



V Bruselu dne 30.10.2019  
COM(2019) 552 final

**SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, EVROPSKÉ RADĚ A RADĚ**

**Dvacátá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii**

## I. ÚVOD

Tato dvacátá zpráva o dalším pokroku na cestě k vytvoření účinné a skutečné bezpečnostní unie zachycuje vývoj ve dvou hlavních pilířích: prvním je boj proti terorismu a organizované trestné činnosti, jakož i proti prostředkům, které je podporují, a druhým pak posílení naší obrany a budování odolnosti vůči uvedeným hrozbám.

Junckerova Komise považuje bezpečnost za svoji nejvyšší prioritu již od prvního dne svého působení. Na sérii teroristických útoků a další bezpečnostní výzvy reagovala EU v návaznosti na Evropský program pro bezpečnost z dubna 2015<sup>1</sup> a sdělení o položení základů účinné a skutečné bezpečnostní Unie z dubna 2016<sup>2</sup> koordinovaným přístupem a dosáhla při posilování kolektivní bezpečnosti značného pokroku<sup>3</sup>. Je stále zřejmější, že bezpečnostní výzvy – ať už jde o terorismus, organizovanou trestnou činnost, kybernetické útoky, dezinformace nebo jiné vyvíjející se kybernetické hrozby – jsou společnými hrozbami. Úrovně kolektivní bezpečnosti, kterou občané oprávněně požadují a očekávají, můžeme dosáhnout pouze spoluprací. Tento společný poznatek byl základem pro pokrok dosažený na cestě k účinné a skutečné bezpečnostní unii. Podpora na úrovni EU se na základě potřeb vnitrostátních orgánů, které usilují o bezpečnost občanů, zaměřila na legislativní a operativní opatření v případech, kdy společná opatření mohou mít dopad na bezpečnost členských států. Tato činnost byla vykonána v úzké spolupráci s Evropským parlamentem a Radou a s plnou transparentností vůči širší veřejnosti. Jádrem této práce bylo úplné dodržování základních práv, neboť zajistit bezpečnost Unie lze pouze tehdy, pokud jsou občané přesvědčeni, že jsou jejich základní práva plně dodržována.

EU se snažila **bojovat proti terorismu** tím, že minimalizovala manévrovací prostor teroristů, přičemž nová pravidla jim ztížila přístup k výbušninám, palným zbraním a financování a omezila jejich pohyb. EU zintenzivnila **výměnu informací** s cílem zajistit těm, kdo jsou v první linii, policistům a příslušníkům pohraniční stráže, účinný přístup k přesným a úplným údajům, a tak co nejlépe využívat stávající informace a odstranit nedostatky a slabé stránky. Podmínkou bezpečnosti v oblasti volného pohybu bez kontrol na vnitřních hranicích je silná ochrana vnějších hranic. V březnu 2019 dosáhly Evropský parlament a Rada dohody o dalším posílení a plném vybavení **Evropské pohraniční a pobřežní stráže** a očekává se, že nové nařízení vstoupí v platnost počátkem prosince 2019. EU poskytla platformu a finanční prostředky pro ty, kdo pracují v místních komunitách, aby si vyměňovali osvědčené postupy **v boji proti radikalizaci a prevenci násilného extremismu**, a navrhla nová pravidla pro účinné odstraňování teroristického obsahu online. Podpora ze strany EU přispěla k tomu, že se **města stala odolnějšími** vůči útokům, a to na základě akčních plánů na podporu ochrany veřejných prostorů a zvýšení připravenosti na chemická, biologická, radiologická a jaderná bezpečnostní rizika. EU řešila otázku **kybernetické bezpečnosti a kybernetických hrozeb** tím, že zavedla novou strategii EU pro kybernetickou bezpečnost, přijala příslušné právní předpisy a bojovala proti **dezinformacím** s cílem lépe chránit naše volby. Pokračuje úsilí o posílení bezpečnosti naší **digitální kritické infrastruktury**, včetně posílení spolupráce v oblasti **kybernetické bezpečnosti sítí 5G** v celé Evropě.

Je třeba udělat toho ještě více. Útok na synagogu živě přenášený po internetu a zabití dvou

<sup>1</sup> COM(2015) 185 final ze dne 28. dubna 2015.

<sup>2</sup> COM(2016) 230 final ze dne 20. dubna 2016.

<sup>3</sup> Viz předchozí zprávy o pokroku na cestě k účinné a skutečné bezpečnostní unii: [https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en).

občanů v Halle v Německu 9. října 2019 byly šokující připomínkou hrozby, kterou představuje pravicový násilný extremismus a antisemitismus. Tento útok také znovu upozornil na zneužívání internetu k teroristické propagandě, a tudíž na **potřebu celounijních pravidel pro odstraňování teroristického obsahu online**. Rada ve složení pro spravedlnost a vnitřní věci na zasedání ve dnech 7. a 8. října 2019 jednala o pravicovém násilném extremismu a terorismu a zdůraznila potřebu dalšího úsilí, a to i v boji proti šíření nezákonného pravicového extremistického obsahu online a offline. Zabití tří policistů a dalšího zaměstnance v pařížském ústředí policie 3. října 2019 zároveň ukazuje, že hrozba terorismu inspirovaného džihádisty je nadále reálná a že snahy o podporu členských států při řešení této hrozby musí pokračovat. Únik vězněných členů ISIS/Dá'iš v souvislosti s nedávnými událostmi v severní Sýrii by mohl mít vážný dopad na bezpečnost v Evropě. Je důležité, aby členské státy plně využívaly existující informační systémy k odhalování a identifikaci zahraničních teroristických bojovníků při překračování vnějších hranic. I nadále se vyvíjí úsilí o využívání informací z bojišť ke stíhání zahraničních teroristických bojovníků.

Tato zpráva nastiňuje pokrok, jehož bylo v úsilí o vytvoření účinné a skutečné bezpečnostní unie nedávno dosaženo, s důrazem na oblasti, v nichž je třeba přijmout další opatření. Poskytuje aktuální informace o provádění dohodnutých opatření, pokud jde o **kybernetickou bezpečnost sítí 5G**, zejména o **zprávě EU o posouzení rizik** zveřejněné 9. října 2019 a o **boji proti dezinformacím**.

Tato zpráva se zaměřuje zejména na **vnější rozměr** spolupráce v bezpečnostní unii, a to s ohledem na podpis dvou dvoustranných **ujednání o boji proti terorismu** – s Albánií a Republikou Severní Makedonie – a na pokrok, jehož bylo dosaženo ve spolupráci s partnerskými třetími zeměmi při výměně **údajů jmenné evidence cestujících**. Kromě toho Komise spolu s touto zprávou přijala žádost o zmocnění zahájit jednání o dohodě mezi EU a **Novým Zélandem** o výměně osobních údajů za účelem boje proti závažné trestné činnosti a terorismu.

## II. PLNĚNÍ LEGISLATIVNÍCH PRIORIT

### 1. *Předcházení radikalizaci v online prostředí a v komunitách*

**Předcházení radikalizaci** je základem reakce Unie na hrozby, které představuje terorismus. V tomto ohledu je internet nejvýznamnějším bojištěm, na němž jsou teroristé činní v 21. století. Prostory, v nichž mohou radikalizovaní jednotlivci komunikovat a sdílet obsah, umožňují rozvoj celosvětových a rozšiřujících se sítí džihádistických i pravicových násilných extremistů. Proto Komise i nadále prosazuje svůj přístup k radikalizaci online ve dvou rovinách – navržená pravidla pro odstraňování nezákonného teroristického obsahu online by měla posílit dobrovolné partnerství s online platformami.

Zásadní význam pro to má **legislativní návrh týkající se prevence šíření teroristického obsahu online** s jasnými pravidly a zárukami, na jejichž základě by internetové platformy byly povinny odstranit teroristický obsah do jedné hodiny od přijetí odůvodněné žádosti příslušných orgánů a přijímat aktivní opatření přiměřená úrovni vystavení teroristickému obsahu<sup>4</sup>. Probíhají interinstitucionální jednání mezi Evropským parlamentem a Radou – dne 17. října 2019 se uskutečnilo první trojstranné setkání. Vzhledem k hrozbě, kterou představuje teroristický obsah online, vyzývá Komise spolunormotvůrce, aby dosáhli dohody

<sup>4</sup> COM(2018) 640 final ze dne 12. září 2018.

o navrhovaném právním aktu do konce roku 2019.

