EURÓPSKA
KOMISIA

V Bruseli 25. 1. 2017
COM(2017) 41 final

**OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, EURÓPSKEJ RADE A RADE**

**Štvrtá správa o pokroku smerom k dosiahnutiu účinnej a skutočnej bezpečnostnej únie**

**Štvrtá správa o pokroku smerom k dosiahnutiu účinnej a skutočnej bezpečnostnej únie**

## I. ÚVOD

Toto je štvrtá z mesačných správ o pokroku dosiahnutom pri budovaní účinnej a skutočnej bezpečnostnej únie, ktorá sa venuje vývoju v rámci dvoch hlavných pilierov: *boj proti terorizmu a organizovanej trestnej činnosti, ako aj prostriedkom, ktorými sa podporujú, a posilňovanie našej obranyschopnosti a budovanie odolnosti proti týmto hrozbám*. Táto správa sa zameriava na štyri kľúčové oblasti, ktorými sú informačné systémy a interoperabilita, ochrana mäkkých cieľov, kybernetická hrozba a ochrana údajov v rámci vyšetrovania trestnej činnosti.

Decembrový útok na vianočnom trhu v Berlíne opäť upozornil na závažné nedostatky našich informačných systémov, ktoré je potrebné urýchlene riešiť, najmä na úrovni EÚ, aby pohraničné orgány a orgány presadzovania práva jednotlivých štátov v teréne mohli svoju náročnú prácu vykonávať účinnejšie. Skutočnosť, že jednotlivé informačné systémy nie sú navzájom prepojené, čo útočníkom umožňuje používať viacnásobné totožnosti a pohybovať sa bez toho, aby boli odhalení, a to aj pri prekročení hraníc, a to, že členské štáty tieto informácie nezadávajú systematicky do príslušných databáz EÚ, sú nedostatkami praktického vykonávania, ktoré je potrebné urýchlene napraviť. Okrem toho je potrebné vyvinúť ďalšie úsilie aj pokiaľ ide o opatrenia na presadzovanie práva na hraniciach a návrat osôb, ktorých žiadosti o azyl boli zamietnuté[1].

Pokiaľ ide o ochranu mäkkých cieľov, Komisia urýchli svoju činnosť zameranú na nadviazanie spolupráce medzi odborníkmi z členských štátov na účely výmeny najlepších postupov a schválenia štandardných usmernení.

Kybernetická hrozba, ktorej EÚ čelí, má rozsiahle mediálne pokrytie a táto správa sa zaoberá rôznymi oblasťami činnosti, ktoré už v tejto súvislosti prebiehajú. Toto zahŕňa prevenciu – prostredníctvom spolupráce s priemyslom s cieľom podporiť cielenú bezpečnosť a vykonávanie smernice o kybernetickej bezpečnosti – a podporu spolupráce medzi členskými štátmi a s medzinárodnými organizáciami a partnermi pri riešení aktuálnych kybernetických útokov. V nadchádzajúcich mesiacoch určia Komisia a vysoká predstaviteľka Únie pre zahraničné veci a bezpečnostnú politiku opatrenia potrebné na to, aby sa na základe stratégie kybernetickej bezpečnosti EÚ z roku 2013 zabezpečila účinná reakcia na tieto hrozby v celej EÚ.

Ochrana súkromia a osobných údajov fyzických osôb je kľúčovým základným právom, a teda základným prvkom akýchkoľvek krokov smerom k skutočnej bezpečnostnej únii. Smernica o ochrane údajov pre oblasť polície a trestného súdnictva prijatá v apríli 2016 zabezpečuje spoločnú vysokú úroveň ochrany údajov, a preto uľahčí bezproblémovú výmenu relevantných údajov medzi orgánmi presadzovania práva členských štátov. Komisia v rámci svojho balíka týkajúceho sa ochrany údajov takisto začala revíziu smernice o súkromí a elektronických komunikáciách, vďaka ktorej sa má rozsah pôsobnosti smernice rozšíriť na všetkých poskytovateľov elektronických komunikácií a jej ustanovenia majú byť zosúladené so všeobecným nariadením o ochrane údajov.

[1] Komisia nadchádzajúcich týždňoch predloží revidovaný akčný plán v oblasti návratu, pozri správu Komisie Európskemu parlamentu, Európskej rade a Rade o sfunkčnení európskej pohraničnej a pobrežnej stráže COM(2017) 42.

