v júli, septembri a októbri 2019. Hoci sa na týchto rokovaníach dosiahol značný pokrok, stále však treba riešiť niekoľko hlavných tém, ktoré sú pre Úniu predmetom značného záujmu, ako sú záruky ochrany údajov. Rokovania o druhom dodatkovom protokole budú pokračovať aj v novembri 2019 a počas celého roka 2020. Dôležité je rýchlo napredovať v oboch rokovaníach s cieľom prehĺbiť medzinárodnú spoluprácu v oblasti výmeny elektronických dôkazov a zároveň zabezpečiť súlad s právnymi predpismi EÚ a povinnosťami členských štátov, ktoré z nich vyplývajú, pri súčasnom zohľadnení budúceho vývoja práva EÚ.

Vzhľadom na pretrvávajúce obavy týkajúce sa prania špinavých peňazí Európsky parlament prijal 19. septembra 2019 **uznesenie o stave vykonávania právnych predpisov Únie v oblasti boja proti praniu špinavých peňazí**²³, ktorým reaguje na súbor štyroch správ o boji proti praniu špinavých peňazí, ktoré Komisia prijala 24. júla 2019²⁴. Európsky parlament vyzval členské štáty, aby zabezpečili riadne a rýchle vykonávanie smerníc o boji proti praniu špinavých peňazí. Európsky parlament takisto vyzval Komisiu, aby posúdila, či by nariadenie o boji proti praniu špinavých peňazí bolo vhodnejšie ako smernica, a aby posúdila potrebu koordinačného a podporného mechanizmu pre finančné spravodajské jednotky.

V záujme zlepšenia prístupu k elektronickým dôkazom pri presadzovaní práva Komisia vyzýva Európsky parlament a Radu, aby:

- dosiahli rýchlu dohodu o legislatívnych návrhoch týkajúcich sa **elektronických dôkazov** (*Priorita uvedená v rámci spoločného vyhlásenia*).

4. Posilnenie kybernetickej bezpečnosti

Posilnenie kybernetickej bezpečnosti zostáva kľúčovým aspektom úsilia o vytvorenie skutočnej a účinnej bezpečnostnej únie. Vykonávaním stratégie kybernetickej bezpečnosti EÚ z roku 2017²⁵ Únia posilnila svoju odolnosť tým, že sa stala rezistentnejšou voči útokom a je schopná sa rýchlejšie zotaviť, ako aj odradzujúci efekt tým, že zvýšila šance, aby boli útočníci chytení a potrestaní, a to aj prostredníctvom rámca pre spoločnú diplomatickú reakciu EÚ na

²² COM(2018) 225 final zo 17. 4. 2018 a COM(2018) 226 final zo 17. 4. 2018.

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

²⁴ Správa o hodnotení rizika prania špinavých peňazí a financovania terorizmu, ktoré má vplyv na vnútorný trh a súvisí s cezhraničnou činnosťou [COM(2019) 370 final z 24. 7. 2019], správa o vzájomnom prepojení vnútroštátnych centralizovaných automatizovaných mechanizmov (centrálnych registrov alebo centrálnych elektronických systémov vyhľadávania údajov) členských štátov v oblasti bankových účtov [COM(2019) 372 final z 24. 7. 2019], správa o posúdení nedávnych prípadov údajného prania špinavých peňazí týkajúcich sa úverových inštitúcií EÚ [COM(2019) 373 final z 24. 7. 2019], správa o posúdení rámca pre spoluprácu medzi finančnými spravodajskými jednotkami [COM(2019) 371 final z 24. 7. 2019].

²⁵ JOIN(2017) 450 final z 13. 9. 2017.

škodlivé kybernetické činnosti. Vykonávaním politického rámca EÚ pre kybernetickú obranu Únia podporuje v kybernetickej obrane aj členské štáty²⁶.

Nadobudnutím účinnosti aktu o kybernetickej bezpečnosti²⁷ v júni 2019 sa formuje **rámec EÚ pre certifikáciu kybernetickej bezpečnosti**. Certifikácia zohráva mimoriadne dôležitú úlohu pri zvyšovaní dôveryhodnosti a bezpečnosti produktov a služieb, ktoré sú rozhodujúce pre fungovanie digitálneho jednotného trhu. Rámec pre certifikáciu poskytne celoeurópske systémy certifikácie ako komplexný súbor pravidiel, technických požiadaviek, štandardov a postupov. Zahŕňa dve skupiny odborníkov, konkrétne európsku skupinu pre certifikáciu kybernetickej bezpečnosti, ktorá zastupuje orgány členských štátov a skupinu zainteresovaných strán pre certifikáciu kybernetickej bezpečnosti, ktorá zastupuje priemysel. Uvedená skupina zainteresovaných strán spája dopyt a ponuku produktov a služieb informačných a komunikačných technológií vrátane malých a stredných podnikov, poskytovateľov digitálnych služieb, európskych a medzinárodných organizácii pre normalizáciu, vnútroštátnych akreditačných orgánov, orgánov dohľadu nad ochranou údajov a orgánov posudzovania zhody.

Európsky parlament a Rada ešte musia dosiahnuť dohodu o legislatívnej iniciatíve²⁸, ktorá sa týka **Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a siete národných koordinačných centier**. Cieľom návrhu je posilniť schopnosť Únie v oblasti kybernetickej bezpečnosti podporovaním európskeho technologického a priemyselného ekosystému kybernetickej bezpečnosti, ako aj koordináciou a združovaním súvisiacich zdrojov. Komisia vyzýva oboch spoluzákonodarcov, aby obnovili a urýchlili uzavrili medziinštitucionálne rokovania o tejto prioritnej iniciatíve na posilnenie kybernetickej bezpečnosti.

Práca na zvyšovaní kybernetickej bezpečnosti zahŕňa podporu na národnej aj regionálnej úrovni²⁹.