Navrhovaný právní akt doplňuje dobrovolné partnerství s internetovým odvětvím a dalšími zúčastněnými stranami v rámci **internetového fóra EU**. To od svého vytvoření v roce 2015 napomáhá tomu, aby internetové společnosti podnikaly aktivně kroky k určení a odstranění teroristického obsahu online, a připravilo půdu pro iniciativu vedenou odvětvím známou jako „společná databáze hashů“<sup>5</sup> a zřízení globálního internetového fóra pro boj proti terorismu. Jednotka EU pro oznamování internetového obsahu, která je součástí agentury EU pro prosazování práva Europol, pomohla posílit spolupráci s internetovými společnostmi a přispěla k dosažení celkových cílů internetového fóra EU. Na posledním ministerském zasedání internetového fóra EU dne 7. října 2019 se členské státy EU a vysocí představitelé internetových společností zavázali, že budou spolupracovat na základě takzvaného **krizového protokolu EU**. Krizový protokol EU určuje kritéria pro posílenou spolupráci a zavádí nové způsoby, jak zlepšit reakci na krize. Je to součást úsilí na mezinárodní úrovni o realizaci „christchurchské výzvy k přijetí opatření“<sup>6</sup>, jejímž cílem je zajistit koordinovanou a rychlou reakci, která zabrání šíření virálního teroristického obsahu nebo násilného extremistického obsahu online.

Kromě těchto opatření proti radikalizaci online Komise nadále podporuje snahy na vnitrostátní a místní úrovni **předcházet radikalizaci a bojovat proti ní na místě**. EU na základě bohatých zkušeností a odborných znalostí získaných v rámci sítě pro zvyšování povědomí o radikalizaci nabízí cílenou podporu místním aktérům, včetně měst<sup>7</sup>, a poskytuje příležitosti pro výměnu mezi odborníky z praxe, výzkumnými pracovníky a tvůrci politik. Tato síť například vydala konkrétní pokyny a uspořádala pracovní setkání na podporu příslušných orgánů při práci s dětmi, které pocházejí z oblastí konfliktů<sup>8</sup>. Aby Komise zajistila kontinuitu činností prováděných v rámci sítě pro zvyšování povědomí o radikalizaci, zahájila postup pro novou rámcovou smlouvu týkající se finančních prostředků odhadovaných na 61 milionů EUR na čtyřleté období s počátkem v roce 2020<sup>9</sup>.

#### **Za účelem boje proti hrozbě, kterou představuje teroristický obsah online, vyzývá Komise Evropský parlament a Radu:**

- **do konce tohoto roku dokončit jednání o legislativním návrhu týkajícím se prevence šíření teroristického obsahu online.**

<sup>5</sup> Nástroj vytvořený konsorciem společností, který má usnadnit spolupráci, aby se zabránilo šíření teroristického obsahu napříč platformami.

<sup>6</sup> V reakci na útoky ve městě Christchurch na Novém Zélandu z 15. března 2019 pozvali francouzský prezident Emmanuel Macron a novozélandská premiérka Jacinda Ardernová vedoucí představitele a online platformy do Paříže, aby 15. května 2019 přijali „christchurchskou výzvu k přijetí opatření“. Předseda Juncker výzvu podpořil a oznámil vypracování krizového protokolu EU.

<sup>7</sup> Pokud jde o spolupráci s městy ohledně bezpečnosti, viz také oddíl V.2 o připravenosti a ochraně a zejména o ochraně veřejných prostorů.

<sup>8</sup> [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](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)

<sup>9</sup> Rámcová smlouva je rozdělena do dvou částí: 29 000 000 EUR na podporu činnosti sítě pro zvyšování povědomí o radikalizaci v příštích čtyřech letech a 32 000 000 EUR na posílení kapacit členských států, vnitrostátních, regionálních a místních orgánů a prioritních třetích zemí při účinném boji proti radikalizaci, zejména nabídkou příležitostí pro navazování kontaktů, cílených služeb založených na potřebách a výzkumu a analýz.

## 2. *Silnější a inteligentnější informační systémy pro bezpečnost, správu hranic a řízení migrace*

EU zintenzivňuje výměnu informací, usnadňuje boj proti podvodnému zneužívání totožnosti<sup>10</sup>, zesiluje hraniční kontroly<sup>11</sup>, modernizuje celoevropské databáze donucovacích orgánů<sup>12</sup>, zaplňuje informační mezery<sup>13</sup> a posiluje agenturu EU pro prosazování práva Europol<sup>14</sup>. Klíčem k tomu je **interoperabilita informačních systémů EU**<sup>15</sup>, jež vyžaduje co nejlepší využívání dostupných informací a odstraňování slabých míst. Interoperabilita, která reaguje na potřeby osob pracujících v první linii, povede k rychlejšímu a systematictějšímu přístupu k informacím pro příslušníky donucovacích orgánů, příslušníky pohraniční stráže a imigrační úředníky, a tak přispěje ke zlepšení vnitřní bezpečnosti a správy hranic.

Interoperabilita a veškeré inovace, které s sebou přináší, však budou mít význam pro bezpečnost, správu hranic a řízení migrace na místě, pouze když bude každý členský stát plně uplatňovat související právní předpisy. Proto je **realizace** interoperability nejvyšší prioritou bezpečnostní unie, a to jak na politické, tak na technické úrovni. Komise a Agentura EU pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (eu-LISA) podporují členské státy pomocí odborných znalostí a výměnou osvědčených postupů, přičemž využívají síť národních koordinátorů a vytvářejí přehled výsledků, jehož účelem je umožnit účinná opatření, pokud jde o monitorování a koordinaci. Při plnění ambiciózního cíle, kterým je dosažení plné interoperability informačních systémů EU pro bezpečnost, správu hranic a řízení migrace do roku 2020, bude mít zásadní význam úzká spolupráce mezi agenturami EU, všemi členskými státy a zeměmi přidruženými k schengenskému prostoru.

---

<sup>10</sup> Nařízení (EU) 2019/1157 ze dne 20. června 2019 o posílení zabezpečení průkazů totožnosti občanů Unie a povolení k pobytu vydávaných občanům Unie a jejich rodinným příslušníkům, kteří vykonávají své právo volného pohybu.

<sup>11</sup> Zavedení systematických kontrol prováděných na vnějších hranicích u všech občanů s využitím Schengenského informačního systému. Všechny státy schengenského prostoru, jakož i Rumunsko, Bulharsko, Chorvatsko a Kypr uplatňují pravidla pro systematické kontroly na základě příslušných databází, které byly na vnějších hranicích zavedeny v dubnu 2017. V souladu s těmito pravidly jsou možné dočasné odchylky na pozemních nebo námořních hranicích, ale pouze ve vztahu k občanům EU, a to s ohledem na nepřiměřený dopad na plynulost provozu. Dosud takové odchylky oznámilo šest členských států schengenského prostoru / zemí přidružených k schengenskému prostoru (Finsko, Chorvatsko, Lotyšsko, Maďarsko, Norsko a Slovinsko). Pokud jde o vzdušné hranice, v dubnu 2019 uplynula doba, kdy bylo možné se odchýlit od pravidel pro systematické kontroly.

<sup>12</sup> Posílený Schengenský informační systém (nařízení (EU) 2018/1860 ze dne 28. listopadu 2018, nařízení (EU) 2018/1861 ze dne 28. listopadu 2018, nařízení (EU) 2018/1862 ze dne 28. listopadu 2018) a Evropský informační systém rejstříků trestů rozšířený na státní příslušníky třetích zemí (nařízení (EU) 2019/816 ze dne 17. dubna 2019). Posílení Schengenského informačního systému zahrnuje obecnou povinnost vkládat do systému záznamy související s terorismem.

<sup>13</sup> Systém vstupu/výstupu EU (nařízení (EU) 2017/2226 ze dne 30. listopadu 2017) a Evropský systém pro cestovní informace a povolení (nařízení (EU) 2018/1240 ze dne 12. září 2018) a nařízení (EU) 2018/1241 ze dne 12. září 2018).

