NSZ ČR

Zpráva o činnosti národního korespondenta pro boj proti kybernetické kriminalitě, pro ochranu práv k nehmotným statkům a kybernetickou bezpečnost za rok 2019

Mgr. Petr Klement

V Brně dne 29. ledna 2020
3 SE 101/2020

Trendy v oblasti kybernetické kriminality, zaznamenané v minulých letech, lze označit za pokračující. Pokračuje i nárůst této trestné činnosti (v roce 2019 bylo ze strany Policie ČR vykázáno celkem 8417 případů, což je téměř o 25% více než v minulém roce[1]), který může být statisticky způsoben i nárůstem její identifikace ze strany orgánů činných v trestním řízení. Lze také konstatovat, že nadále přetrvává již dříve popsaná latence tohoto druhu kriminality a nízké právní vědomí veřejnosti v kombinaci s poměrně omezenými schopnostmi rozpoznat, předcházet a bránit se útokům využívajícím informační technologie.

Dynamický rozvoj informačních technologií a jejich uvádění na trh v neustálých vylepšeních a obměnách (například využití šifrování jako standardu, včetně využití biometrických dat, bezdrátové šifrované přenosy mezi synchronizovanými zařízeními, masivní ukládání dat ve vzdálených úložištích, stále se zjednodušující možnosti využití kryptoměn, alternativní využití *blockchainu*, nové elektronické platební metody, atd.) přináší nové právní otázky s takovou rychlostí, že je možné je řešit pouze analogickým výkladem stávajících norem, které byly často vytvořeny v době, kdy uvedené technologie neexistovaly. Na úrovni tvorby legislativy proto představuje tento trend do blízké budoucnosti zásadní otázku, jakým legislativně-technickým způsobem na tyto technologické a s nimi související společenské změny reagovat.

Nejvýznamnější problematikou v tomto směru je nastupující využití umělé inteligence v informačních technologiích a jejich zpřístupnění široké veřejnosti.

Události a trendy v oblasti kyberkriminality v roce 2019

Za zřetelně nejvýznamnější nejen pro oblast kybernetické kriminality lze považovat nález Ústavního soudu ČR ze dne 14. května 2019, sp. zn. Pl. ÚS 45/17, ve věci návrhu na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, § 88a zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, § 68 odst. 2 a § 71 písm. a) zákona č. 273/2008 Sb., o Policii České republiky, a vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

Tímto nálezem reagoval Ústavní soud mimo jiné na rozhodnutí Tele2 Sverige AB[2] a vymezil rámec pro uplatnění zákonných zásahů do práva na soukromí ze strany státu v podobě tzv. uchování dat (pro označení uchování dat se i v českém jazyce vžil pojem *data retention*).

Napadená právní úprava se podle Ústavního soudu evropskému standardu nevymyká.[3] Stejně jako technologie se vyvíjí i forma páchání trestné činnosti, stále častěji vznikají po pachatelích pouze elektronické stopy, vyšetřovací metody minulých let proto nelze srovnávat.

[1] Statistické přehledy kriminality za rok 2019, dostupné z: https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2019.aspx
[2] Rozhodnutí Soudního dvora EU ze dne 21. 12. 2016 ve spojených věcech C-203/15 and C-698/15
[3] Následující odstavce jsou citací z předmětného rozhodnutí Ústavního soudu.

Současná úprava tzv. *data retention* naplňuje požadavky kladené citovanou dřívější judikaturou Ústavního soudu a lze ji aplikovat ústavně konformním způsobem, tedy tak, aby byla maximálně šetřena práva jednotlivců, garantovaná články 10 a 13 Listiny.

V podmínkách dnešní informační společnosti, v níž běžný jednotlivec využívá služeb elektronické komunikace takřka na každém kroku a dobrovolně přijímá, že se o něm ukládají kvanta dat, bylo by nemoudré tolerovat stav, v němž by poskytovatelé služeb údaji uživatelů disponovali, a státní aparát (v odůvodněných případech) nikoli. Plošné uchovávání provozních a lokalizačních údajů představuje snahu státu „neztratit v době informační společnosti krok“ a mít v rukou efektivní nástroje k plnění svých úkolů – zde zejména v oblasti bezpečnosti státu a jeho obyvatel. Principiálně proto z pohledu Ústavního soudu nelze *data retention* zavrhovat.

V tiskové zprávě ze dne 22. 5. 2019 pak Ústavní soud doplnil, že každou žádost o zpřístupnění provozních a lokalizačních údajů a odůvodněnost jejího podání je třeba ze strany oprávněného orgánu důkladně zvážit a ze strany soudu pečlivě přezkoumat s ohledem na konkrétní okolnosti posuzovaného případu.

