EVROPSKÁ
KOMISE

V Bruselu dne 25.1.2017
COM(2017) 41 final

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, EVROPSKÉ RADĚ A RADĚ

Čtvrtá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii

Čtvrtá zpráva o pokroku na cestě k účinné a skutečné bezpečnostní unii

I. ÚVOD

Tato zpráva je čtvrtou měsíční zprávou o pokroku, jehož bylo dosaženo na cestě k vytvoření účinné a skutečné bezpečnostní unie, a pojednává o vývoji v rámci dvou hlavních pilířů: *boj proti terorismu a organizované trestné činnosti, jakož i proti prostředkům, které tyto jevy podporují; a posílení naší obrany a budování odolnosti vůči uvedeným hrozbám*. Tato zpráva se zaměřuje na čtyři klíčové oblasti, informační systémy a interoperabilitu, ochranu snadno zranitelných cílů, kybernetické hrozby a ochranu údajů v souvislosti s vyšetřováním trestných činů.

Prosincový útok na vánočním trhu v Berlíně znovu upozornil na závažné nedostatky našich informačních systémů, které je naléhavě třeba řešit, zejména na úrovni EU, aby vnitrostátní pohraniční a donucovací orgány na místě mohly svou náročnou práci vykonávat účinněji. Skutečnost, že různé informační systémy nejsou vzájemně propojeny, což útočníkům umožňuje používat k přesunům vícenásobné identity, aniž by byli odhaleni, též při překračování hranic, a skutečnost, že členské státy tyto údaje nezadávají systematicky do příslušných databází EU, jsou nedostatky praktického provádění, které je třeba co nejdříve odstranit. Kromě toho, pokud jde o opatření pro vymáhání práva na hranicích a navracení osob, jejichž žádosti o azyl byly zamítnuty, je zapotřebí dalšího úsilí[1].

Pokud jde o ochranu snadno zranitelných cílů, Komise urychlí svou činnost zaměřenou na navázání spolupráce mezi odborníky z členských států za účelem sdílení osvědčených postupů a schválení standardních pokynů.

Kybernetickým hrozbám, jimž EU čelí, se dostává široké mediální pozornosti a tato zpráva se zabývá různými oblastmi činnosti, které již v této sféře probíhají. To zahrnuje jak prevenci – prostřednictvím spolupráce s průmyslem za účelem podpory záměrné bezpečnosti a provádění směrnice o bezpečnosti sítí a informací –, tak i podporu spolupráce mezi členskými státy a s mezinárodními organizacemi a partnery na řešení aktuálních kybernetických útoků. V nadcházejících měsících určí Komise a vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku opatření, která je třeba provést, aby se na základě strategie kybernetické bezpečnosti EU z roku 2013 zajistila účinná reakce na tyto hrozby v celé EU.

Ochrana soukromí a osobních údajů jednotlivců je klíčovým základním právem, a tedy základním předpokladem pro jakékoli kroky na cestě ke skutečné bezpečnostní unii. Směrnice o ochraně údajů pro oblast policie a trestního soudnictví přijatá v dubnu 2016 zajišťuje společnou vysokou úroveň ochrany osobních údajů, a usnadní tak rychlou výměnu příslušných údajů mezi donucovacími orgány členských států. Komise v rámci svého balíčku týkajícího se údajů rovněž zahájila revizi směrnice o soukromí a elektronických komunikacích, díky níž se má směrnice vztahovat na všechny poskytovatele elektronických komunikací a její ustanovení mají být sladěna s obecným nařízením o ochraně údajů. Návrh byl vypracován s cílem zajistit soukromí elektronické

[1] Komise v nadcházejících týdnech předloží revidovaný akční plán v oblasti navracení – viz zpráva Komise Evropskému parlamentu, Evropské radě a Radě o zajištění plné operativnosti Evropské pohraniční a pobřežní stráže, COM(2017) 42.

komunikace a zároveň stanovit důvody, na základě kterých lze předpokládat omezení oblasti působnosti nařízení o soukromí a elektronických komunikacích, též z důvodů národní bezpečnosti nebo vyšetřování trestných činů.