<sup>14</sup> V posledních letech byla úloha Europolu značně posílena z hlediska jak rozsahu, tak hloubky. Agentura byla posílena přijetím nařízení o Europolu v roce 2016 (nařízení (EU) 2016/794 ze dne 11. května 2016). Členské státy výrazně zvýšily objem informací sdílených s Eupolem a prostřednictvím Europolu. Zřízení centra Europolu pro boj proti terorismu posílilo analytické schopnosti Europolu v případech terorismu. Rozpočet Europolu se v posledních letech soustavně zvyšoval – z 82 milionů EUR v roce 2014 na 138 milionů EUR v roce 2019. Jednání o rozpočtu na rok 2020 pokračují.

<sup>15</sup> Nařízení (EU) 2019/817 ze dne 20. května 2019 a nařízení (EU) 2019/818 ze dne 20. května 2019.

Na druhé straně Evropský parlament a Rada v tomto ohledu ještě **nedokončily legislativní činnost**. Rychlé dosažení dohody o všech dosud nepřijatých legislativních návrhů má zásadní význam pro úplné a včasné zavedení interoperability. Za prvé, jako součást technického provedení **Evropského systému pro cestovní informace a povolení** jsou zapotřebí technické změny souvisejících nařízení<sup>16</sup>, aby byl systém plně připraven. Komise vyzývá Evropský parlament, aby urychlil práci na těchto technických změnách, a umožnil tak co nejdříve zahájit interinstitucionální jednání. Za druhé, probíhají interinstitucionální jednání o návrhu z května 2018, jehož cílem je posílit a zdokonalit stávající **Vízový informační systém**<sup>17</sup>. Na základě prvního trojstranného setkání, které se uskutečnilo dne 22. října 2019, vyzývá Komise oba spolunormotvůrce, aby jednání urychleně dokončili. Za třetí, stále nebylo dosaženo dohody o návrhu Komise z května 2016, který rozšiřuje oblast působnosti systému **Eurodac**<sup>18</sup> tím, že se uchovávají nejen otisky prstů a příslušné údaje žadatelů o azyl a osob zadržovaných v souvislosti s neoprávněným překročením vnější hranice, ale také údaje týkající se neoprávněně pobývajících státních příslušníků třetích zemí. Navrhované změny by také prodloužily dobu uchovávání otisků prstů a příslušných údajů osob, které vstupují do EU nelegálně. Komise vyzývá spolunormotvůrce, aby přikročili k přijetí návrhu.

**V zájmu posílení informačních systémů EU pro bezpečnost, správu hranic a řízení migrace vyzývá Komise Evropský parlament a Radu:**

- aby pokračovaly v práci na rychlém dosažení dohody o navrhovaných technických změnách, které jsou nezbytné pro zřízení **Evropského systému pro cestovní informace a povolení**,
- aby urychleně vedly a dokončily jednání o návrhu na posílení stávajícího **Vízového informačního systému**,
- aby přijaly legislativní návrh týkající se systému **Eurodac** (*priorita společného prohlášení*).

### 3. *Minimalizace manévrovacího prostoru teroristů*

EU podnikla různé kroky k minimalizaci manévrovacího prostoru teroristů na základě nových pravidel, které jim ztěžují přístup k výbušninám<sup>19</sup>, palným zbraním a financování<sup>20</sup>, a k omezení jejich pohybu<sup>21</sup>.

V zájmu posílení reakce justičních orgánů na terorismus zřídila Agentura EU pro justiční spolupráci v trestních věcech (Eurojust) dne 1. září 2019 **Evropský justiční rejstřík pro boj proti terorismu**. Rejstřík bude shromažďovat justiční informace s cílem vytvářet propojení v řízeních proti osobám podezřelým z teroristických trestných činů, a posílí tak koordinaci mezi státními zástupci při protiteroristických vyšetřováních s možnými přeshraničními dopady.

<sup>16</sup> Nařízení (EU) 2018/1240 ze dne 12. září 2018 a nařízení (EU) 2018/1241 ze dne 12. září 2018.

<sup>17</sup> COM(2018) 302 final ze dne 16. května 2018.

<sup>18</sup> COM(2016) 272 final ze dne 4. května 2016.

<sup>19</sup> Nařízení (EU) 2019/1148 ze dne 20. června 2019 o uvádění prekurzorů výbušnin na trh a o jejich používání. Nařízení vstoupilo v platnost dne 31. července 2019 a použije se 18 měsíců od jeho vstupu v platnost.

<sup>20</sup> Směrnice (EU) 2019/1153 ze dne 11. července 2019 o stanovení pravidel usnadňujících používání finančních a dalších informací k prevenci, odhalování, vyšetřování či stíhání určitých trestných činů.

<sup>21</sup> Zavedení systematických kontrol prováděných na vnějších hranicích u všech občanů s využitím Schengenského informačního systému.

Je však zapotřebí dalšího úsilí o podporu a usnadnění vyšetřování v přeshraničních případech, zejména pokud jde o **přístup k elektronickým důkazům** pro účely prosazování práva. V souvislosti s legislativními návrhy z dubna 2018 na zlepšení přeshraničního přístupu k elektronickým důkazům při vyšetřováních trestních činů<sup>22</sup> musí Evropský parlament ještě přijmout svůj vyjednávací postoj a až poté budou moci spolunormotvůrci zahájit vyjednávání. Komise vyzývá Evropský parlament, aby urychlil projednávání tohoto legislativního návrhu tak, aby spolunormotvůrci mohli usilovat o jeho rychlé přijetí. Na základě svého návrhu vnitřních pravidel EU se Komise rovněž zapojuje do **mezinárodních jednání**, která mají zlepšit přeshraniční přístup k elektronickým důkazům. Dne 25. září 2019 uspořádaly Komise a orgány Spojených států amerických první formální kolo jednání o **dohodě mezi EU a USA o přeshraničním přístupu k elektronickým důkazům**. Další kolo je plánováno na 6. listopad 2019. V souvislosti s probíhajícími rozhovory o **druhém dodatkovém protokolu k Budapešťské úmluvě Rady Evropy o kyberkriminalitě** se Komise jménem Unie zúčastnila tří jednání: v červenci, září a říjnu 2019. I když bylo v těchto rozhovorech dosaženo značného pokroku, je stále třeba se zabývat řadou témat, která jsou pro Unii důležitá, jako jsou záruky ochrany údajů. Jednání o druhém dodatkovém protokolu budou pokračovat v listopadu 2019 a v roce 2020. Urychlený postup v jednáních je důležitý pro to, aby se zlepšila mezinárodní spolupráce při sdílení elektronických důkazů a současně byl zajištěn soulad s právem EU a povinnostmi členských států, které jsou jím vázány, a to i s ohledem na budoucí vývoj tohoto práva.

S ohledem na přetrvávající obavy týkající se praní peněz přijal Evropský parlament dne 19. září 2019 **usnesení o stavu provádění právních předpisů Unie proti praní peněz**<sup>23</sup>, v němž reagoval na soubor čtyř zpráv o boji proti praní peněz, které Komise přijala dne 24. července 2019<sup>24</sup>. Evropský parlament vyzval členské státy, aby zajistily řádné a rychlé provedení směrnic o boji proti praní peněz. Evropský parlament rovněž vyzval Komisi, aby posoudila, zda by nařízení o boji proti praní peněz nebylo vhodnější než směrnice, a aby posoudila potřebu koordinačního a podpůrného mechanismu pro finanční zpravodajské jednotky.

**S cílem zlepšit přístup k elektronickým důkazům pro účely vymáhání práva vyzývá Komise Evropský parlament a Radu:**

- aby dosáhly urychleně dohody o legislativních návrzích týkajících se **elektronických důkazů** (*priorita společného prohlášení*).

#### 4. Zvýšení kybernetické bezpečnosti

Zvýšení kybernetické bezpečnosti je i nadále klíčovým aspektem úsilí o vytvoření skutečné a účinné bezpečnostní unie. Unie provádí strategii kybernetické bezpečnosti EU z roku 2017<sup>25</sup> a posiluje svou odolnost, protože díky jejím opatřením se na ni obtížněji útočí a ona sama se rychleji zotavuje, a posiluje i svůj odrazující účinek, protože zvyšuje pravděpodobnost, že

<sup>22</sup> COM(2018) 225 final ze dne 17. dubna 2018 a COM(2018) 226 final ze dne 17. dubna 2018.