Okrem kybernetických hrozieb zacielených na systémy a údaje EÚ naďalej prijíma opatrenia na riešenie komplexných a mnohostranných výziev, ktoré predstavujú **hybridné hrozby**. V Rade bola zriadená horizontálna pracovná skupina pre boj proti hybridným hrozbám s cieľom zlepšiť odolnosť EÚ a jej členských štátov proti hybridným hrozbám a podporiť opatrenia na posilnenie odolnosti spoločností voči kríze. Komisia a Európska služba pre vonkajšiu činnosť podporujú toto úsilie na základe spoločného rámca pre boj proti hybridným hrozbám z roku 2016³⁰ a spoločného oznámenia z roku 2018³¹ o zvyšovaní odolnosti a posilňovanie spôsobilosti riešiť hybridné hrozby. Okrem toho Spoločné výskumné centrum momentálne vytvára koncepčný model, v rámci ktorého budú charakterizované hybridné hrozby s cieľom pomôcť členským štátom a ich príslušným orgánom identifikovať typ hybridného útoku, ktorému by mohli čeliť. Model sa zaoberá spôsobom, akým aktér (štátny alebo neštátny) využíva súbor nástrojov (od dezinformácií po špionáž alebo fyzické operácie) v rôznych oblastiach (hospodárska, vojenská, sociálna, politická oblasť), aby ovplyvnil terč v snahe dosiahnuť celý rad cieľov.

²⁶ Politický rámec EÚ pre kybernetickú obranu (aktualizácia z roku 2018), ktorý Rada prijala 19. novembra 2018 (dokument 14413/18).

²⁷ Nariadenie (EÚ) 2019/881 zo 17. apríla 2019.

²⁸ COM(2018) 630 final z 12. 9. 2018.

²⁹ Komisia napríklad podporuje medziregionálne inovačné partnerstvo v oblasti kybernetickej bezpečnosti, do ktorého sú zapojené Bretónsko, Kastília-León, Severné Porýnie-Vestfálsko, stredné Fínsko a Estónsko, s cieľom vyvinúť európsky hodnotový reťazec kybernetickej bezpečnosti so zameraním na komercializáciu a rozšírenie.

³⁰ JOIN(2016) 18 final zo 6. 4. 2016.

³¹ JOIN(2018) 16 final z 13. 6. 2018.

V záujme posilnenia kybernetickej bezpečnosti Komisia vyzýva Európsky parlament a Radu, aby:

- urýchlene dosiahli dohodu o legislatívnom návrhu na zriadenie **Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a siete národných koordinačných centier.**

III. POSILNENIE BEZPEČNOSTI DIGITÁLNYCH INFRAŠTRUKTÚR

Budúcim pilierom čoraz viac digitalizovaných hospodárstiev a spoločností budú siete piatej generácie (5G). Prepoja miliardy predmetov a systémov, a to aj v kritických sektoroch ako energetika, doprava, bankovníctvo a zdravotníctvo, ako aj priemyselné riadiace systémy, ktoré uchovávajú citlivé informácie a podporujú bezpečnostné systémy. Zaistenie kybernetickej bezpečnosti a odolnosti sietí 5G je preto nevyhnutné.

Ako súčasť koordinovaného prístupu, členské štáty s podporou Komisie a Agentúry Európskej únie pre kybernetickú bezpečnosť uverejnili 9. októbra 2019 správu o **koordinovanom posúdení rizík na úrovni EÚ, pokiaľ ide o bezpečnosť sietí 5G**³². Tento významný krok je súčasťou vykonávania odporúčania Komisie, ktoré bolo prijaté v marci 2019 s cieľom zaistiť vysokú úroveň kybernetickej bezpečnosti sietí 5G v celej EÚ³³. Správa vychádza z výsledkov vnútroštátnych posúdení rizík v oblasti kybernetickej bezpečnosti, ktoré vykonali všetky členské štáty EÚ. Identifikujú sa v nej hlavné hrozby a aktéri hrozieb, najohrozenejšie zariadenia, najzraniteľnejšie miesta (vrátane technických a iných druhov zraniteľných miest) a niekoľko strategických rizík. Toto posúdenie poskytuje základ na identifikáciu zmiernujúcich opatrení, ktoré sa budú môcť uplatňovať na vnútroštátnej a európskej úrovni.

V správe sa uvádza niekoľko dôležitých výziev v oblasti **kybernetickej bezpečnosti**, ktoré sa v súvislosti so sieťami 5G pravdepodobne objavia alebo v nich budú viditeľnejšie. Tieto bezpečnostné výzvy súvisia najmä s kľúčovými *inováciami* technológií 5G, najmä s významom softvéru a širokej škály služieb a aplikácií, ktoré siete 5G umožňujú, ako aj s úlohou *dodávateľov* pri budovaní a prevádzke sietí 5G a s mierou závislosti od jednotlivých dodávateľov. Produkty, služby a operácie dodávateľov sa tak čoraz viac stávajú súčasťou „priestoru na útok“ v rámci sietí 5G. Obzvlášť dôležitý bude aj rizikový profil jednotlivých dodávateľov, ako aj pravdepodobnosť, že dodávateľ môže podliehať vplyvu krajiny, ktorá nie je členom EÚ.

V súlade s postupom stanoveným v odporúčaní Komisie z marca 2019 by sa členské štáty mali do 31. decembra 2019 dohodnúť na **súbore zmiernujúcich opatrení** na riešenie zistených rizík v oblasti kybernetickej bezpečnosti na vnútroštátnej úrovni a na úrovni Únie. Komisia a Európska služba pre vonkajšiu činnosť budú v oblasti kybernetickej bezpečnosti a odolnosti sietí 5G takisto naďalej spolupracovať s podobne zmýšľajúcimi partnermi. V tejto súvislosti je Komisia v kontakte s NATO a to so zreteľom na posúdenie rizík kybernetickej bezpečnosti sietí 5G, koordinované EÚ.

³² Skupina pre spoluprácu príslušných orgánov v zmysle smernice o bezpečnosti sietí a informačných systémov [smernica (EÚ) 2016/1148 zo 6. 7. 2016] dokončila v spolupráci s Komisiou a Európskou agentúrou pre kybernetickú bezpečnosť posúdenie rizík v oblasti kybernetickej bezpečnosti sietí 5G, ktoré bolo koordinované na úrovni EÚ: <https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>.

³³ C(2019)2355 final z 26. 3. 2019.