II. POSÍLENÍ INFORMAČNÍCH SYSTÉMŮ A INTEROPERABILITY

V projevu předsedy Junckera o stavu Unie v září 2016 a v závěrech Evropské rady z prosince 2016 je zmiňován význam překonání současných nedostatků v oblasti správy informací a zlepšení **interoperability a vzájemného propojení stávajících informačních systémů**. Nedávné události opět zdůraznily naléhavou potřebu propojit stávající databáze EU, v neposlední řadě i proto, aby pohraniční a donucovací orgány na místě měly k dispozici nástroje, které potřebují k odhalování podvodného zneužití totožnosti. Například pachatel teroristického útoku v Berlíně v prosinci 2016 používal alespoň čtrnáct různých totožností a byl schopen se pohybovat mezi jednotlivými členskými státy, aniž by byl odhalen. Je zřejmé, že je zapotřebí umožnit souběžné vyhledávání ve stávajících a budoucích informačních systémech EU pomocí biometrických identifikátorů, aby se tato cesta pro teroristy a zločince uzavřela.

Komise v tomto ohledu zahájila práci v dubnu 2016 prostřednictvím svých návrhů týkajících se „silnějších a inteligentnějších informačních systémů pro ochranu hranic a bezpečnost“[2]. Ty poukázaly na nedostatečné fungování stávajících systémů, mezery v architektuře správy údajů v EU, problémy se složitým prostředím různě řízených informačních systémů a na celkovou roztříštěnost způsobenou tím, že stávající systémy byly navrženy spíše samostatně, než aby se hodily k sobě navzájem. V rámci tohoto procesu Komise vytvořila **expertní skupinu na vysoké úrovni pro informační systémy a interoperabilitu** s agenturami EU, členskými státy a příslušnými zainteresovanými stranami. Zpráva předsedy ze dne 21. prosince 2016[3] uvádí **prozatímní zjištění** skupiny, jež zahrnují prioritní variantu spočívající ve vytvoření jednotného vyhledávacího portálu, který by vnitrostátním donucovacím orgánům a pohraničním orgánům umožnil souběžně vyhledávat ve stávajících databázích a informačních systémech EU. Prozatímní zpráva rovněž zdůrazňuje důležitost kvality údajů, jelikož účinnost informačních systémů se odvíjí od kvality a formátu údajů do nich zadávaných, a obsahuje doporučení ke zlepšení kvality údajů v systémech EU prostřednictvím automatizované kontroly kvality údajů.

Komise urychleně naváže na variantu spočívající ve vytvoření jednotného vyhledávacího portálu a společně s Evropskou agenturou pro provozní řízení rozsáhlých informačních systémů (eu-LISA) zahájí práci na portálu umožňujícím paralelní vyhledávání ve všech příslušných stávajících systémech EU. Do června by měla být dokončena související studie, jako základ pro navržení a vyzkoušení prototypu portálu před koncem tohoto roku. Komise má za to, že Europol by měl zároveň pokračovat ve své práci na systémovém rozhraní, které umožní, aby úředníci v první linii jednotlivých členských států při nahlížení do svých vlastních vnitrostátních systémů mohli souběžně automaticky nahlížet i do databází Europolu.

[2] Sdělení „Silnější a inteligentnější informační systémy pro ochranu hranic a bezpečnost“ (COM(2016) 205 Final).

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

Cílem práce na zajištění interoperability informačních systémů je překonat současnou roztříštěnost v architektuře správy údajů v EU pro ochranu hranic a bezpečnost a vyřešit související nevyjasněné otázky. Pokud databáze využívají společné úložiště údajů o totožnosti, jak předpokládá návrh systému vstupu/výstupu EU a navrhovaný evropský systém pro cestovní informace a povolení (ETIAS), může být určitá osoba zaregistrována v různých databázích pouze pod jednou totožností, což brání používání různých falešných totožností. Jako první krok navržený v předběžných zjištěních expertní skupiny na vysoké úrovni Komise požádala agenturu eu-LISA, aby analyzovala technické a provozní aspekty zavedení společné služby pro porovnávání biometrických údajů. Taková služba by umožnila vyhledávání v různých databázích s biometrickými údaji, což by mohlo odhalit falešné totožnosti používané dotčenou osobou v jiném systému. Expertní skupina na vysoké úrovni by nyní navíc měla posoudit, zda je nezbytné, technicky proveditelné a přiměřené rozšířit **společné úložiště údajů o totožnosti**, které se předpokládá pro systém vstupu/výstupu a systém ETIAS, na jiné systémy. Kromě biometrických údajů uchovávaných ve službě pro porovnávání biometrických údajů by takové společné úložiště údajů rovněž zahrnovalo alfanumerické údaje o totožnosti. Skupina by měla předložit svá zjištění v závěrečné zprávě do konce dubna 2017.