Návrhom by sa malo zabezpečiť súkromie elektronickej komunikácie a zároveň by sa ním mali stanoviť dôvody, na základe ktorých možno obmedziť rozsah pôsobnosti nariadenia o súkromí a elektronických komunikáciách, ako napríklad dôvody národnej bezpečnosti alebo vyšetrovania trestných činov.

## II. POSILNENIE INFORMAČNÝCH SYSTÉMOV A INTEROPERABILITY

V správe predsedu Komisie Junckera o stave Únie v septembri 2016 a záveroch Európskej rady z decembra 2016 sa poukazuje na význam odstránenia súčasných nedostatkov v riadení informácií a zlepšenia **interoperability a vzájomného prepojenia medzi existujúcimi informačnými systémami**. Nedávne udalosti opäť zdôraznili naliehavú potrebu prepojiť existujúce databázy EÚ, v neposlednom rade aj preto, aby pohraničné orgány a orgány presadzovania práva v teréne mali k dispozícii nástroje, ktoré potrebujú na odhaľovanie krádeže identity. Napríklad páchateľ teroristického útoku v Berlíne v decembri 2016 používal aspoň 14 rôznych totožností a bol schopný prechádzať medzi členskými štátmi bez toho, aby bol odhalený. Je jednoznačne potrebné umožniť súčasné vyhľadávanie v existujúcich a budúcich informačných systémoch EÚ s použitím biometrických identifikačných znakov, aby teroristi a zločinci už viac nemohli takéto niečo robiť.

Komisia začala v tejto súvislosti v apríli 2016 pracovať na svojich návrhoch týkajúcich sa „silnejších a inteligentnejších informačných systémov pre hranice a bezpečnosť“[2]. V rámci tejto činnosti sa zistili nedostatky vo funkciách existujúcich systémov, medzery v štruktúre správy údajov v EÚ, problémy so zložitým prostredím odlišne riadených informačných systémov a celková roztrieštenosť spôsobená tým, že existujúce systémy boli navrhnuté samostatne namiesto toho, aby boli zosúladené. Ako súčasť tohto procesu Komisia vytvorila *expertnú skupinu na vysokej úrovni pre informačné systémy a interoperabilitu,* v ktorej sú zastúpené agentúry EÚ, členské štáty a príslušné zainteresované strany. V správe predsedu z 21. decembra 2016[3] sa uvádzajú **predbežné zistenia** skupiny, ktoré zahŕňajú prioritnú možnosť spočívajúcu vo vytvorení jednotného vyhľadávacieho portálu, ktorý by pohraničným orgánom a orgánom presadzovania práva jednotlivých štátov umožnil súčasne vyhľadávať v existujúcich databázach a informačných systémoch EÚ. V predbežnej správe sa takisto zdôrazňuje význam kvality údajov, keďže účinnosť informačných systémov závisí od kvality a formátu údajov, ktoré sa do nich zadávajú, a uvádzajú sa odporúčania na zlepšenie kvality údajov v systémoch EÚ prostredníctvom automatizovanej kontroly kvality údajov.

Komisia sa urýchlene bude zaoberať možnosťou vytvorenia jednotného vyhľadávacieho portálu a spolu s agentúrou EÚ pre prevádzkové riadenie rozsiahlych informačných systémov (eu-LISA) začne pracovať na portáli umožňujúcom súbežné vyhľadávanie vo všetkých príslušných systémoch EÚ, ktoré existujú. Do júna by mala byť dokončená súvisiaca štúdia ako základ pre navrhnutie a testovanie prototypu portálu pred koncom tohto roka. Komisia sa domnieva, že Europol by mal súbežne pokračovať v práci na systémovom rozhraní, ktoré umožní, aby úradníci jednotlivých členských štátov, ktorí pôsobia v prvej línii, mohli pri nahliadaní do vlastných vnútroštátnych systémov súčasne automaticky nahliadať aj do databáz Europolu.

---

[2] Oznámenie „Silnejšie a inteligentnejšie systémy pre hranice a bezpečnosť“, COM(2016) 205 final.