<sup>23</sup> [https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_EN.html)

<sup>24</sup> Zpráva o posouzení rizik praní peněz a financování terorismu, která mají dopad na vnitřní trh a souvisejí s přeshraničními činnostmi (COM(2019) 370 ze dne 24. července 2019), zpráva o propojení vnitrostátních centralizovaných automatizovaných mechanismů (centrálních registrů nebo centrálních elektronických systémů vyhledávání dat) členských států týkajících se bankovních účtů (COM(2019) 372 final ze dne 24. července 2019), zpráva o posouzení nedávných případů údajného praní peněz v evropských úvěrových institucích (COM(2019) 373 final ze dne 24. července 2019), zpráva o posouzení rámce spolupráce mezi finančními zpravodajskými jednotkami (COM(2019) 371 final ze dne 24. července 2019).

<sup>25</sup> JOIN(2017) 450 final ze dne 13. září 2017.

útočníci budou dopadeni a potrestáni, a to i na základě souboru nástrojů pro diplomacii v oblasti kybernetiky. Unie rovněž podporuje členské státy při kybernetické obraně a provádí politický rámec EU pro kybernetickou obranu<sup>26</sup>.

Vstupem aktu o kybernetické bezpečnosti<sup>27</sup> v platnost v červnu 2019 se rýsuje **rámec EU pro certifikaci kybernetické bezpečnosti**. Certifikace hraje rozhodující roli při zvyšování důvěry v produkty a služby a jejich bezpečnost, které mají zásadní význam pro jednotný digitální trh. Rámec pro certifikaci poskytne celounijní systémy certifikace jako komplexní soubor pravidel, technických požadavků, norem a postupů. Týká se dvou skupin odborníků, a to Evropské skupiny pro certifikaci kybernetické bezpečnosti, zastupující orgány členských států, a Skupiny zúčastněných stran pro certifikaci kybernetické bezpečnosti, zastupující průmysl. Posledně uvedená skupina spojuje stranu poptávky a nabídky produktů a služeb informačních a komunikačních technologií, včetně malých a středních podniků, poskytovatelů digitálních služeb, evropských a mezinárodních normalizačních orgánů, vnitrostátních akreditačních orgánů, orgánů dozoru nad ochranu údajů a subjektů pro posuzování shody.

Na druhé straně musí Evropský parlament a Rada ještě dosáhnout dohody o legislativní iniciativě<sup>28</sup> týkající se **Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost a sítě národních koordinačních center**. Účelem návrhu je posílit kapacitu Unie v oblasti kybernetické bezpečnosti podporou evropského technologického a průmyslového kybernetickobezpečnostního ekosystému i koordinací a sdružováním souvisejících zdrojů. Komise vyzývá oba spolunormotvůrce, aby v zájmu zvýšení kybernetické bezpečnosti obnovili a urychleně uzavřeli interinstitucionální jednání o této prioritní iniciativě.

Práce na posílení kybernetické bezpečnosti zahrnuje podporu na celostátní i regionální úrovni<sup>29</sup>.

EU se i nadále zabývá nejen kybernetickými hrozbami zacílenými na systémy a údaje, ale i komplexními a mnohotvárnými výzvami představovanými **hybridními hrozbami**. V Radě byla zřízena horizontální pracovní skupina pro boj proti hybridním hrozbám, aby byla zlepšena odolnost EU a jejích členských států vůči hybridním hrozbám a podpořena opatření na posílení odolnosti společností vůči krizi. Komise a Evropská služba pro vnější činnost tyto snahy podporují na základě Společného rámce pro boj proti hybridním hrozbám z roku 2016<sup>30</sup> a společného sdělení z roku 2018 o zvýšení odolnosti a posílení kapacit pro řešení hybridních hrozeb<sup>31</sup>. Kromě toho Společné výzkumné středisko rozpracovává rámec „konceptního modelu“, který má charakterizovat hybridní hrozby, s cílem pomoci členským státům a jejich příslušným orgánům určit typ hybridního útoku, jemuž by mohly čelit. Model se zabývá způsobem, jakým určitý aktér (státní nebo nestátní) využívá v různých oblastech (hospodářské, vojenské, sociální a politické) řadu nástrojů (od dezinformací po špionáž nebo fyzické operace) k ovlivnění svého terče tak, aby dosáhl řady cílů.

<sup>26</sup> Politický rámec EU pro kybernetickou obranu (aktualizace z roku 2018) ve znění přijatém Radou dne 19. listopadu 2018 (14413/18).

<sup>27</sup> Nařízení (EU) 2019/881 ze dne 17. dubna 2019.

<sup>28</sup> COM(2018) 630 final ze dne 12. září 2018.

<sup>29</sup> Komise například podporuje meziregionální inovační partnerství v kybernetické bezpečnosti, jehož se účastní Bretaň, Castilla y León, Nordrhein-Westfalen, Střední Finsko a Estonsko, s cílem vytvořit hodnotové řetězce evropské kybernetické bezpečnosti se zaměřením na uvádění na trh a rozvoj.

<sup>30</sup> JOIN(2016) 18 final ze dne 6. dubna 2016.

<sup>31</sup> JOIN(2018) 16 final ze dne 13. června 2018.

### V zájmu zvýšení kybernetické bezpečnosti vyzývá Komise Evropský parlament a Radu:

- aby urychleně dosáhly dohody o legislativním návrhu týkajícím se **Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center**.

### III. ZVÝŠENÍ BEZPEČNOSTI DIGITÁLNÍ INFRASTRUKTURY

Sítě páté generace (5G) budou tvořit páteř stále digitalizovanějších ekonomik a společností. Propojí miliardy předmětů a systémů, a to i v tak kriticky významných odvětvích, jako jsou energetika, doprava, bankovníctví a zdravotnictví, a budou je využívat i průmyslové řídicí systémy, které obsahují citlivé informace a podporují bezpečnostní systémy. Je proto zásadní zajistit kybernetickou bezpečnost a odolnost sítí 5G.

Členské státy dne 9. října 2019 zveřejnily – jako součást koordinovaného přístupu – zprávu o **posouzení rizik souvisejících s kybernetickou bezpečností sítí 5G, koordinovaném EU**, a to s podporou Komise a Agentury Evropské unie pro kybernetickou bezpečnost<sup>32</sup>. Tento významný krok je součástí provádění doporučení Evropské komise z března 2019 s cílem zajistit vysokou úroveň kybernetické bezpečnosti sítí 5G v celé EU<sup>33</sup>. Zpráva vychází z výsledků vnitrostátních posouzení rizik v oblasti kybernetické bezpečnosti vypracovaných všemi členskými státy. Poukazuje na hlavní hrozby a jejich původce, nejohroženější zařízení, hlavní slabiny (včetně technických a jiných typů zranitelných míst) a řadu strategických rizik. Posouzení poskytuje základ pro stanovení opatření na zmírnění rizik, která lze uplatnit na vnitrostátní i unijní úrovni.

Zpráva uvádí řadu významných **výzev v oblasti kybernetické bezpečnosti**, které se v sítích 5G pravděpodobně objeví nebo stanou výraznějšími. Tyto bezpečnostní výzvy souvisí především s klíčovými *inovacemi* v technologii 5G, zejména s důležitostí softwaru a širokou škálou služeb a aplikací, které umožňuje 5G, jakož i s úlohou *dodavatelů* při budování a provozování sítí 5G a s mírou závislosti na jednotlivých dodavatelích. To znamená, že produkty, služby a činnost dodavatelů se stále více stávají součástí „prostoru k útoku“ v sítích 5G. Navíc bude obzvláště důležitý rizikový profil jednotlivých dodavatelů, včetně pravděpodobnosti, že dodavatel je předmětem zasahování třetí země.

V souladu s postupem stanoveným v doporučení Komise z března 2019 by se členské státy měly do 31. prosince 2019 dohodnout na **souboru zmírňujících opatření**, jež budou zjištěná rizika v oblasti kybernetické bezpečnosti na vnitrostátní úrovni a na úrovni Unie řešit. Komise a Evropská služba pro vnější činnost budou rovněž pokračovat ve výměně názorů na kybernetickou bezpečnost a odolnost sítí 5G s podobně smýšlejícími partnery. V tomto ohledu je Komise v kontaktu s NATO, a to v souvislosti s posouzením rizik kybernetické bezpečnosti sítí 5G, koordinovaným EU.