IV. BOJ PROTI DEZINFORMÁCIÁM A OCHRANA VOLIEB PRED ĎALŠÍMI KYBERNETICKÝMI HROZBAMI

EÚ zaviedla **rámec pre koordinovanú činnosť proti dezinformáciám**, ktorý plne zohľadňuje európske hodnoty a základné práva³⁴. Na základe akčného plánu proti dezinformáciám³⁵ sa pokračuje v úsilí o obmedzovanie priestoru pre dezinformácie, a to aj s cieľom chrániť integritu volieb.

V tejto súvislosti je ústredným prvkom spolupráca s priemyselným sektorom prostredníctvom samoregulačného **Kódexu postupov proti šíreniu dezinformácií** pre online platformy a reklamný sektor, ktorý sa začal uplatňovať v októbri 2018³⁶. Komisia posúdila účinnosť kódexu po prvom roku jeho uplatňovania na základe sebahodnotiacich výročných správ, ktoré predložili online platformy a ostatní signatári kódexu a ktoré boli uverejnené 29. októbra 2019 spolu s vyhlásením Komisie³⁷. Správy vo všeobecnosti preukazujú značné úsilie signatárov o plnenie ich záväzkov.

Opatrenia, ktoré platformy prijali, sa líšia z hľadiska rýchlosti a rozsahu pôsobnosti v rámci všetkých piatich pilierov záväzkov, ktorými sa kódex zaoberá. Vo všeobecnosti sa pokrok dosiahol v súvislosti so záväzkami týkajúcimi sa volieb do Európskeho parlamentu v roku 2019, konkrétne pokiaľ ide o odrádzanie od reklamných a peňažných stimulov pre dezinformácie (1. pilier), zabezpečenie transparentnosti politickej a tematicky zameranej reklamy (2. pilier) a zabezpečenie integrity služieb proti neautentickým účtom a správaniu (3. pilier). Oproti tomu je pokrok len malý alebo nulový v súvislosti so záväzkami posilniť postavenie spotrebiteľov (4. pilier) a záväzkami posilniť postavenie výskumnej komunity, a to aj na základe toho, že platformy v súlade s požiadavkami na ochranu súkromia poskytujú príslušný prístup k databázam na výskumné účely (5. pilier). Existujú aj rozdiely v rozsahu opatrení, ktoré prijala každá platforma s cieľom zabezpečiť plnenie svojich záväzkov, ako aj rozdiely medzi členskými štátmi, pokiaľ ide o zavádzanie jednotlivých politík. Komisia pokračuje v spolupráci so signatármi kódexu a ďalšími zainteresovanými stranami s cieľom zintenzívniť opatrenia prijaté proti šíreniu dezinformácií.

V rámci akčného plánu proti dezinformáciám Komisia a vysoká predstaviteľka v spolupráci s členskými štátmi vytvorili **system včasného varovania** na riešenie dezinformačných kampaní. System včasného varovania umožnil inštitúciám EÚ a členským štátom vymieňať si informácie a analýzy pred voľbami do Európskeho parlamentu v roku 2019 a koordinovať reakcie. Po voľbách sa táto práca ešte zintenzívnila, pričom výmeny na pracovnej úrovni prebiehali každodenne a rôzne členské štáty zorganizovali tri zasadnutia kontaktných miest systému včasného varovania.

³⁴ Pozri akčný plán proti dezinformáciám [JOIN(2018) 36 final z 5. 12. 2018].

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

³⁶ Na základe kódexu sa online platformy Google, Facebook, Twitter a Microsoft zaviazali, že zabránia manipulatívne využívaniu svojich služieb pochybnými aktérmi, zabezpečia transparentnosť a zverejňovanie politickej reklamy a prijmú iné opatrenia na zlepšenie transparentnosti, zodpovednosti a dôveryhodnosti online ekosystému. Obchodné združenia z reklamného sektora sa tiež zaviazali, že budú s platformami spolupracovať s cieľom zlepšiť kontrolu umiestňovania reklám a vyvinúť nástroje na ochranu značky, ktorých účelom je obmedziť umiestňovanie reklamy na webových sídlach, ktoré šíria dezinformácie.

³⁷ https://ec.europa.eu/commission/presscorner/detail/sk/statement_19_6166. Medzi ďalších signatárov tohto kódexu okrem spoločností Google, Facebook, Twitter a Microsoft patrí spoločnosť Mozilla, sedem združení na európskej alebo vnútroštátnej úrovni zastupujúcich reklamný sektor, a EDiMA, európske združenie zastupujúce platformy a iné technologické spoločnosti pôsobiace v online sektore.

Ďalším praktickým krokom na identifikáciu dezinformácií je práca **tímu pre strategickú komunikáciu** („StratComms“), a najmä jej pracovnej skupiny East StratCom, ktorá realizuje projekt „EUvsDisinfo“ s cieľom monitorovať a analyzovať prokremel'ské dezinformácie a reagovať na ne³⁸. Od začiatku roka 2019 prvý na tento účel vyčlenený rozpočet vo výške 3 milióny EUR umožnil zvýšiť a rozšíriť túto činnosť tak, aby zahŕňala monitorovanie a analýzu prokremel'ských dezinformácií na internete, vo vysielaní a sociálnych médiách v 19 jazykoch od angličtiny po srbčinu a arabčinu. Objem odhalených dezinformačných činností sa v dôsledku zlepšenej monitorovacej kapacity viac ako zdvojnásobil, pričom doteraz v roku 2019 bolo zaznamenaných približne 2000 prípadov šírenia dezinformácií v porovnaní s 765 prípadmi v rovnakom období v roku 2018. Pracovná skupina East StratCom zohrala kľúčovú úlohu pri monitorovaní a odhaľovaní prokremel'ských dezinformácií zameraných na voľby do Európskeho parlamentu v roku 2019. Výskum bol spojený s kampaňou na zvýšenie informovanosti o pokusoch o zasahovanie do volebných procesov na celom svete. Jeho aktívna pomoc poskytovaná v úzkej spolupráci s Európskym parlamentom a Komisiou viedla k viac ako 20 mediálnym rozhovorom, pričom na kampani sa zúčastnilo viac ako 300 novinárov.