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

Cieľom úsilia o zabezpečenie interoperability informačných systémov je prekonať súčasnú roztrieštenosť štruktúry EÚ pre správu údajov na kontrolu hraníc a bezpečnosť a odstrániť súvisiace nepokryté oblasti. Ak databázy využívajú spoločné úložisko údajov o totožnosti, ako sa predpokladá v návrhu systému vstup/výstup EÚ a navrhovanom systéme EÚ pre cestovné informácie a povolenia (ETIAS), môže byť jedna osoba zaregistrovaná v rôznych databázach len pod jednou totožnosťou, čo bráni používaniu rôznych falošných totožností. Ako prvý krok navrhnutý v predbežných zisteniach skupiny na vysokej úrovni Komisia požiadala agentúru eu-LISA, aby analyzovala technické a prevádzkové aspekty zavedenia spoločnej služby pre porovnávanie biometrických údajov. Takáto služba by umožnila vyhľadávanie v rôznych databázach na základe biometrických údajov, čo by mohlo odhaliť nepravé totožnosti, ktoré daná osoba používa v inom systéme. Skupina na vysokej úrovni by okrem toho mala teraz posúdiť, či je potrebné, technicky možné a primerané rozšíriť **spoločné úložisko údajov o totožnosti**, ktoré sa predpokladá pre systém vstup/výstup a systém ETIAS, aj na iné systémy. Okrem biometrických údajov uložených v službe pre porovnávanie biometrických údajov by takéto spoločné úložisko údajov o totožnosti zahŕňalo aj alfanumerické údaje o totožnosti. Skupina by mala predložiť svoje zistenia vo svojej záverečnej správe do konca apríla 2017.

Nedávne udalosti týkajúce sa bezpečnosti poukazujú na to, že je potrebné opätovne preskúmať otázku **povinnej výmeny informácií** medzi členskými štátmi. V návrhu Komisie z decembra 2016 zameranom na posilnenie **Schengenského informačného systému** sa po prvýkrát predpokladá povinnosť členských štátov vydávať zápisy o osobách, ktoré súvisia s teroristickými trestnými činmi. Je dôležité, aby spoluzákonodarcovia teraz spolupracovali na urýchlenom prijatí navrhovaných opatrení. Komisia je pripravená preskúmať, či by povinnosť výmeny informácií mala byť zavedená aj pre ďalšie databázy EÚ.

## III. OCHRANA NAŠICH MÄKKÝCH CIEĽOV PRED TERORISTICKÝMI ÚTOKMI

Berlínsky útok je posledným útokom v EÚ zameraným proti tzv. mäkkým cieľom, čo sú zväčša civilné objekty, kde sa zhromažďuje veľké množstvo ľudí (napr. verejné priestory, nemocnice, školy, športové arény, kultúrne centrá, kaviarne a reštaurácie, nákupné strediská a dopravné uzly). Tieto miesta sú vo svojej podstate zraniteľné, je ťažké ich chrániť a vyznačujú sa vysokou pravdepodobnosťou veľkého počtu obetí v prípade útoku. Vzhľadom na všetky tieto dôvody ich uprednostňujú teroristi. Hrozba budúcich útokov na mäkké ciele vrátane dopravy zostáva vysoká, ako potvrdzujú dostupné posúdenia, vrátane správy Europolu o zmenách modu operandi organizácie Dá'iš[4].

V Európskom programe v oblasti bezpečnosti z roku 2015 a oznámení o bezpečnostnej únii z roku 2016 sa poukázalo na potrebu zvýšiť úsilie o zlepšenie bezpečnosti a využívanie inovačných detekčných nástrojov a technológií pri ochrane mäkkých cieľov. Komisia podporuje a podnecuje výmenu najlepších postupov medzi členskými

[4] Europol, *Changes in modus operandi of Islamic State (IS) revisited (Zmeny v mode operandi Islamského štátu, prehodnotené )*, november 2016 – verejné informácie Europolu, dokument dostupný na webovej stránke: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited

štátmi pri vývoji lepších nástrojov na predchádzanie útokom na mäkké ciele a reakciu na tieto útoky. Výsledkom tejto činnosti sú operatívne príručky a usmernenia. Komisia v súčasnosti pripravuje, v úzkej spolupráci s odborníkmi z členských štátov, komplexnú príručku o bezpečnostných postupoch a vzoroch, ktoré sa vzťahujú na rôzne mäkké ciele (napr. nákupné strediská, nemocnice, športové a kultúrne podujatia). Cieľom je začiatkom roka 2017 vydať usmernenia pre členské štáty týkajúce sa ochrany mäkkých cieľov, ktoré budú založené na najlepších postupoch v členských štátoch.