<sup>32</sup> Skupina pro spolupráci příslušných orgánů, jak je stanoveno ve směrnici o bezpečnosti sítí a informačních systémů (směrnice (EU) 2016/1148 ze dne 6. července 2016), s pomocí Komise a Evropské agentury pro kybernetickou bezpečnost dokončila posouzení rizik souvisejících s kybernetickou bezpečností sítí 5G, koordinované EU: <https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>.

<sup>33</sup> C(2019) 2355 final ze dne 26. března 2019.

#### IV. BOJ PROTI DEZINFORMACÍM A OCHRANA VOLEB PŘED DALŠÍMI KYBERNETICKÝMI HROZBAMI

EU zavedla **rámec pro koordinovaná opatření proti dezinformacím**, který plně respektuje evropské hodnoty a základní práva<sup>34</sup>. Na základě akčního plánu proti dezinformacím<sup>35</sup> pokračuje úsilí o minimalizaci prostoru pro dezinformace, a to i za účelem chránit integritu voleb.

Ústředním bodem je spolupráce s odvětvím prostřednictvím samoregulačního **kodexu zásad boje proti dezinformacím** pro online platformy a odvětví reklamy, který začal platit v říjnu 2018.<sup>36</sup> Po prvním roce fungování kodexu posoudila Komise jeho účinnost na základě výročních sebehodnotících zpráv, které předložily online platformy a další signatáři kodexu a které byly zveřejněny dne 29. října 2019 spolu s prohlášením Komise<sup>37</sup>. Zprávy obecně dokládají, že signatáři vynakládají na plnění svých závazků značné úsilí.

Opatření přijatá signatáři platformy se liší co do rychlosti a rozsahu ve všech pěti oblastech závazků, jimiž se kodex zabývá. Obecně je pokrok větší, pokud jde o závazky týkající se evropských voleb v roce 2019, zejména závazek narušit reklamní a peněžité pobídky k dezinformacím (oblast 1), zajistit transparentnost politické a tematické reklamy (oblast 2) a zajistit integritu služeb ve vztahu k neautentickým účtům a chování (oblast 3). Oproti tomu je pokrok menší nebo nulový, pokud jde o závazky posílit postavení spotřebitelů (oblast 4) a závazky posílit postavení výzkumné obce, a to i na základě toho, že by platformy v souladu s požadavky na ochranu soukromí poskytovaly příslušný přístup k datovým souborům pro výzkumné účely (oblast 5). Jednotlivé platformy se rovněž liší v rozsahu opatření, která přijímají, aby zajistily plnění svých závazků, a stejně tak existují rozdíly mezi členskými státy v tom, jak uplatňují jednotlivé politiky. Komise i nadále spolupracuje se signatáři kodexu a dalšími zúčastněnými stranami, aby se boj proti dezinformacím vystupňoval.

Komise a vysoká představitelka ve spolupráci s členskými státy zřídily na základě akčního plánu proti dezinformacím **systém včasného varování**, který má řešit dezinformační kampaně. Systém včasného varování umožnil orgánům EU a členským státům sdílet informace a analýzy před volbami do Evropského parlamentu v roce 2019 a koordinovat reakci. Po volbách se tato práce ještě zintenzivnila: každý den probíhaly výměny na pracovní úrovni a různé členské státy uspořádaly tři zasedání kontaktních míst systému včasného varování.

Další praktický krok ke zjištění dezinformací souvisí s prací **týmu pro strategickou komunikaci**, a zejména pracovní skupiny East StratCom, která realizuje projekt „EUvsDisinfo“ s účelem monitorovat a analyzovat prokremelské dezinformace a reagovat na

<sup>34</sup> Viz akční plán proti dezinformacím (JOIN(2018) 36 final ze dne 5. prosince 2018).

<sup>35</sup> JOIN(2019) 12 final ze dne 14. června 2019.

<sup>36</sup> Online platformy Google, Facebook, Twitter a Microsoft se na základě kodexu zavázaly, že zabrání manipulativnímu využívání svých služeb pochybnými subjekty, zajistí transparentnost a zveřejňování politické reklamy a přijmou další opatření ke zlepšení transparentnosti, odpovědnosti a důvěryhodnosti online ekosystému. Obchodní sdružení z odvětví reklamy se rovněž zavázala spolupracovat s platformami, aby byla zlepšena kontrola umísťování reklamy a byly vytvořeny nástroje na ochranu značky, jejichž účelem je omezit reklamu na internetových stránkách šířících dezinformace.

<sup>37</sup> [https://ec.europa.eu/commission/presscorner/detail/cs/statement\\_19\\_6166](https://ec.europa.eu/commission/presscorner/detail/cs/statement_19_6166). Vedle společností Google, Facebook, Twitter a Microsoft jsou dalšími signatáři kodexu společnost Mozilla, sedm sdružení na evropské nebo národní úrovni zastupující odvětví reklamy a EDiMA, evropské sdružení zastupující platformy a další technologické společnosti působící v online odvětví.

ně<sup>38</sup>. Od začátku roku 2019 umožnil první zvláštní rozpočet ve výši 3 milionů EUR zvýšit a rozšířit tuto práci tak, aby zahrnovala monitorování a analýzu prokremelských dezinformací na internetu, ve vysílání a v sociálních médiích v 19 jazycích od angličtiny po srbštinu a arabštinu. Množství odhalených dezinformačních činností se v důsledku zlepšené monitorovací kapacity více než zdvojnásobilo, přičemž v roce 2019 bylo dosud zaznamenáno 2 000 případů dezinformací, zatímco v roce 2018 ve stejném období 765 případů. Pracovní skupina East StratCom hrála klíčovou roli při monitorování a odhalování prokremelských dezinformací zaměřených na volby do Evropského parlamentu v roce 2019. Výzkum byl spojen s kampaní ke zvýšení povědomí o pokusech o vměšování do volebních procesů po celém světě. Aktivní pomoc pracovní skupiny poskytovaná v úzké spolupráci s Evropským parlamentem a Komisí vedla k více než 20 rozhovorům ve sdělovacích prostředcích, zatímco v kampani se angažovalo více než 300 novinářů.

Komise rovněž přijala opatření, aby **omezila šíření dezinformací a mýtů o orgánech a politikách EU**. Vytvořila síť odborníků na komunikaci, která má online portál poskytující interaktivní informační materiály o politikách EU a problému dezinformací i jejich dopadu na společnost. Zahájila také – ve spolupráci s Evropským parlamentem a Evropskou službou pro vnější činnost – řadu kampaní v sociálních médiích zaměřených na boj proti dezinformacím<sup>39</sup>.

## V. PROVÁDĚNÍ DALŠÍCH PRIORIT V OBLASTI BEZPEČNOSTI

### 1. *Provádění legislativních opatření v rámci bezpečnostní unie*

Dohodnutá opatření v bezpečnostní unii budou plně přínosná pro bezpečnost, pouze pokud členské státy zajistí jejich rychlé a úplné provedení. Za tímto účelem Komise členské státy aktivně podporuje při provádění právních předpisů EU, mimo jiné financováním a usnadňováním výměny osvědčených postupů. Komise plně využívá své pravomoci podle Smluv k prosazování práva EU, včetně případných řízení o nesplnění povinnosti.

Lhůta pro provedení **směrnice EU o jmenné evidenci cestujících**<sup>40</sup> uplynula dne 25. května 2018. K dnešnímu datu oznámilo úplné provedení 25 členských států<sup>41</sup>, což představuje významný pokrok od července 2018, kdy Komise zahájila řízení o nesplnění povinnosti proti 14 členským státům<sup>42</sup>. Dva členské státy dosud neoznámily plné provedení, a to navzdory probíhajícímu řízení o nesplnění povinnosti zahájeným dne 19. července 2018<sup>43</sup>. Komise souběžně i nadále podporuje všechny členské státy v jejich úsilí o dokončení vývoje systémů jmenné evidence cestujících, a to i tím, že usnadňuje výměnu informací a osvědčených postupů.

Lhůta pro provedení **směrnice o boji proti terorismu**<sup>44</sup> uplynula dne 8. září 2018. K

<sup>38</sup> [www.euvdisinfo.eu](http://www.euvdisinfo.eu)

<sup>39</sup> <https://europa.eu/euprotects/>

<sup>40</sup> Směrnice (EU) 2016/681 ze dne 27. dubna 2016. Dánsko se nepodílelo na přijímání této směrnice, která pro ně není závazná ani použitelná.