Komisia prijala aj opatrenia na **zníženie šírenia dezinformácií a mýtov o inštitúciách a politikách EÚ**. Zriadila sieť odborníkov v oblasti komunikácie, ktorá prostredníctvom online portálu poskytuje interaktívny informačný materiál o politikách EÚ a o probléme šírenia dezinformácií a ich vplyve na spoločnosť. V spolupráci s Európskym parlamentom a Európskou službou pre vonkajšiu činnosť³⁹ Komisia začala aj sériu kampaní v sociálnych médiách zameraných na odstraňovanie dezinformácií.

V. VYKONÁVANIE OSTATNÝCH PRIORÍT V OBLASTI BEZPEČNOSTI

1. Vykonávanie legislatívnych opatrení v rámci bezpečnostnej únie

Dohodnuté opatrenia v rámci bezpečnostnej únie budú pre bezpečnosť prínosné v plnej miere len vtedy, ak všetky členské štáty zabezpečia ich rýchle a úplné vykonávanie. Na tento účel Komisia aktívne podporuje členské štáty pri vykonávaní právnych predpisov EÚ, okrem iného aj prostredníctvom financovania a uľahčovania výmeny najlepších postupov. V plnej miere pri tom využíva svoje právomoci vyplývajúce zo zmlúv, ktoré sa týkajú presadzovania právnych predpisov EÚ, vrátane prípadných postupov v prípade nesplnenia povinnosti.

Lehota na transpozíciu **smernice EÚ o osobných záznamoch o cestujúcich**⁴⁰ uplynula 25. mája 2018. Do dnešného dňa oznámilo úplnú transpozíciu 25 členských štátov⁴¹, čo od júla 2018, keď Komisia začala postup v prípade nesplnenia povinnosti proti 14 členským štátom, predstavuje významný pokrok⁴². Napriek prebiehajúcejmu postupu v prípade nesplnenia povinnosti, ktorý sa začal 19. júla 2018, úplnú transpozíciu dosiaľ neoznámili ešte dva členské štáty⁴³. Komisia zároveň naďalej podporuje všetky členské štáty v ich úsilí o dokončenie vývoja systémov na vedenie osobných záznamov o cestujúcich, okrem iného aj zjednodušením výmeny informácií a najlepších postupov.

³⁸ www.euvsdisinfo.eu

³⁹ <https://europa.eu/euprotects/>

⁴⁰ Smernica (EÚ) 2016/681 (27. 4. 2016). Dánsko sa na prijatí tejto smernice nezúčastnilo, nie je ňou viazané ani nepodlieha jej uplatňovaniu.

⁴¹ Odkazy na oznámenia úplnej transpozície vychádzajú z vyhlásení členských štátov a nemajú vplyv na kontrolu transpozície zo strany útvarov Komisie (stav k 17. 10. 2019).

⁴² Pozri šestnástu správu o pokroku dosiahnutom pri budovaní účinnej a skutočnej bezpečnostnej únie [COM(2018) 690 final z 10. 10. 2018].

⁴³ Slovinsko oznámilo čiastočnú transpozíciu. Španielsko transpozíciu neoznámilo (stav k 17. 10. 2019).

Lehota na transpozíciu **smernice o boji proti terorizmu**⁴⁴ uplynula 8. septembra 2018. Úplnú transpozíciu dosiaľ oznámilo 22 členských štátov, čo od novembra 2018, keď Komisia začala postup v prípade nesplnenia povinnosti proti 16 členským štátom, predstavuje významný pokrok⁴⁵. Napriek prebiehajúcemu postupu v prípade nesplnenia povinnosti úplnú transpozíciu neoznámili ešte tri členské štáty⁴⁶. Komisia zaslala 25. júla 2019 odôvodnené stanoviská dvom členským štátom z dôvodu neoznánenia úplnej transpozície smernice⁴⁷. Oba členské štáty vo svojej odpovedi oznámili, že legislatívny proces dokončia do konca tohto roka.

Lehota na transpozíciu **smernice o kontrole získavania a vlastníctva zbraní**⁴⁸ uplynula 14. septembra 2018. K dnešnému dňu oznámilo úplnú transpozíciu 13 členských štátov. Napriek prebiehajúcemu postupu v prípade nesplnenia povinnosti, ktorý sa začal 22. novembra 2018, úplnú transpozíciu neoznámilo ešte 15 členských štátov⁴⁹. Komisia zaslala 25. júla 2019 odôvodnené stanoviská 20 členským štátom z dôvodu neoznánenia úplnej transpozície smernice. V reakcii na to oznámilo úplnú transpozíciu smernice päť členských štátov⁵⁰.

Lehota na transpozíciu **smernice o ochrane údajov pri presadzovaní práva**⁵¹ uplynula 6. mája 2018. Do dnešného dňa oznámilo úplnú transpozíciu 25 členských štátov, čo od júla 2018, keď Komisia začala postup v prípade nesplnenia povinnosti proti 19 členským štátom, predstavuje významný pokrok⁵². Napriek prebiehajúcemu postupu v prípade nesplnenia povinnosti úplnú transpozíciu neoznámili ešte tri členské štáty⁵³. Komisia 25. júla 2019 rozhodla o postúpení prípadu dvoch členských štátov⁵⁴ na Súdny dvor Európskej únie za netransponovanie smernice a jednému členskému štátu zaslala formálnu výzvu⁵⁵ z dôvodu nevykonania úplnej transpozície smernice⁵⁶.

Komisia posudzuje transpozíciu **štvrtej smernice o boji proti praniu špinavých peňazí**⁵⁷, a zároveň overuje, či členské štáty uplatňujú dané pravidlá. Smernicu mali transponovať do vnútroštátneho práva do 26. júna 2018. Komisia vedie postup v prípade nesplnenia povinnosti proti 21 členským štátom, keďže dospela k záveru, že oznámenia predložené členskými štátmi nesvedčia o úplnej transpozícii tejto smernice⁵⁸.

⁴⁴ Smernica (EÚ) 2017/541 (15. 3. 2017). Smernica sa neuplatňuje v Spojenom kráľovstve, Írsku a Dánsku.