Nedávné události týkající se bezpečnosti ukazují, že je třeba přezkoumat otázku **povinného sdílení informací** mezi členskými státy. Návrh Komise z prosince 2016 zaměřený na posílení **Schengenského informačního systému** vůbec poprvé předpokládá povinnost členských států vydávat upozornění na osoby spojené s teroristickými trestnými činy. Je důležité, aby společní normotvůrci nyní spolupracovali na urychleném přijetí navrhovaných opatření. Komise je připravena prověřit, zda by povinnost sdílení informací měla být zavedena i pro jiné databáze EU.

III. OCHRANA NAŠICH SNADNO ZRANITELNÝCH CÍLŮ PŘED TERORISTICKÝMI ÚTOKY

Berlínský útok byl nejnovějším útokem v EU zaměřeným proti takzvaným snadno zranitelným cílům, což jsou zpravidla civilní objekty, kde se shromažďuje velké množství lidí (např. veřejné prostory, nemocnice, školy, sportovní arény, kulturní střediska, kavárny a restaurace, nákupní střediska a dopravní uzly). Tato místa jsou se své podstaty zranitelná, je obtížné je chránit a vyznačují se pravděpodobností velkého počtu obětí v případě útoku. Ze všech těchto důvodů je teroristé upřednostňují. Hrozba budoucích útoků proti snadno zranitelným cílům, včetně dopravy, zůstává vysoká, jak potvrzují dostupná posouzení, včetně zprávy Europolu o změnách *modu operandi* organizace DÁ'IŠ[4].

Evropský program pro bezpečnost z roku 2015 a sdělení o bezpečnostní unii z roku 2016 zdůraznily potřebu zvýšit úsilí o zlepšení bezpečnosti a využívání inovativních detekčních nástrojů a technologií při ochraně snadno zranitelných cílů. Komise podporuje a podněcuje sdílení osvědčených postupů mezi jednotlivými členskými státy při vyvíjení lepších nástrojů k předcházení útokům na snadno zranitelné cíle a reakci na tyto útoky. Výsledkem této práce jsou operativní příručky a pokyny. V současné době

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

Komise v úzké spolupráci s odborníky z členských států připravuje komplexní příručku týkající se bezpečnostních postupů a šablon použitelných pro různé snadno zranitelné cíle (např. nákupní střediska, nemocnice, sportovní a kulturní akce). Cílem je vydat počátkem roku 2017 pokyny pro členské státy týkající se ochrany snadno zranitelných cílů, které jsou založeny na osvědčených postupech v členských státech.

Souběžně s tím Komise v únoru svolá první seminář s vnitrostátními orgány zaměřený na ochranu snadno zranitelných cílů, a to za účelem výměny informací a vypracování osvědčených postupů týkajících se složité otázky, jíž je ochrana snadno zranitelných cílů a veřejná bezpečnost. Komise rovněž v rámci Fondu pro vnitřní bezpečnost financuje pilotní projekt Belgie, Nizozemska a Lucemburska, jehož cílem je zřídit regionální středisko excelence pro zvláštní zásahy zaměřené na prosazování práva, jež bude poskytovat odbornou přípravu policistům, kteří jsou často prvními zásahovými složkami v případě útoku.

Reagování na útoky na snadno zranitelné cíle je klíčovým prvkem práce Komise v oblasti civilní ochrany. V prosinci Komise oznámila opatření, jež má spolu s členskými státy v úmyslu přijmout, aby byli občané EU bezprostředně po teroristických útocích chráněni a snížila se zranitelnost. Tato opatření posílí koordinaci mezi všemi aktéry, kteří jsou zapojeni do zvládání následků útoků, a Komise se zavázala, že úsilí členských států podpoří tím, že usnadní společnou odbornou přípravu a cvičení a zajistí trvalý dialog prostřednictvím stávajících kontaktních míst a skupin odborníků. Komise rovněž podpoří rozvoj specializovaných modulů pro reakci na teroristické útoky v rámci mechanismu civilní ochrany Unie a iniciativ zaměřených na sdílení poznatků a zvýšení informovanosti veřejnosti.