<sup>41</sup> Odkazy na oznámení o úplném provedení zohledňují prohlášení členských států a není jimi dotčena kontrola provedení ve vnitrostátním právu ze strany útvarů Komise (stav ke dni 17. října 2019).

<sup>42</sup> Viz šestnáctá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii (COM(2018) 690 final ze dne 10. října 2018).

<sup>43</sup> Slovinsko oznámilo částečné provedení. Španělsko provedení neoznámilo (stav ke dni 17. října 2019).

<sup>44</sup> Směrnice (EU) 2017/541 ze dne 15. března 2017. Tato směrnice není použitelná ve Spojeném království, Irsku a Dánsku.

dnešnímu datu oznámilo úplné provedení 22 členských států, což představuje významný pokrok od listopadu 2018, kdy Komise zahájila řízení o nesplnění povinnosti proti 16 členským státům<sup>45</sup>. Tři členské státy dosud neoznámily plné provedení, a to navzdory probíhajícím řízením o nesplnění povinnosti<sup>46</sup>. Dne 25. července 2019 zaslala Komise dvěma členským státům odůvodněná stanoviska, protože neoznámily úplné provedení směrnice<sup>47</sup>. V reakci na to oba členské státy oznámily, že legislativní činnost bude dokončena v tomto roce.

Lhůta pro provedení **směrnice o kontrole nabývání a držení zbraní**<sup>48</sup> uplynula dne 14. září 2018. K dnešnímu dni oznámilo úplné provedení 13 členských států. Patnáct členských států dosud úplné provedení neoznámilo, a to navzdory probíhajícím řízením o nesplnění povinnosti zahájeným dne 22. listopadu 2018<sup>49</sup>. Dne 25. července 2019 zaslala Komise 20 členským státům odůvodněná stanoviska, protože neoznámily úplné provedení směrnice. V reakci na to oznámilo pět členských států provedení směrnice v plném rozsahu<sup>50</sup>.

Lhůta pro provedení **směrnice o ochraně údajů při prosazování práva**<sup>51</sup> uplynula dne 6. května 2018. K dnešnímu datu oznámilo úplné provedení 25 členských států, což představuje významný pokrok od července 2018, kdy Komise zahájila řízení o nesplnění povinnosti proti 19 členským státům<sup>52</sup>. Tři členské státy dosud neoznámily plné provedení, a to navzdory probíhajícím řízením o nesplnění povinnosti<sup>53</sup>. Dne 25. července 2019 se Komise rozhodla předložit věc dvou členských států<sup>54</sup> Soudnímu dvoru Evropské unie, protože tuto směrnici neprovedly, a zaslala výzvu jednomu členskému státu<sup>55</sup>, protože tuto směrnici neprovedl plně<sup>56</sup>.

Komise nyní posuzuje provedení **čtvrté směrnice o boji proti praní peněz**<sup>57</sup> a zároveň ověřuje, zda členské státy tato pravidla provedly. Měly povinnost tuto směrnici provést ve vnitrostátním právu do 26. června 2018. Komise pokračuje v řízení o nesplnění povinnosti proti 21 členským státům, neboť na základě informací od těchto členských států usoudila, že směrnici neprovedly v plném rozsahu<sup>58</sup>.

---

<sup>45</sup> Viz sedmnáctá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii (COM(2018) 845 final ze dne 11. prosince 2018).

<sup>46</sup> Řecko a Lucembursko neoznámily vnitrostátní prováděcí opatření. Polsko oznámilo vnitrostátní opatření odpovídající částečnému provedení (stav k 17. říjnu 2019).

<sup>47</sup> Řecko a Lucembursko.

<sup>48</sup> Směrnice (EU) 2017/853 ze dne 17. října 2019.

<sup>49</sup> Belgie, Česko, Estonsko, Polsko, Slovensko, Spojené království a Švédsko oznámily prováděcí opatření týkající se části nových ustanovení. Kypr, Lucembursko, Maďarsko, Německo, Řecko, Španělsko, Rumunsko a Slovinsko neoznámily žádná prováděcí opatření (stav ke dni 17. října 2019).

<sup>50</sup> Finsko, Irsko, Litva, Nizozemsko a Portugalsko (stav ke dni 17. října 2019).

<sup>51</sup> Směrnice (EU) 2016/680 ze dne 27. dubna 2016.

<sup>52</sup> Viz šestnáctá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii (COM(2018) 690 final ze dne 10. října 2018).

<sup>53</sup> Slovinsko oznámilo částečné provedení. Španělsko provedení neoznámilo. Německo sice oznámilo úplné provedení směrnice ve vnitrostátním právu, ale Komise toto provedení považuje za neúplné (stav ke dni 17. října 2019).

<sup>54</sup> Řecko a Španělsko.

<sup>55</sup> Německo.

<sup>56</sup> Řecko oznámilo úplné provedení a Komise je nyní posuzuje.

<sup>57</sup> Směrnice (EU) 2015/849 ze dne 20. května 2015.

<sup>58</sup> Belgie, Bulharsko, Česko, Dánsko, Německo, Estonsko, Irsko, Francie, Itálie, Kypr, Lotyšsko, Litva, Maďarsko, Nizozemsko, Rakousko, Polsko, Rumunsko, Slovensko, Finsko, Švédsko a Spojené království

Komise posoudila soulad provedení **směrnic souvisejících s kybernetickou kriminalitou**. V červenci a říjnu 2019 zahájila řízení o nesplnění povinnosti proti 23 členským státům<sup>59</sup>, protože usoudila, že jimi oznámená vnitrostátní prováděcí opatření nepředstavují správné provedení **směrnice o boji proti pohlavnímu zneužívání dětí**<sup>60</sup>. Komise obdobně v červenci a říjnu 2019 zahájila řízení o nesplnění povinnosti proti čtyřem členským státům<sup>61</sup>, protože usoudila, že jimi oznámená vnitrostátní prováděcí opatření nepředstavují správné provedení **směrnice o útocích na informační systémy**<sup>62</sup>.

**Komise naléhavě vyzývá členské státy, aby přijaly nezbytná opatření k úplnému provedení následujících směrnic ve vnitrostátním právu a oznámily je Komisi:**

- **směrnice EU o jmenné evidenci cestujících**, u níž jeden členský stát dosud neoznámil provedení ve vnitrostátním právu a jeden členský stát ještě musí oznámení o provedení dokončit<sup>63</sup>,
- **směrnice o boji proti terorismu**, u níž dva členské státy dosud neoznámily provedení ve vnitrostátním právu a jeden členský stát ještě musí oznámení o provedení dokončit<sup>64</sup>,
- **směrnice o kontrole nabývání a držení zbraní**, u níž osm členských států dosud neoznámilo provedení ve vnitrostátním právu a sedm členských států ještě musí oznámení o provedení dokončit<sup>65</sup>,
- **směrnice o ochraně údajů při prosazování práva**, u níž jeden členský stát dosud neoznámil provedení ve vnitrostátním právu a dva členské státy ještě musí oznámení o provedení dokončit<sup>66</sup>,
- **čtvrtá směrnice o boji proti praní peněz**, u níž 21 členských států ještě musí dokončit oznámení o provedení<sup>67</sup>;
- **směrnice o boji proti pohlavnímu zneužívání dětí**, u níž bylo zahájeno řízení o nesplnění povinnosti proti 23 členským státům z důvodu nesprávného provedení ve vnitrostátním právu<sup>68</sup>,
- **směrnice o útocích na informační systémy**, u níž bylo zahájeno řízení o nesplnění povinnosti proti čtyřem členským státům z důvodu nesprávného provedení ve vnitrostátním právu<sup>69</sup>.

(stav ke dni 17. října 2019). Předtím bylo 7 řízení o nesplnění povinnosti v souvislosti s touto směrnicí uzavřeno.

<sup>59</sup> Belgie, Bulharsko, Česko, Německo, Estonsko, Řecko, Španělsko, Francie, Chorvatsko, Itálie, Lotyšsko, Litva, Lucembursko, Maďarsko, Malta, Rakousko, Polsko, Portugalsko, Rumunsko, Slovinsko, Slovensko, Finsko a Švédsko.

<sup>60</sup> Směrnice 2011/93/EU ze dne 13. prosince 2011.

<sup>61</sup> Bulharsko, Itálie, Portugalsko a Slovinsko.

<sup>62</sup> Směrnice 2013/40/EU ze dne 12. srpna 2013.