Súbežne s tým Komisia vo februári zvolá prvé pracovné stretnutie s vnútroštátnymi orgánmi zamerané na ochranu mäkkých cieľov, ktorého cieľom bude výmena informácií a vypracovanie najlepších postupov týkajúcich sa zložitej otázky, ktorou je ochrana mäkkých cieľov a zaistenie verejného poriadku a verejnej bezpečnosti. Komisia okrem toho v rámci Fondu pre vnútornú bezpečnosť financuje aj pilotný projekt Belgicka, Holandska a Luxemburska, ktorého cieľom je zriadiť regionálne centrum excelentnosti pre osobitné zásahy zamerané na presadzovania práva, ktoré bude poskytovať odbornú prípravu pre príslušníkov polície, ktorí sú často prvými zásahovými zložkami v prípade útoku.

Reakcia na útoky na mäkké ciele je kľúčovým prvkom činnosti Komisie v oblasti civilnej ochrany. Komisia v decembri oznámila opatrenia, ktoré má v úmysle uskutočniť s členskými štátmi, aby bezprostredne po teroristických útokoch boli občania EÚ chránení a znížila sa ich zraniteľnosť. Tieto opatrenia posilnia koordináciu medzi všetkými subjektmi zapojenými do zvládania následkov útokov, pričom Komisia sa zaviazala, že úsilie členských štátov podporí tým, že uľahčí spoločnú odbornú prípravu a cvičenia a zabezpečí nepretržitý dialóg prostredníctvom existujúcich kontaktných miest a expertných skupín. Komisia takisto podporí rozvoj špecializovaných modulov pre reakciu na teroristické útoky v rámci mechanizmu Únie v oblasti civilnej ochrany a iniciatív zameraných na výmenu získaných poznatkov a zvýšenie informovanosti verejnosti.

Komisia spolu s členskými štátmi takisto preskúma, akú podporu by EÚ mohla poskytnúť na pomoc pri budovaní odolnosti a posilnení bezpečnosti v okolí potenciálnych mäkkých cieľov. Členské štáty by takisto mohli požiadať o financovanie z Európskej investičnej banky (EIB) (vrátane Európskeho fondu pre strategické investície) v súlade s politikou EÚ a skupiny EIB. Na každý projekt by sa vzťahovali bežné rozhodovacie postupy stanovené v právnych predpisoch.

Pokiaľ ide o konkrétne mäkké ciele týkajúce sa verejných priestorov v rámci dopravy, ako sú verejné časti letísk alebo železničných staníc, Komisia v novembri 2016 na osobitnom pracovnom stretnutí so širokou škálou zainteresovaných strán zdôraznila potrebu zachovať rovnováhu medzi potrebami v oblasti bezpečnosti, pohodlia cestujúcich a prevádzkovania dopravy. V záveroch sa zdôrazňuje význam budovania kultúry bezpečnosti zahŕňajúcej nielen zamestnancov, ale aj cestujúcich, dôležitosť posúdenia miestnych rizík ako základu pre stanovenie vhodných protiopatrení a potrebu zlepšiť komunikáciu medzi všetkými zainteresovanými stranami.

## IV. RIEŠENIE VÝZIEV V OBLASTI KYBERNETICKÝCH HROZIEB

Počítačová kriminalita a kybernetické útoky sú kľúčovými výzvami, ktorým Únia čelí, pričom opatrenia na úrovni EÚ môžu pomôcť posilniť našu kolektívnu odolnosť voči týmto hrozbám. Incidenty v oblasti kybernetickej bezpečnosti každý deň vážne poškodzujú životy ľudí a európskemu hospodárstvu a podnikom spôsobujú značné hospodárske škody. Kybernetické útoky sú kľúčovou zložkou hybridných hrozieb – presne načasované a v kombinácii s fyzickými hrozbami, napríklad v súvislosti

s terorizmom, môžu mať ničivé následky. Môžu tiež prispieť k destabilizácii krajiny alebo spochybneniu jej politických inštitúcií a základných demokratických procesov. Keďže sa na online technológie spoliehame čoraz viac, naše kritické infraštruktúry (od nemocníc až po jadrové elektrárne) budú čoraz zraniteľnejšie.