Ve spolupráci s členskými státy Komise rovněž prozkoumá, jakou podporu by EU mohla poskytnout na pomoc při budování odolnosti a posílení bezpečnosti v okolí potenciálních snadno zranitelných cílů. Členské státy by v souladu s politikou EU a skupiny EIB rovněž mohly požádat o financování z Evropské investiční banky (EIB) (včetně Evropského fondu pro strategické investice). Na každý projekt by se vztahovaly běžné rozhodovací postupy stanovené v právních předpisech.

Pokud jde o konkrétní zranitelné cíle týkající se oblasti veřejné dopravy, jako jsou veřejné části letišť či železničních stanic, na zvláštním semináři pořádaným Komisí v listopadu 2016, jehož se účastnila široká škála zainteresovaných stran, zaznělo, že je třeba zachovat rovnováhu mezi potřebami v oblasti bezpečnosti, pohodlím cestujících a provozováním dopravy. Závěry zdůrazňují význam budování kultury bezpečnosti zahrnující nejen zaměstnance, nýbrž i cestující, důležitost posouzení místních rizik jakožto základ pro stanovení vhodných protiopatření a potřebu posílit komunikaci mezi všemi zúčastněnými stranami.

IV. TVÁŘÍ V TVÁŘ VÝZVÁM V OBLASTI KYBERNETICKÝCH HROZEB

Počítačová kriminality a kybernetické útoky jsou klíčovými problémy, s nimiž se Unie potýká, a opatření na úrovni EU může napomoci k posílení naší kolektivní odolnosti. Kybernetické bezpečnostní incidenty každodenně vážně poškozují lidské životy a způsobují evropskému hospodářství a podnikům velké hospodářské škody. Kybernetické útoky jsou klíčovou složkou hybridních hrozeb – přesně načasované a v kombinaci s fyzickými hrozbami, například ve spojení s terorismem, mohou mít ničivý dopad. Mohou také přispět k destabilizaci země nebo zpochybnění jejích politických institucí

a základních demokratických procesů. Jelikož na on-line technologie spoléháme ve stále větší míře, naše kritické infrastruktury (od nemocnic až po jaderné elektrárny) budou stále zranitelnější.

Součástí klíčové politické reakce na problémy v oblasti kybernetické bezpečnosti je Strategie kybernetické bezpečnosti EU z roku 2013. Hlavním opatřením je směrnice o bezpečnosti sítí a informací[5], která byla přijata v červenci minulého roku. Ta vytváří základ pro lepší spolupráci na úrovni EU a kybernetickou odolnost tím, že podporuje spolupráci a výměnu informací mezi členskými státy a prosazuje operativní spolupráci při konkrétních kybernetických bezpečnostních incidentech a sdílení informací o rizicích. Aby bylo zajištěno jednotné uplatňování v různých odvětvích a různých zemích, uspořádá Komise v únoru první zasedání skupiny pro spolupráci v oblasti bezpečnosti sítí a informací s členskými státy.

V dubnu 2016 Komise a vysoká představitelka EU přijaly společný rámec pro boj proti hybridním hrozbám[6], ve kterém bylo navrženo 22 operativních opatření zaměřených na zvyšování informovanosti, posilování odolnosti, zlepšení reakce na krize a posílení spolupráce mezi EU a NATO. Na základě požadavku Rady předloží Komise a vysoká představitelka EU do července 2017 zprávu za účelem posouzení dosaženého pokroku.

Komise rovněž prosazuje a podporuje technologické inovace, včetně využívání fondů EU v oblasti výzkumu k podpoře nových řešení a vytváření nových technologií, které mohou pomoci posílit naši odolnost proti kybernetickým útokům (např. projekty „záměrné bezpečnosti“). V létě minulého roku jsme zahájili partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost[7] o hodnotě 1,8 miliardy EUR.

V oblasti dopravy se digitalizace stává hlavním faktorem tolik potřebné transformace současného dopravního systému. Rychlé tempo digitalizace přináší mnoho výhod, nicméně doprava se též stává zranitelnější vůči rizikům v oblasti kybernetické bezpečnosti. Přijímá se řada opatření pro zmírnění hrozby na různých úrovních, zejména v oblasti letectví, avšak také v námořní, říční, železniční a silniční dopravě[8]. Je třeba dále vyjasnit, harmonizovat a doplnit činnosti různých zúčastněných stran, které se podílejí na posilování různých aspektů kybernetické odolnosti.

Z širšího hlediska a s ohledem na to, že se povaha hrozby rychle vyvíjí, Komise a vysoká představitelka EU v nadcházejících měsících určí opatření, která je třeba provést, aby byla na základě strategie kybernetické bezpečnosti EU z roku 2013 zajištěna účinná reakce na tyto hrozby v celé EU.