⁴⁵ Pozri sedemnástu správu o pokroku dosiahnutom pri budovaní účinnej a skutočnej bezpečnostnej únie [COM(2018) 845 final z 11. 12. 2018].

⁴⁶ Grécko a Luxembursko neoznámili vnútroštátne vykonávacie opatrenia. Poľsko oznámilo vnútroštátne opatrenia, ktoré predstavujú čiastočnú transpozíciu (stav k 17. 10. 2019).

⁴⁷ Grécko a Luxembursko.

⁴⁸ Smernica (EÚ) 2017/853 zo 17. 10. 2019).

⁴⁹ Transpozičné opatrenia týkajúce sa časti nových ustanovení oznámilo Belgicko, Česko, Estónsko, Poľsko, Slovensko, Spojené kráľovstvo a Švédsko. Žiadne transpozičné opatrenia zatiaľ neoznámil Cyprus, Grécko, Luxembursko, Maďarsko, Nemecko, Rumunsko, Slovinsko a Španielsko (stav k 17. 10. 2019).

⁵⁰ Fínsko, Holandsko, Írsko, Litva, Portugalsko (stav ku 17. 10. 2019).

⁵¹ Smernica (EÚ) 2016/680 (27. 4. 2016).

⁵² Pozri šestnástu správu o pokroku dosiahnutom pri budovaní účinnej a skutočnej bezpečnostnej únie [COM(2018) 690 final z 10. 10. 2018].

⁵³ Slovinsko oznámilo čiastočnú transpozíciu. Španielsko transpozíciu neoznámilo. Hoci Nemecko oznámilo úplnú transpozíciu, Komisia považuje túto transpozíciu za neúplnú (stav k 17. 10. 2019).

⁵⁴ Grécko a Španielsko.

⁵⁵ Nemecko.

⁵⁶ Grécko oznámilo úplnú transpozíciu, ktorú Komisia posudzuje.

⁵⁷ Smernica (EÚ) 2015/849 (20. 5. 2015).

⁵⁸ Belgicko, Bulharsko, Česko, Dánsko, Nemecko, Estónsko, Írsko, Francúzsko, Taliansko, Cyprus, Lotyšsko, Litva, Maďarsko, Holandsko, Rakúsko, Poľsko, Rumunsko, Slovensko, Fínsko, Švédsko

Komisia posúdila súlad transpozície smerníc **týkajúcich sa počítačovej kriminality**. V júli a októbri 2019 začala postup v prípade nesplnenia povinnosti proti 23 členským štátom⁵⁹ keďže dospela k záveru, že vnútroštátne vykonávacie právne predpisy, ktoré uvedené členské štáty oznámili, nesvedčia o správnej transpozícii **smernice o boji proti sexuálnemu zneužívaniu detí**⁶⁰. V júli a októbri 2019 Komisia takisto začala postup v prípade nesplnenia povinnosti proti štyrom členským štátom,⁶¹ keďže dospela k záveru, že vnútroštátne vykonávacie právne predpisy, ktoré uvedené členské štáty oznámili, nesvedčia o správnej transpozícii **smernice o útokoch na informačné systémy**⁶².

Komisia naliehavo vyzýva členské štáty, aby prijali potrebné opatrenia na úplnú transpozíciu týchto smerníc do vnútroštátneho práva a oznámili ju Komisii:

- **smernica EÚ o osobných záznamoch o cestujúcich**, v súvislosti s ktorou jeden členský štát ešte stále neoznámil transpozíciu do vnútroštátneho práva a jeden členský štát musí oznámenie o transpozícii dokončiť⁶³;
- **smernica o boji proti terorizmu**, v súvislosti s ktorou dva členské štáty ešte stále neoznámili transpozíciu do vnútroštátneho práva a jeden členský štát musí oznámenie o transpozícii dokončiť⁶⁴;
- **smernica o kontrole získavania a vlastníctva zbraní**, v súvislosti s ktorou osem členských štátov ešte stále neoznámilo transpozíciu do vnútroštátneho práva a sedem členských štátov musí oznámenie o transpozícii dokončiť⁶⁵;
- **smernica o ochrane údajov pri presadzovaní práva**, v súvislosti s ktorou jeden členský štát ešte stále neoznámil transpozíciu do vnútroštátneho práva a dva členské štáty musia oznámenie o transpozícii dokončiť⁶⁶;
- **štvrtá smernica proti praniu špinavých peňazí**, v súvislosti s ktorou 21 členských štátov musí oznámenie o transpozícii dokončiť⁶⁷;
- **smernica o boji proti sexuálnemu zneužívaniu detí**, v súvislosti s ktorou sa začal postup v prípade nesplnenia povinnosti kvôli nesprávnej transpozícii proti 23 členským štátom⁶⁸;
- **smernica o útokoch na informačné systémy**, v súvislosti s ktorou sa začal postup v prípade nesplnenia povinnosti kvôli nesprávnej transpozícii proti štyrom členským štátom⁶⁹.

a Spojené kráľovstvo (stav k 17. 10. 2019). Predtým bolo ukončených sedem postupov o nesplnení povinnosti súvisiacich s touto smernicou.

⁵⁹ Belgicko, Bulharsko, Česká republika, Nemecko, Estónsko, Grécko, Španielsko, Francúzsko, Chorvátsko, Taliansko, Lotyšsko, Litva, Luxembursko, Maďarsko, Malta, Rakúsko, Poľsko, Portugalsko, Rumunsko, Slovinsko, Slovensko, Fínsko a Švédsko.

⁶⁰ Smernica 2011/93/EÚ (13. 12. 2011).

⁶¹ Bulharsko, Taliansko, Portugalsko a Slovinsko.

⁶² Smernica 2013/40/EÚ (12. 8. 2013).

⁶³ Slovinsko oznámilo čiastočnú transpozíciu. Španielsko transpozíciu neoznámilo (stav k 17. 10. 2019).

⁶⁴ Grécko a Luxembursko transpozíciu neoznámili. Poľsko oznámilo čiastočnú transpozíciu (stav k 17. 10. 2019).