<sup>63</sup> Slovinsko oznámilo částečné provedení. Španělsko provedení neoznámilo (stav ke dni 17. října 2019).

<sup>64</sup> Řecko a Lucembursko provedení neoznámily. Polsko oznámilo částečné provedení (stav ke dni 17. října 2019).

<sup>65</sup> Belgie, Česko, Estonsko, Polsko, Švédsko, Slovensko a Spojené království oznámily prováděcí opatření týkající se části nových ustanovení. Kypr, Německo, Řecko, Španělsko, Lucembursko, Maďarsko, Rumunsko a Slovinsko neoznámily žádná prováděcí opatření (stav ke dni 17. října 2019).

<sup>66</sup> Slovinsko oznámilo částečné provedení. Španělsko provedení neoznámilo. Německo sice oznámilo úplné provedení směrnice ve vnitrostátním právu, ale Komise toto provedení považuje za neúplné (stav ke dni 17. října 2019).

<sup>67</sup> Belgie, Bulharsko, Česko, Dánsko, Německo, Estonsko, Irsko, Francie, Itálie, Kypr, Lotyšsko, Litva, Maďarsko, Nizozemsko, Rakousko, Polsko, Rumunsko, Slovensko, Finsko, Švédsko a Spojené království (stav ke dni 17. října 2019).

<sup>68</sup> Belgie, Bulharsko, Česko, Německo, Estonsko, Řecko, Španělsko, Francie, Chorvatsko, Itálie, Lotyšsko, Litva, Lucembursko, Maďarsko, Malta, Rakousko, Polsko, Portugalsko, Rumunsko, Slovinsko, Slovensko, Finsko a Švédsko.

## 2. Přípravenost a ochrana

Podstatnou součástí úsilí o vytvoření účinné a skutečné bezpečnostní unie je vytváření odolnosti vůči bezpečnostním hrozbám. Komise podporuje členské státy a místní orgány při posilování ochrany veřejných prostorů, realizaci akčního plánu z října 2017 a partnerství pro bezpečnost ve veřejných prostorech v rámci městské agendy EU z ledna 2019. Tato činnost se týká měst, která se obrátila na Komisi a požádala o podporu při řešení problémů, s nimiž se potýkají při ochraně veřejných prostorů.

Klíčem k posílení bezpečnosti veřejných prostorů je výměna osvědčených postupů mezi místními orgány a soukromými subjekty. To bylo středobodem **Evropského týdne bezpečnosti**, který byl ve dnech 14. až 18. října 2019 uspořádán v Nice ve Francii v rámci projektu „Chránit spřízněná města proti terorismu při zabezpečování městských oblastí“, financovaného z prostředků EU. Setkání, na němž se sešlo 500 účastníků z měst z celé Evropy, vnitrostátních orgánů a výzkumných institucí, zdůraznilo význam úzké spolupráce všech zúčastněných stran, veřejných i soukromých, a úlohu nových technologií při zlepšování ochrany měst. Ochrana veřejných prostorů byla také důležitým prvkem **Evropského týdne regionů a měst**, který se konal v Bruselu ve dnech 7. až 10. října 2019 a během něhož se uskutečnil workshop na téma městská agenda pro partnerství EU v zájmu bezpečnosti ve veřejných prostorech. Zaměřil se na úlohu místních orgánů v oblasti bezpečnostní politiky, unijní regulaci a financování, jejichž účelem je řešit hlavní bezpečnostní problémy v městských veřejných prostorech, a na klíčová témata, jako jsou inovace prostřednictvím inteligentních řešení a technologií, včetně koncepce bezpečnosti již od fáze návrhu, prevence a sociálního začleňování. Komise rovněž přispívá k podpoře inovací měst v těchto oblastech svou poslední výzvou k podávání návrhů na Městská inovativní opatření, jejíž výsledky byly oznámeny v srpnu 2019. V rámci vybraných projektů budou tři města (Pireus v Řecku, Tampere ve Finsku a Turín v Itálii) testovat nová řešení týkající se bezpečnosti ve městech<sup>70</sup>.

S cílem lépe **chránit místa pro konání bohoslužeb** a prozkoumat potřeby různých náboženských skupin uspořádala Komise dne 7. října 2019 setkání se zástupci židovských, muslimských, křesťanských a buddhistických společenství. Setkání, které bylo součástí provádění akčního plánu EU na podporu ochrany veřejných prostorů z roku 2017, poukázalo na to, že se povědomí o bezpečnosti a připravenost mezi různými náboženskými komunitami značně liší, a zdůraznilo význam další výměny osvědčených postupů. Ze zasedání rovněž vyplynulo, že zavedení základních bezpečnostních opatření a lepší povědomí o bezpečnosti nejsou neslučitelné se zachováním otevřeného a přístupného charakteru míst pro konání bohoslužeb. Komise bude shromažďovat osvědčené postupy a informační materiály na své elektronické expertní platformě a na tuto věc upozorní bezpečnostní orgány členských států na fóru veřejného a soukromého sektoru pro ochranu veřejných prostorů.

Jednou z konkrétních oblastí, které vyžadují další pozornost, je rostoucí bezpečnostní hrozba, kterou pro kritickou infrastrukturu a veřejné prostory představují **drony**. Komise podporuje členské státy při sledování trendů v zneužívání dronů, financuje relevantní výzkum a usnadňuje testování protiopatření, a doplňuje tak nedávné právní předpisy EU<sup>71</sup> týkající se bezpečného provozu dronů ve vzdušném prostoru s letadly s posádkou, aniž ohrožuje

<sup>69</sup> Bulharsko, Itálie, Portugalsko a Slovinsko.

<sup>70</sup> Městská inovativní opatření jsou nástrojem spolufinancovaným Evropským fondem pro regionální rozvoj. Další informace naleznete zde: <https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals>.

<sup>71</sup> Prováděcí nařízení Komise (EU) 2019/947 ze dne 24. května 2019 o pravidlech a postupech pro provoz bezpilotních letadel.

možnosti přínosného používání dronů. Výměna zkušeností a osvědčených postupů má zásadní význam, jak ukázala mezinárodní konference na vysoké úrovni, která se uskutečnila v Bruselu dne 17. října 2019 a byla věnována boji proti hrozbám ze strany systémů bezpilotních letadel. Na této akci uspořádané Komisí jednalo více než 250 zástupců členských států, mezinárodních organizací, partnerů ze třetích zemí, odvětví, akademické obce a občanské společnosti o bezpečnostních problémech, které představují drony, a o způsobech jejich řešení. Setkání ukázalo, že je třeba, aby byla rizika spojená s drony pravidelně posuzována a aby letecké a donucovací orgány při dalším rozpracovávání evropských právních předpisů o bezpečném provozu dronů úzce spolupracovaly. Je také zapotřebí dále testovat protipatření v souvislosti s drony na základě koordinovaného evropského přístupu. Kromě toho se účastníci shodli na tom, že pro to, aby byly drony bezpečné, zabezpečené, provozně spolehlivé a obtížně zneužitelné k nekalým účelům, je zásadní úzká spolupráce mezi orgány a odvětvím.

### 3. *Vnější rozměr*

Jelikož většina bezpečnostních rizik, jimž Unie čelí, přesahuje hranice EU a představuje globální hrozby, hraje při budování účinné a skutečné bezpečnostní unie zásadní roli spolupráce s partnerskými zeměmi, organizacemi a příslušnými zúčastněnými stranami.

Hlavním prvkem této spolupráce je výměna informací. Komise spolu s touto zprávou přijala doporučení, aby Rada schválila zmocnění k zahájení jednání o **dohodě mezi EU a Novým Zélandem o výměně osobních údajů za účelem boje proti závažné trestné činnosti a terorismu** mezi Europolem a novozélandskými příslušnými orgány. Tato dohoda dále posílí schopnost Europolu spolupracovat s Novým Zélandem za účelem prevence trestných činů, které spadají do působnosti Europolu, a boje proti nim. Třebaže pracovní ujednání mezi Europolem a novozélandskou policií z dubna 2019 poskytuje rámec pro strukturovanou spolupráci na strategické úrovni, neposkytuje právní základ pro výměnu osobních údajů. Výměna osobních údajů při plném dodržování práva EU a základních práv má zásadní význam pro účinnou operativní policejní spolupráci. Komise již dříve na základě teroristické hrozby, výzev spojených s migrací a operativních potřeb Europolu zahájit jednání určila osm prioritních zemí v oblasti Blízkého východu / severní Afriky<sup>72</sup>. S ohledem na operativní potřeby donucovacích orgánů v celé EU a na možné výhody užší spolupráce v této oblasti, jak ukázaly i kroky následující po útoku ve městě Christchurch z března 2019, Komise považuje za nezbytné přidat Nový Zéland mezi prioritní země, s nimiž je třeba zahájit jednání v krátkodobém výhledu.