Súčasťou kľúčovej politickej reakcie na problémy v oblasti kybernetickej bezpečnosti je Stratégia kybernetickej bezpečnosti EÚ z roku 2013. Hlavným opatrením je smernica o sieťovej a informačnej bezpečnosti (NIS)[5], ktorá bola prijatá v júli minulého roku. Smernica vytvára základ pre lepšiu spoluprácu na úrovni EÚ a kybernetickú odolnosť tým, že podporuje spoluprácu a výmenu informácií medzi členskými štátmi a propaguje operatívnu spoluprácu pri konkrétnych incidentoch v oblasti kybernetickej bezpečnosti a pri výmene informácií o rizikách. S cieľom zabezpečiť jednotné vykonávanie v rámci jednotlivých odvetví, ako aj cezhranične Komisia vo februári usporiada prvé zasadnutie skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti s členskými štátmi.

V apríli 2016 Komisia a vysoká predstaviteľka EÚ prijali spoločný rámec pre boj proti hybridným hrozbám[6], v ktorom navrhli 22 operačných akcií zameraných na zvyšovanie informovanosti, posilňovanie odolnosti, lepšie reagovanie na krízy a zintenzívnenie spolupráce medzi EÚ a NATO. Tak, ako to žiadala Rada, Komisia a vysoká predstaviteľka EÚ predložia do júla 2017 správu s cieľom posúdiť pokrok.

Komisia takisto propaguje a podporuje technologickú inováciu, okrem iného prostredníctvom využívania fondov EÚ v oblasti výskumu, s cieľom stimulovať nové riešenia a vytvoriť nové technológie, ktoré môžu pomôcť posilniť našu odolnosť voči kybernetickým útokom [napr. projekty cielenej bezpečnosti („*security by design*“)]. V lete minulého roku sme začali rozvíjať verejno-súkromné partnerstvo v oblasti kybernetickej bezpečnosti s hodnotou 1,8 mld. EUR[7].

V oblasti dopravy sa digitalizácia stáva významným faktorom umožňujúcim veľmi potrebnú transformáciu súčasného dopravného systému. Rýchle tempo digitalizácie prináša mnoho výhod, ale zároveň spôsobuje, že sa doprava stáva zraniteľnejšou voči rizikám v oblasti kybernetickej bezpečnosti. Prijímajú sa mnohé opatrenia na zmiernenie tejto hrozby na rôznych úrovniach, najmä v oblasti letectva, ale aj v námornej, riečnej, železničnej a cestnej doprave[8]. Ešte stále je však potrebné ďalej objasniť, harmonizovať a doplniť činnosti jednotlivých zainteresovaných strán, ktoré sa podieľajú na posilňovaní rôznych aspektov kybernetickej odolnosti.

Zo širšieho hľadiska a vzhľadom na rýchlo sa meniacu povahu hrozieb Komisia a vysoká predstaviteľka EÚ v nasledujúcich mesiacoch určia opatrenia, ktoré je potrebné vykonať, aby bola na základe stratégie kybernetickej bezpečnosti EÚ z roku 2013 zabezpečená účinná reakcia na tieto hrozby v celej EÚ.

---

5 Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

6 JOIN(2016) 18.

7 Ohlásené v oznámení o kybernetickej odolnosti z roku 2016, COM(2016) 410 final.

8 Ako príklad možno uviesť medzinárodné usmernenia, ako napríklad tie, ktoré vypracovala Medzinárodná námorná organizácia, alebo tie, ktoré boli stanovené prostredníctvom nedávno prijatej rezolúcie ICAO, so spoločnou iniciatívou EÚ a USA; oznamovanie incidentov, v rámci ktorého Európska agentúra pre bezpečnosť letectva v súčasnosti vyvíja režim umožňujúci lepšiu reakciu, a cielená kybernetická bezpečnosť, ktorá sa vzťahuje na novo vyvíjané systémy, ako je hlavný plán riadenia letovej prevádzky vypracovaný spoločným podnikom SESAR.