⁶⁵ Transpozíčné opatrenia týkajúce sa časti nových ustanovení oznámilo Belgicko, Česko, Estónsko, Poľsko, Slovensko, Spojené kráľovstvo a Švédsko. Žiadne transpozíčné opatrenia zatiaľ neoznámil Cyprus, Grécko, Luxembursko, Maďarsko, Nemecko, Rumunsko, Slovinsko a Španielsko (stav k 17. 10. 2019).

⁶⁶ Slovinsko oznámilo čiastočnú transpozíciu. Španielsko transpozíciu neoznámilo. Hoci Nemecko oznámilo úplnú transpozíciu, Komisia považuje túto transpozíciu za neúplnú (stav k 17. 10. 2019).

⁶⁷ Belgicko, Bulharsko, Česko, Dánsko, Nemecko, Estónsko, Írsko, Francúzsko, Taliansko, Cyprus, Lotyšsko, Litva, Maďarsko, Holandsko, Rakúsko, Poľsko, Rumunsko, Slovensko, Fínsko, Švédsko a Spojené kráľovstvo (stav k 17. 10. 2019).

⁶⁸ Belgicko, Bulharsko, Česká republika, Nemecko, Estónsko, Grécko, Španielsko, Francúzsko, Chorvátsko, Taliansko, Lotyšsko, Litva, Luxembursko, Maďarsko, Malta, Rakúsko, Poľsko, Portugalsko, Rumunsko, Slovinsko, Slovensko, Fínsko a Švédsko.

2. Pripravenosť a ochrana

Budovanie odolnosti proti bezpečnostným hrozbám je dôležitým aspektom úsilia o vybudovanie účinnej a skutočnej bezpečnostnej únie. Komisia podporuje členské štáty a miestne orgány pri zvyšovaní ochrany verejných priestorov na základe vykonávania akčného plánu z októbra 2017 a partnerstva pre bezpečnosť vo verejných priestoroch v rámci mestskej agendy pre EÚ z januára 2019. Táto činnosť sa týka tých miest, ktoré sa obrátili na Komisiu so žiadosťou o podporu pri riešení problémov, s ktorými sa pri ochrane verejných priestorov stretli.

Kľúčom k posilneniu bezpečnosti verejných priestorov je výmena najlepších postupov medzi miestnymi orgánmi a so súkromnými prevádzkovateľmi. To bolo ústrednou témou podujatia **Európsky týždeň bezpečnosti**, ktoré sa vo francúzskom Nice konalo od 14. do 18. októbra 2019 v rámci projektu financovaného EÚ s názvom „*Protect Allied Cities against Terrorism in Securing Urban Areas*“ (ochrana spojených miest proti terorizmu zabezpečovaním mestských oblastí). Na podujatí, na ktorom sa zišlo 500 účastníkov z miest v celej Európe, vnútroštátnych orgánov a výskumných inštitúcií, sa zdôraznil význam úzkej spolupráce medzi všetkými zainteresovanými stranami, tak verejnými, ako aj súkromnými, a úloha nových technológií pri lepšej ochrane miest. Otázke ochrany verejných priestorov sa venovala pozornosť aj počas **Európskeho týždňa regiónov a miest** od 7. do 10. októbra 2019 v Bruseli, v rámci ktorého sa uskutočnil seminár o mestskej agende pre partnerstvo EÚ v oblasti bezpečnosti vo verejných priestoroch. Seminár bol zameraný na úlohu miestnych orgánov v oblasti bezpečnostnej politiky, na právne predpisy a financovanie EÚ pri riešení hlavných bezpečnostných výziev v mestských verejných priestoroch a na kľúčové témy, ako sú inovácie prostredníctvom inteligentných riešení a technológií, vrátane koncepcie bezpečnosti už v štádiu návrhu, prevencia a sociálne začlenenie. Komisia takisto prispieva k podpore inovácií miest v týchto oblastiach prostredníctvom svojej poslednej výzvy na predkladanie návrhov na mestské inovačné opatrenia, ktorej výsledky boli oznámené v auguste 2019. Spomedzi vybraných projektov budú tri mestá (Pireus v Grécku, Tampere vo Fínsku a Turíno v Taliansku) testovať nové riešenia v oblasti bezpečnosti miest⁷⁰.

V záujme lepšej **ochrany miest na konanie bohoslužieb** a preskúmania potrieb rôznych náboženských skupín Komisia zorganizovala 7. októbra 2019 stretnutie so zástupcami židovských, moslimských, kresťanských a budhistických spoločenstiev. Na zasadnutí, ktoré bolo súčasťou vykonávania akčného plánu EÚ na podporu ochrany verejných priestorov z roku 2017, sa ukázalo, že povedomie a pripravenosť v oblasti bezpečnosti sa v rôznych náboženských spoločenstvách výrazne líšia, čo poukazuje na význam ďalšej výmeny osvedčených postupov. Zo stretnutia takisto vyplynulo, že zavedenie základných bezpečnostných opatrení a zlepšenie informovanosti o bezpečnosti nie je nezlučiteľné so zachovaním otvorenosti a prístupnosti miest na konanie bohoslužieb. Komisia bude zhromažďovať osvedčené postupy a materiály na zvyšovanie informovanosti na svojej elektronickej platforme odborníkov a na túto záležitosť upozorní bezpečnostné orgány členských štátov vo verejno-súkromnom fóre na ochranu verejných priestorov.

Jednou z osobitných oblastí, ktorá si vyžaduje bližšiu pozornosť, je narastajúca bezpečnostná hrozba pre kritickú infraštruktúru a verejné priestory, ktorú predstavujú **drony**. Komisia podporuje členské štáty pri analyzovaní trendov pri zneužívaní dronov na škodlivé účely,

⁶⁹ Bulharsko, Taliansko, Portugalsko a Slovinsko.