---

5 Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

6 JOIN(2016) 18.

7 Oznámeno ve sdělení o kybernetické odolnosti z roku 2016, COM(2016) 410 final.

8 Příkladem jsou mezinárodní pokyny, jako jsou pokyny vypracované rámci Mezinárodní námořní organizací nebo prostřednictvím nedávno přijatého usnesení ICAO, se společnou iniciativou EU a USA; podávání zpráv o incidentech, v rámci něhož Evropská agentura pro bezpečnost letectví v současné době vyvíjí režim umožňující lepší reakci, a záměrná kybernetická bezpečnost, která se vztahuje na nově vyvíjené systémy, jako je evropský hlavní plán uspořádání letového provozu vypracovaný společným podnikem SESAR.

V. OCHRANA OSOBNÍCH ÚDAJŮ ZA SOUČASNÉ PODPORY ÚČINNÉHO VYŠETŘOVÁNÍ TRESTNÝCH ČINŮ

Směrnice o ochraně údajů pro oblast policie a trestního soudnictví[9] je stavebním kamenem v boji proti terorismu a závažné trestné činnosti. Na základě společného standardu ochrany údajů stanoveného ve směrnici si donucovací orgány členských států budou moci bez problémů vyměňovat příslušné údaje, přičemž údaje obětí, svědků a osob podezřelých ze spáchání trestného činu budou náležitě chráněny.

Kromě toho za účelem zajištění vysoké úrovně důvěrnosti komunikace, jak pro jednotlivce, tak i podniky, a rovných podmínek pro všechny účastníky trhu, jak stanoví strategie pro jednotný digitální trh z dubna 2015, přijala Komise dne 11. ledna návrh **nařízení o soukromí a elektronických komunikacích** (kterým se nahrazuje směrnice 2002/58/ES)[10]. Revidované nařízení o soukromí a elektronických komunikacích, stejně jako stávající směrnice, upřesňuje obecné nařízení o ochraně údajů[11] a stanoví rámec pro ochranu osobních údajů a soukromí v odvětví elektronických komunikací.

Na základě této revize jsou všechna data elektronických komunikací, i když má komunikace doplňkovou funkci, považována za důvěrná/omezená – ať už jsou zprostředkována tradičními telekomunikačními službami, nebo jinými takzvanými službami „over the top“ (OTT), jež jsou z hlediska funkce rovnocenné (např. Skype a WhatsApp) a které jsou již často pro mnohé uživatele zaměnitelné s běžnými telekomunikačními operátory[12]. Povinnosti uložené poskytovatelům služeb – kromě respektování rozhodnutí jejich klientů v oblasti soukromí při používání, uchovávání a zpracovávání jejich údajů – také zahrnují povinnost poskytovatelů služeb, kteří mají sídlo mimo EU, jmenovat svého zástupce v členském státě. To rovněž členským státům dá možnost usnadnit spolupráci donucovacích orgánů a justičních orgánů s poskytovateli služeb za účelem přístupu k elektronickým důkazům (viz níže).

Stejně jako podle stávajících pravidel v oblasti soukromí a elektronických komunikací se bude přístup donucovacích a justičních orgánů k příslušným elektronickým údajům potřebným pro vyšetřování trestné činnosti řídit výjimkou stanovenou v článku 11 navrhovaného nařízení o soukromí a elektronických komunikacích[13]. Toto ustanovení

---

9 Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV. Tato směrnice, která je v platnosti od 5. května 2016, má být členskými státy provedena do 6. května 2018. Za účelem výměny názorů o provedení policejní směrnice Komise zřídila skupinu odborníků s členskými státy.

10 Nařízení o soukromí a elektronických komunikacích, COM(2017) 10.

11 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), které bude použitelné od 25. května 2018.

12 To je v souladu s přístupem použitým v návrhu směrnice, kterou se stanoví evropský kodex pro elektronické komunikace, který předložila Komise dne 14. září 2016 (dále jen „telekomunikační balíček“), COM(2016) 590 final.