## V. OCHRANA OSOBNÝCH ÚDAJOV A SÚČASNÁ PODPORA EFEKTÍVNEHO VYŠETROVANIA TRESTNÝCH ČINOV

Základným stavebným kameňom v boji proti terorizmu a závažnej trestnej činnosti je smernica o ochrane údajov pre oblasť polície a trestného súdnictva[9]. Na základe spoločnej normy ochrany údajov stanovenej v smernici si orgány presadzovania práva členských štátov budú môcť bez problémov vymieňať príslušné údaje, zatiaľ čo údaje obetí, svedkov a podozrivých zo zločinov budú náležite chránené.

Okrem toho s cieľom zabezpečiť vysokú úroveň dôvernosti komunikácie, tak pre fyzické osoby, ako aj pre podniky, a rovnaké podmienky pre všetkých účastníkov trhu, ako sa to uvádza v stratégii jednotného digitálneho trhu z apríla 2015, Komisia prijala 11. januára návrh **nariadenia o súkromí a elektronických komunikáciách** (ktorým sa nahrádza smernica 2002/58/ES)[10]. V revidovanom nariadení o súkromí a elektronických komunikáciách sa, rovnako ako v platnej smernici, rozpracováva všeobecné nariadenie o ochrane údajov[11] a stanovuje sa rámec pre ochranu súkromia a osobných údajov v sektore elektronických komunikácií.

Na základe tejto revízie sú všetky údaje elektronickej komunikácie, aj keď má komunikácia doplnkovú funkciu, považované za dôverné a rešpektujú sa – bez ohľadu na to, či komunikácia prebieha prostredníctvom tradičných telekomunikačných služieb alebo iných tzv. Over-The-Top (OTT) služieb, ktoré sú z hľadiska funkcie rovnocenné (napr. Skype a WhatsApp) a ktoré sú pre mnohých používateľov často vzájomne zameniteľné s bežnými telekomunikačnými operátormi[12]. Povinnosti uložené poskytovateľom služieb zahŕňajú – okrem rešpektovania rozhodnutí zákazníkov týkajúcich sa súkromia pri používaní, uchovávaní a spracúvaní ich údajov – aj povinnosť vymenovať zástupcu v členskom štáte, ktorá sa vzťahuje na poskytovateľov služieb so sídlom mimo EÚ. To členským štátom takisto umožní uľahčiť spoluprácu orgánov presadzovania práva a súdnych orgánov s poskytovateľmi služieb na účely prístupu k elektronickým dôkazom (pozri ďalej v texte).

Rovnako ako podľa súčasných pravidiel v oblasti ochrany súkromia v elektronických komunikáciách sa na prístup orgánov presadzovania práva a súdnych orgánov k príslušným elektronickým informáciám potrebným na vyšetrovanie trestnej činnosti bude vzťahovať výnimka stanovená v článku 11 navrhovaného nariadenia o súkromí a elektronických komunikáciách[13]. Toto ustanovenie umožňuje obmedziť v právnych

---

9 Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV. Túto smernicu, ktorá nadobudla účinnosť 5. mája 2016, majú členské štáty transponovať do 6. mája 2018. Na účely výmeny názorov o transpozícii policajnej smernice Komisia v spolupráci s členskými štátmi zriadila expertnú skupinu.

10 Nariadenie o súkromí a elektronických komunikáciách, COM(2017) 10.

11 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), ktoré sa začne uplatňovať od 25. mája 2018.

12 Je to v súlade s prístupom použitým v navrhovanej smernici, ktorou sa zavádza európsky kódex elektronickej komunikácie, ktorú Komisia predložila 14. septembra 2016 (ďalej len „telekomunikačný balík“), COM(2016) 590 final.

13 Pozri „ustanovenie o uchovávaní údajov“ v článku 11 ods. 1, ktoré bolo bez zmeny prevzaté z článku 15 smernice o súkromí a elektronických komunikáciách a zosúladené s požiadavkami všeobecného nariadenia o ochrane údajov. Takéto obmedzenie musí rešpektovať podstatu základných práv a musí byť nevyhnutné, vhodné a primerané.