⁷⁰ Mestské inovačné opatrenia sú nástrojom spolufinancovaným z Európskeho regionálneho rozvoja. Viac informácií možno nájsť na adrese: <https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals>.

financuje príslušný výskum a uľahčuje testovanie protopatrení, čím dopĺňa nedávno prijaté právne predpisy EÚ⁷¹ pre bezpečnú prevádzku dronov vo vzdušnom priestore s lietadlami s posádkou a to bez toho, aby sa oslabili možnosti prospešného využívania dronov. Výmena skúseností a najlepších postupov má zásadný význam, čoho dôkazom je aj medzinárodná konferencia na vysokej úrovni, ktorá sa uskutočnila v Bruseli 17. októbra 2019 a ktorá sa zamerala na eliminovanie hrozieb, ktoré predstavujú bezpilotné vzdušné systémy. Na tomto podujatí usporiadanom Komisiou sa zúčastnilo 250 účastníkov z členských štátov, medzinárodných organizácií, partnerov z tretích krajín, priemyslu, akademickej obce a občianskej spoločnosti s cieľom diskutovať o bezpečnostných výzvach, ktoré predstavujú drony, a o spôsoboch ich riešenia. Na zasadnutí sa ukázalo, že je potrebné pravidelné posudzovanie rizika v súvislosti s dronmi a úzka spolupráca medzi leteckými úradmi a orgánmi presadzovania práva pri ďalšom rozvoji európskych právnych predpisov týkajúcich sa bezpečnej prevádzky dronov. Takisto je potrebné ďalej testovať protopatrenia proti dronom na základe koordinovaného európskeho prístupu. Okrem toho sa dospelo k dohode, že na to, aby drony boli bezpečné, zabezpečené, prevádzkovo spoľahlivé a ťažko zneužívané na škodlivé účely, je nevyhnutná úzka spolupráca medzi príslušnými orgánmi a priemyslom.

3. Vonkajší rozmer

Vzhľadom na to, že väčšina bezpečnostných rizík, ktorým Únia čelí, presahuje hranice EÚ a predstavuje globálne hrozby, dôležitú úlohu pri budovaní účinnej a skutočnej bezpečnostnej únie zohráva spolupráca s partnerskými krajinami, organizáciami a príslušnými zainteresovanými stranami.

Výmena informácií je pre túto spoluprácu kľúčová. Spolu s touto správou prijala Komisia odporúčanie, aby Rada povolila začať rokovania o **dohode medzi EÚ a Novým Zélandom o výmene osobných údajov** medzi Europolom a príslušnými orgánmi Nového Zélandu **na účely boja proti závažnej trestnej činnosti a terorizmu**. Vďaka tejto dohode sa ešte výraznejšie posilní schopnosť Europolu zapájať sa do spolupráce s Novým Zélandom v záujme predchádzania trestným činom a boja proti nim, čo je základným poslaním Europolu. Hoci pracovná dohoda medzi Europolom a Novým Zélandom z apríla 2019 poskytuje rámec pre štruktúrovanú spoluprácu na strategickej úrovni, neposkytuje právny základ na výmenu osobných údajov. Výmena osobných údajov pri plnom dodržiavaní práva EÚ a základných práv má zásadný význam pre účinnú operačnú policajnú spoluprácu. Komisia už predtým na základe teroristických hrozieb, výziev súvisiacich s migráciou a operačných potrieb Europolu určila osem prioritných krajín v regióne Blízkeho východu/severnej Afriky, s ktorými by sa mali začať rokovania⁷². Vzhľadom na operačné potreby orgánov presadzovania práva v celej EÚ a možné výhody užšej spolupráce v tejto oblasti, ako sa ukázalo aj v nadväznosti na útok v Christchurch v marci 2019, Komisia považuje za potrebné pridať Nový Zéland medzi prioritné krajiny, s ktorými treba začať rokovania v krátkodobom horizonte.

Ďalším zo základných prvkov bezpečnostnej spolupráce Únie s partnermi z tretích krajín je prenos **údajov zo záznamov o cestujúcich**. Komisia prijala 27. septembra 2019 odporúčanie, aby Rada povolila začať rokovania o dohode medzi **EÚ a Japonskom o prenose údajov zo záznamov o cestujúcich** s cieľom predchádzať terorizmu a závažnej nadnárodnej trestnej

⁷¹ Vykonávacie nariadenie Komisie (EÚ) 2019/947 z 24. mája 2019 o pravidlách a postupoch prevádzky bezpilotných lietadiel

⁷² Pozri jedenástu správu o pokroku dosiahnutom pri budovaní účinnej a skutočnej bezpečnostnej únie [COM(2017) 608 final z 18. 10. 2017]. Prioritnými krajinami sú Alžírsko, Egypt, Izrael, Jordánsko, Libanon, Maroko, Tunisko a Turecko.

činnosti a bojovať proti nim v plnom súlade so zárukami ochrany údajov a základnými právami⁷³. Odporúčanie sa skúma na úrovni pracovnej skupiny Rady a Komisia vyzýva Radu, aby urýchlene prijala mandát na rokovania s Japonskom. Včasné prijatie opatrení pred olympiádou v roku 2020 by znamenalo skutočný prínos z hľadiska bezpečnosti.

Na celosvetovej úrovni Komisia podporuje úsilie Medzinárodnej organizácie civilného letectva o stanovenie štandardu pre spracovanie údajov zo záznamov o cestujúcich. Je to reakcia na rezolúciu Bezpečnostnej rady OSN č. 2396, v ktorej sa naliehavo vyzývajú všetky členské štáty Organizácie Spojených národov, aby rozvíjali schopnosť zhromažďovať, spracúvať a analyzovať údaje zo záznamov o cestujúcich. Komisia 13. septembra 2019 predložila návrh⁷⁴ rozhodnutia Rady o pozícii, ktorá sa má v mene EÚ zaujať v Medzinárodnej organizácii civilného letectva, pokiaľ ide o štandardy a odporúčania týkajúce sa údajov zo záznamov o cestujúcich. Návrh sa skúma na úrovni pracovnej skupiny Rady a Komisia vyzýva na urýchlené prijatie rozhodnutia Rady. Pozícia Únie a jej členských štátov sa uvádza aj v informačnom dokumente o štandardoch a zásadách zhromažďovania, využívania, spracúvania a ochrany údajov zo záznamov o cestujúcich, ktorý bol predložený na 40. zasadnutí zhromaždenia Medzinárodnej organizácie civilného letectva.