13 Viz „ustanovení o uchovávání údajů“ v čl. 11 odst. 1, které bylo beze změny převzato z článku 15 směrnice o soukromí a elektronických komunikacích a sladěno s požadavky obecného nařízení o ochraně osobních údajů. Taková omezení musí respektovat podstatu základních práv a musí být nezbytná, vhodná a přiměřená.

umožňuje omezit v právních předpisech EU nebo vnitrostátních právních předpisech důvěrnost komunikace, je-li to nezbytné a přiměřené za účelem zajištění národní bezpečnosti, obrany, veřejné bezpečnosti a za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů. Toto ustanovení je obzvláště důležité pro vnitrostátní pravidla pro **uchovávání údajů**, tj. pro povinnost poskytovatelů telekomunikačních služeb uchovávat komunikační údaje po určitou dobu pro případný přístup k nim pro účely vymáhání práva, a to v návaznosti na rozhodnutí Evropského soudního dvora (ESD) o neplatnosti směrnice o uchovávání údajů z roku 2014[14]. Od té doby žádný nástroj EU pro uchovávání údajů neexistuje a některé členské státy přijaly v oblasti uchovávání údajů vlastní vnitrostátní právní předpisy. Švédský a britský předpis o uchovávání údajů byly napadeny před ESD, který vydal svůj rozsudek ve věci *Tele2* dne 21. prosince[15]. ESD shledal, že vnitrostátní právní předpisy pro boj proti zločinu, které stanoví všeobecné a nerozlišující uchovávání veškerých provozních a lokalizačních údajů účastníků a uživatelů, které se vztahuje na veškeré prostředky elektronické komunikace, nejsou slučitelné s právem EU. V současné době se zkoumají důsledky tohoto rozhodnutí a Komise vypracuje pokyny, jak mohou být koncipovány vnitrostátní předpisy o uchovávání údajů, aby byly v souladu s uvedeným rozhodnutím.

Trestná činnost zanechává digitální stopy, které mohou sloužit jako důkaz v soudním řízení; elektronická komunikace mezi podezřelými je často jediným vodítkem, jež mohou donucovací orgány a státní zástupci shromažďovat. Nicméně přístup k **elektronickým důkazům**, zejména jsou-li uchovávány v zahraničí nebo v cloudu, může být technicky i právně složitý a často procedurálně obtížný, což vyšetřovatelům komplikuje rychlé přijímání opatření. S ohledem na tyto problémy Komise v současnosti posuzuje řešení, jak vyšetřovatelům umožnit získávání přeshraničních elektronických důkazů, včetně zefektivnění vzájemné právní pomoci, nalezení způsobů, jak přímo spolupracovat s poskytovateli internetových služeb, a jak navrhnout kritéria pro určení a prosazení jurisdikce v kyberprostoru, plně v souladu s platnými pravidly pro ochranu údajů.[16] Dne 9. prosince 2016 podala Komise Radě pro spravedlnost a vnitřní věci zprávu o dosaženém pokroku[17].

Komplexní (a stále probíhající) konzultace s odborníky umožnily Komisi, aby vymezila různé, často složité problémy, které přináší přístup k elektronickým důkazům, získala lepší povědomí o současných pravidlech a postupech v členských státech a stanovila různé možnosti politiky. Zpráva o pokroku poskytuje přehled myšlenek, které doposud vyvstaly při shromažďování informací a odborném procesu, a uvádí, že se Komise po konzultaci se zúčastněnými stranami bude touto záležitostí dále zabývat v nadcházejících měsících. Jak Komise oznámila ve svém pracovním programu, hodlá předložit iniciativu v roce 2017.

---

[14] Viz rozsudek Soudního dvora ve spojených věcech C-293/12 a C-594/12 *Digital Rights Ireland* ze dne 8. dubna 2014.

[15] Viz rozsudek Soudního dvora ve spojených věcech C-203/15 a C-698/15 *Tele2* ze dne 21. prosince 2016.

[16] V souladu se závazkem v Evropském programu pro bezpečnost, COM(2015) 185 final, a sdělením Komise Naplňování Evropského programu pro bezpečnost v zájmu boje proti terorismu a položení základů účinné a skutečné bezpečnostní unie, COM(2016) 230 final.

[17] Ve svých závěrech o zlepšení trestního soudnictví v kyberprostoru ze dne 9. června 2016 Rada vyzvala Komisi, aby přijala konkrétní opatření, vypracovala společný přístup EU a do června 2017 prezentovala výsledky.

VI. ZÁVĚR

Příští zpráva, která má být předložena dne 1. března, bude příležitostí k přezkumu pokroku, jehož bylo dosaženo při provádění těchto a dalších klíčových oblastí činnosti.