predpisoch EÚ alebo vo vnútroštátnych právnych predpisoch dôvernosť komunikácie, ak je to potrebné a primerané na účely zaistenia národnej bezpečnosti, obrany, verejnej bezpečnosti a na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo výkonu trestov. Toto ustanovenie je obzvlášť dôležité pre vnútroštátne právne predpisy o **uchovávaní údajov**, t. j. vzhľadom na povinnosť poskytovateľov telekomunikačných služieb uchovávať komunikačné údaje na vymedzené obdobie pre prípadný prístup k nim na účely presadzovania práva, v nadväznosti na rozhodnutie Európskeho súdneho dvora (ďalej len „Súdny dvor“) o zrušení smernice o uchovávaní údajov z roku 2014[14]. Odvtedy žiaden nástroj EÚ na uchovávanie údajov neexistuje a niektoré členské štáty prijali vlastné vnútroštátne zákony o uchovávaní údajov. Švédsky a britský predpis o uchovávaní údajov boli napadnuté pred ESD, ktorý 21. decembra vydal svoj rozsudok vo veci *Tele2*[15]. ESD dospel k záveru, že vnútroštátne právne predpisy v oblasti boja proti trestnej činnosti, ktoré stanovujú všeobecné a nediferencované uchovávanie všetkých údajov o prenose dát a polohe týkajúcich sa účastníkov a používateľov, ktoré sa vzťahuje na všetky prostriedky elektronickej komunikácie, nie sú zlučiteľné s právom Únie. V súčasnosti sa analyzujú dôsledky tohto rozsudku a Komisia vypracuje usmernenia, ako môžu byť vnútroštátne predpisy o uchovávaní údajov koncipované, aby boli v súlade s uvedeným rozsudkom.

Trestná činnosť zanecháva digitálne stopy, ktoré môžu slúžiť ako dôkazy v súdnom konaní; elektronická komunikácia medzi podozrivými je často jediným záchytným bodom, ktorý môžu orgány presadzovania práva a prokurátori zhromažďovať. Avšak prístup k **elektronickým dôkazom** – najmä ak sa uchovávajú v zahraničí alebo v cloude – môže byť technicky aj právne zložitý a často procedurálne náročný, čo vyšetrovateľom bráni v rýchlom prijímaní opatrení. S cieľom riešiť tieto výzvy Komisia v súčasnosti posudzuje riešenia, ako vyšetrovateľom umožniť získať cezhraničné elektronické dôkazy, vrátane zefektívnenia vzájomnej právnej pomoci, nachádzania spôsobov priamej spolupráce s poskytovateľmi internetových služieb, a ako navrhnúť kritériá na určenie a presadzovanie jurisdikcie v kybernetickom priestore, v plnom súlade s platnými pravidlami ochrany údajov.[16]Komisia 9. decembra 2016 predložila Rade pre spravodlivosť a vnútorné veci správu o dosiahnutom pokroku[17].

Proces komplexných (a stále prebiehajúcich) konzultácií s expertmi umožnil Komisii vymedziť rôzne a často zložité problémy, ktoré vyplývajú z prístupu k elektronickým dôkazom, na účely lepšieho pochopenia súčasných pravidiel a postupov v členských štátoch a na účely stanovenia rôznych možností politiky. V správe o pokroku sa poskytuje prehľad nápadov, ktoré dosiaľ vznikli v procese zhromažďovania informácií a konzultácií s expertmi a uvádza sa v nej, že Komisia sa po konzultácii so zainteresovanými stranami bude v nadchádzajúcich mesiacoch touto záležitosťou ďalej zaoberať. Ako Komisia oznámila vo svojom pracovnom programe, v roku 2017 predloží iniciatívu.

## VI. ZÁVER

Ďalšia správa, ktorá má byť predložená 1. marca, bude príležitosťou na preskúmanie pokroku dosiahnutého v rámci týchto a ďalších kľúčových oblastí činnosti.

---

[14] Rozsudok Súdneho dvora v spojených veciach C-293/12 a C-594/12, *Digital Rights Ireland* z 8. apríla 2014.

[15] Rozsudok Súdneho dvora v spojených veciach C-203/15 a C-698/15 *Tele2 z* 21. decembra 2016.

[16] V súlade so záväzkom v Európskom programe v oblasti bezpečnosti, COM(2015) 185 final, a oznámením Komisie s názvom Napĺňanie Európskeho programu v oblasti bezpečnosti s cieľom bojovať proti terorizmu a pripraviť pôdu pre účinnú a skutočnú bezpečnostnú úniu COM(2016) 230 final.

[17] Rada vo svojich záveroch o zlepšení trestnej justície v kybernetickom priestore z 9. júna 2016 vyzvala Komisiu, aby prijala konkrétne opatrenia, vypracovala spoločný prístup EÚ a do júna 2017 predložila výsledky.