Pokiaľ ide o prácu na novej dohode o záznamoch o cestujúcich s **Kanadou**, Komisia sa usiluje o urýchlené dokončenie dohody. Medzitým sa toto leto začalo kombinované spoločné preskúmanie a spoločné hodnotenie dohody o záznamoch o cestujúcich s **Austráliou**, ako aj spoločné hodnotenie dohody o záznamoch o cestujúcich so **Spojenými štátmi**, ktorému predchádzala návšteva v Canberre v auguste a Washingtone v septembri 2019. O aktuálnom stave rokovaní s Japonskom, Austráliou a Kanadou o údajoch zo záznamov o cestujúcich Komisia informovala Výbor Európskeho parlamentu pre občianske slobody, spravodlivosť a vnútorné veci na neverejnom zasadnutí 14. októbra 2019.

Pokrok sa dosiahol aj v bezpečnostnej spolupráci s partnermi zo **západného Balkánu**, a to vykonaním spoločného akčného plánu boja proti terorizmu na západnom Balkáne z októbra 2018. Komisia 9. októbra podpísala s Albánskom a Severomacedónskou republikou dve nezáväzné dvojstranné dohody o boji proti terorizmu⁷⁵. V týchto dohodách sa stanovujú ciele priorítne opatrenia, ktoré majú prijať orgány príslušnej partnerskej krajiny v súvislosti s piatimi cieľmi spoločného akčného plánu⁷⁶, pričom sa v nich zároveň uvádza, akú podporu Komisia plánuje poskytnúť. Očakáva sa, že podobné dohody s ostatnými partnermi zo západného Balkánu budú podpísané v nadchádzajúcich týždňoch. Komisia okrem toho 7. októbra 2019 podpísala s Čiernou Horou dohodu o spolupráci v oblasti riadenia hraníc medzi Čiernou Horou a Európskou agentúrou pre pohraničnú a pobrežnú stráž. Táto dohoda umožňuje agentúre pomáhať Čiernej Hore pri riadení hraníc s cieľom riešiť neregulárnu migráciu a cezhraničnú trestnú činnosť, a tak zvyšovať bezpečnosť na vonkajších hraniciach EÚ.

⁷³ COM(2019) 420 final z 27. 9. 2019.

⁷⁴ COM(2019) 416 final z 13. 9. 2019.

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

⁷⁶ V spoločnom akčnom pláne sa stanovujú opatrenia týkajúce sa týchto piatich cieľov: pevný rámec pre boj proti terorizmu; účinné predchádzanie násilnému extrémizmu a boj proti nemu; účinná výmena informácií a operačná spolupráca; budovanie kapacít na boj proti praniu špinavých peňazí a financovaniu terorizmu; posilnenie ochrany občanov a infraštruktúry.

V záujme posilnenia spolupráce s partnerskými krajinami pri riešení spoločných bezpečnostných hrozieb Komisia vyzýva Radu, aby:

- prijala povolenie začať rokovania o dohode medzi EÚ a **Novým Zélandom** o výmene osobných údajov na účely boja proti závažnej trestnej činnosti a terorizmu;
- prijala povolenie začať rokovania o dohode o postupovaní údajov zo záznamov o cestujúcich medzi EÚ a Japonskom;
- prijala navrhované **rozhodnutie Rady o pozícii, ktorá sa má v mene EÚ zaujať v Medzinárodnej organizácii civilného letectva**, pokiaľ ide o štandardy a odporúčania týkajúce sa údajov zo záznamov o cestujúcich.

VI. ZÁVER

V tejto správe sa uvádza široká škála opatrení, ktoré EÚ prijala na riešenie spoločných hrozieb v Európe a posilnenie našej kolektívnej bezpečnosti. Pokrok dosiahnutý pri budovaní účinnej a skutočnej bezpečnostnej únie, založený na spoločnom chápaní toho, že dnešné bezpečnostné výzvy možno najlepšie riešiť vzájomnou spolupracou a spolupracou s tretími krajinami, je výsledkom úzkej spolupráce širokej škály aktérov, budovania dôvery, spoločného využívania zdrojov a spoločného zvládania hrozieb: na všetkých úrovniach verejnej správy, počnúc mestami a ďalšími miestnymi subjektmi, regiónmi a vnútroštátnymi orgánmi až po úroveň EÚ s Európskym parlamentom a Radou; so zapojením orgánov verejnej moci, agentúr EÚ, súkromných subjektov a občianskej spoločnosti a s využitím odborných znalostí, nástrojov a zdrojov v rôznych oblastiach politiky, ako je dopravná politika, digitálny jednotný trh alebo politika súdržnosti. Vytváranie bezpečnostnej únie je úzko prepojené s ochranou základných práv a ochranou a podporou našich hodnôt.

Úsilie vybudovať účinnú a skutočnú bezpečnostnú úniu musí pokračovať. Je potrebné urýchlene dosiahnuť dohodu o dôležitých pripravovaných iniciatívach, najmä o: 1. legislatívnom návrhu na odstránenie teroristického obsahu online, 2. legislatívnom návrhu na zlepšenie prístupu k elektronickým dôkazom pri presadzovaní práva, 3. legislatívnom návrhu na zriadenie Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a siete národných koordinačných centier a 4. prerokovaných legislatívnych návrhoch týkajúcich sa silnejších a inteligentnejších informačných systémov v oblasti bezpečnosti, riadenia hraníc a riadenia migrácie. Dohodnuté opatrenia a nástroje sa musia premietnuť do bežnej praxe, pričom všetky členské štáty musia včas a v plnom rozsahu vykonávať právne predpisy EÚ, aby zaistili všetky ich prínosy pre bezpečnosť. Predovšetkým je nevyhnutné, aby všetky členské štáty vykonávali nedávno schválené právne predpisy o interoperabilite informačných systémov EÚ v oblasti bezpečnosti, riadenia hraníc a riadenia migrácie s cieľom dosiahnuť ambiciózny cieľ, ktorým je dospieť k úplnej interoperabilite do roku 2020. Napokon, Európa musí zostať ostrážitá, pokiaľ ide o vznikajúce a meniace sa hrozby, a naďalej sa zapájať do spolupráce, aby dokázala zvýšiť bezpečnosť všetkých občanov.