Dalším úhelným kamenem bezpečnostní spolupráce Unie s partnery ze třetích zemí je předávání **údajů jmenné evidence cestujících**. Dne 27. září 2019 přijala Komise doporučení Radě týkající se zmocnění k zahájení jednání o dohodě mezi **EU a Japonskem** o předávání údajů jmenné evidence cestujících za účelem prevence terorismu a jiné závažné nadnárodní trestné činnosti a boje proti nim při plném dodržování záruk ochrany údajů a základních práv<sup>73</sup>. Doporučení je přezkoumáváno na úrovni pracovní skupiny Rady a Komise vyzývá Radu, aby urychleně přijala mandát pro jednání s Japonskem. Kdyby byla opatření zavedena včas před olympijskými hrami v roce 2020, znamenalo by to skutečný přínos pro bezpečnost.

<sup>72</sup> Viz jedenáctá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii (COM(2017) 608 final ze dne 18. října 2017). Prioritními zeměmi jsou Alžírsko, Egypt, Izrael, Jordánsko, Libanon, Maroko, Tunisko a Turecko.

<sup>73</sup> COM(2019) 420 final ze dne 27. září 2019.

Na celosvětové úrovni podporuje Komise úsilí **Mezinárodní organizace pro civilní letectví** stanovit standard pro zpracování údajů jmenné evidence cestujících. Je to reakce na rezoluci Rady bezpečnosti OSN č. 2396, která naléhavě vyzývá všechny členské státy OSN, aby rozvíjely schopnost shromažďovat, zpracovávat a analyzovat údaje jmenné evidence cestujících. Dne 13. září 2019 předložila Komise návrh<sup>74</sup> rozhodnutí Rady o postoji, který má být jménem EU zaujat v Mezinárodní organizaci pro civilní letectví, pokud jde o standardy a doporučené postupy pro údaje jmenné evidence cestujících. Návrh je přezkoumáván na úrovni pracovní skupiny Rady a Komise vyzývá k urychlenému přijetí rozhodnutí Rady. Postoj Unie a jejích členských států byl rovněž vytyčen v informačním dokumentu „Normy a zásady pro shromažďování, používání, zpracovávání a ochranu údajů jmenné evidence cestujících“, který byl předložen na 40. zasedání shromáždění Mezinárodní organizace pro civilní letectví.

Pokud jde o práci na nové dohodě o jmenné evidenci cestujících s **Kanadou**, Komise usiluje o rychlou finalizaci dohody. Mezitím byl v létě zahájen kombinovaný společný přezkum a společné hodnocení dohody o jmenné evidenci cestujících s **Austrálií**, jakož i společné hodnocení dohody o jmenné evidenci cestujících se **Spojenými státy**, a to návštěvou Canberry v srpnu a Washingtonu v září 2019. O aktuálním stavu jednání s Japonskem, Austrálií a Kanadou o údajích jmenné evidence cestujících informovala Komise na uzavřeném zasedání dne 14. října 2019 Výbor pro občanské svobody, spravedlnost a vnitřní věci Evropského parlamentu.

Dosaženo bylo i pokroku v bezpečnostní spolupráci s partnery ze **západního Balkánu** a v provádění společného akčního plánu pro boj proti terorismu pro oblast západního Balkánu z října 2018. Dne 9. října podepsala Komise dvě nezávazná dvoustranná ujednání o boji proti terorismu, a to s Albánií a Republikou Severní Makedonie<sup>75</sup>. Tato ujednání stanoví konkrétní prioritní opatření, která mají být přijata orgány příslušné partnerské země, týkají se pěti cílů společného akčního plánu<sup>76</sup> a uvádějí podporu, kterou Komise hodlá poskytnout. Očekává se, že podobná ujednání se zbývajících partnery ze západního Balkánu budou podepsána v nadcházejících týdnech. Komise dále dne 7. října 2019 podepsala s Černou Horou dohodu o spolupráci v oblasti správy hranic mezi Černou Horou a Evropskou agenturou pro pohraniční a pobřežní stráž. Tato dohoda umožňuje agentuře pomáhat Černé Hoře při správě hranic s cílem řešit nelegální migraci a přeshraniční trestnou činnost, a tak zvyšovat bezpečnost na vnějších hranicích EU.

**V zájmu posílení spolupráce s partnerskými zeměmi při řešení společných bezpečnostních hrozeb vyzývá Komise Radu, aby:**

- přijala zmocnění zahájit jednání o dohodě o výměně osobních údajů za účelem boje proti závažné trestné činnosti a terorismu mezi EU a **Novým Zélandem**,
- přijala zmocnění zahájit jednání o dohodě o předávání údajů jmenné evidence cestujících mezi EU a **Japonskem**,
- přijala navržené **rozhodnutí Rady o postoji, který má být jménem EU zaujat**

<sup>74</sup> COM(2019) 416 final ze dne 13. září 2019.

<sup>75</sup> [https://ec.europa.eu/home-affairs/news/news/20191009\\_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia\\_en](https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en)

<sup>76</sup> Společný akční plán stanoví opatření týkající se těchto pěti cílů: pevný rámec pro boj proti terorismu, účinná prevence násilného extremismu a boj proti němu, účinná výměna informací a operativní spolupráce, budování kapacit pro boj proti praní peněz a proti financování terorismu, posílení ochrany občanů a infrastruktury.

**v Mezinárodní organizaci pro civilní letectví, pokud jde o standardy a doporučené postupy pro údaje jmenné evidence cestujících.**

## **VI. ZÁVĚR**

Tato zpráva uvádí širokou škálu opatření, která EU přijímá, aby řešila společné hrozby v Evropě a zvýšila naši kolektivní bezpečnost. Pokrok na cestě k účinné a skutečné bezpečnostní unii, založené na společném chápání toho, že dnešní bezpečnostní výzvy lze nejlépe řešit spoluprací se třetími zeměmi, je výsledkem úzké spolupráce široké škály aktérů, budování důvěry, sdílení zdrojů a společného vyrovnávání se s hrozbami: napříč všemi úrovněmi státní správy, počínaje městy a dalšími místními subjekty, regiony a vnitrostátními orgány až po úroveň EU s Evropským parlamentem a Radou, s účastí orgánů veřejné správy, agentur EU, soukromých subjektů a občanské společnosti a s využitím odborných znalostí, nástrojů a zdrojů v různých oblastech politiky, jako jsou dopravní politika, jednotný digitální trh nebo politika soudržnosti. Práce v rámci bezpečnostní unie je přitom zakotvena v ochraně základních práv, ochraně a podpoře našich hodnot.

Úsilí o účinnou a skutečnou bezpečnostní unii musí pokračovat. Je třeba urychleně dosáhnout dohody o důležitých projednávaných iniciativách, zejména: 1) legislativním návrhu týkajícím se odstraňování teroristického obsahu online, 2) legislativním návrhu na zlepšení přístupu k elektronickým důkazům pro účely vymáhání práva, 3) legislativním návrhu, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center, a 4) dosud neschválených legislativních návrzích týkajících se silnějších a inteligentnějších informačních systémů pro bezpečnost, správu hranic a řízení migrace. Dohodnutá opatření a nástroje se musí proměnit ve funkční realitu v praxi, přičemž všechny členské státy musí včas a v plném rozsahu provádět právní předpisy EU, aby zajistily veškeré jejich přínosy pro bezpečnost. Zejména je nezbytné, aby všechny členské státy prováděly nedávno schválené právní předpisy o interoperabilitě informačních systémů EU pro bezpečnost, správu hranic a řízení migrace, a tak bylo dosaženo ambiciózního cíle dospět k plné interoperabilitě do roku 2020. V neposlední řadě musí Evropa zůstat ostražitá vůči vznikajícím a měnícím se hrozbám a nadále spolupracovat, aby posílila bezpečnost všech občanů.