Dále Ústavní soud v tiskové zprávě uvádí, že přestože neshledal důvody pro zrušení právní úpravy *data retention*, zákonodárce by neměl v době překotného vývoje moderních technologií „usínat na vavřínech“. Současná právní úprava nereflektuje aktuální technologický vývoj a společenský trend co do způsobu a forem využívání elektronické komunikace, např. vymezení okruhu povinných subjektů, neodpovídá dnešnímu způsobu využívání služeb elektronické komunikace – povinnost *data retention* se nevztahuje na poskytovatele tzv. OTT služeb (např. Facebook, WhatsApp, Skype), které již víceméně klasický telekomunikační provoz začínají nahrazovat.

Tento poslední poznatek Ústavního soudu se plně slučuje s trendy popsanými v úvodu tohoto přehledu.

V návaznosti na rozhodnutí Ústavního soudu je nutno zopakovat, že i po několika letech není stále jednotně vyřešena **pojmová otázka provozních a lokalizačních údajů**, které požívají zvláštní ochrany v podobě postupu uvedeného v § 88a trestního řádu.

Z pozitivně právního hlediska nejbližší právní definici takových údajů obsahuje § 97 odst. 3 a 4 zákona č. 127/2005 Sb. o elektronických komunikacích, ve znění pozdějších předpisů, a navazující vyhláška Ministerstva průmyslu a obchodu a Ministerstva vnitra č. 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

Citovaná vyhláška zahrnuje celý výčet údajů, například vztah mezi telefonním číslem a identifikátorem mobilního zařízení IMEI, do rozsahu uchovávaných provozních a lokalizačních údajů, tedy údajů ve smyslu § 97 odst. 3 zákona o elektronických komunikacích, které má příslušný poskytovatel, na něhož tento zákon dopadá, povinnost uchovávat. Trestní řád pak v § 88a stanoví zvláštní způsob přístupu k takto uchovávaným údajům, což díky přísnějším procesním pravidlům představuje i posílení jejich ochrany.

Otázkou je, zda je nutno se daného postupu držet u všech údajů, které vyjmenovává citovaná vyhláška, což by dávalo ministerstvu průmyslu a obchodu spolu s ministerstvem vnitra značný vliv na postup orgánů činných v trestním řízení, nebo zda je zapotřebí další úvaha v podobě vyhodnocení míry zásahu do práva na soukromí, například optikou ve dřívějších zprávách uvedeného případu Breyer[4]. Takový postup by mohl být slučitelný i s vyjádřením Nejvyššího soudu uvedeným v usnesení ze dne 18. 1. 2017, č. j. 7 Tdo 1768/2016, ve kterém se Nejvyšší soud, byť možná i nepřesně, snažil mezi povinně uchovávanými údaji rozlišit mezi „údaji vztahujícími se k osobě uživatele a k mobilnímu zařízení jako k věci“. Jinými slovy, bylo by vhodné rozlišovat mezi údaji vedoucími k identifikaci konkrétního uživatele, jeho zvycích, pohybu, apod. a mezi údaji, které takovou identifikaci neumožňují. Roztříštěná interpretace na úrovni celé soustavy státního zastupitelství se odvíjí od rozdílné interpretace těchto pojmů soudy a vzhledem k tomu, že trestní řád nebyl v tomto ohledu novelizován tak, aby k interpretaci poskytl alespoň určité pravidlo (například ve světle uvedené judikatury), lze očekávat, že uvedená interpretační nejednotnost bude přetrvávat.

Kasační soud Belgie dne 19. 2. 2019 vydal **rozsudek[5] v tzv. věci „Skype“** týkající se povinnosti poskytovatele (společnosti Skype Communications Sarl) umožnit belgickým orgánům činným v trestním řízení odposlech a záznam datového provozu uskutečňovaného pomocí aplikace Skype, a to na základě povinnosti, kterou mají všichni poskytovatelé telekomunikačních služeb se sídlem v Belgii (společnost Skype Communications Sarl sídlí v Lucembursku a je vlastněna nadnárodní společností Microsoft). Kasační soud dovodil, že jelikož uvedená společnost nabízí služby na území Belgie a podstata těchto služeb je poskytování telekomunikačního přenosu dat, musí uvedená společnost podléhat stejným pravidlům, jako všichni ostatní poskytovatelé telekomunikačních služeb na území Belgie. Na toto rozhodnutí navazuje rozhodnutí Soudního dvora EU ze dne 5. 6. 2019[6], ve kterém Soudní dvůr potvrdil, že tzv. služby OTT (*over the top*), jako je například služba uvedené společnosti SkypeOut a SkypeIn, mohou být zahrnuty pod pojem „služba elektronických komunikací“ ve smyslu rámcové směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací, a to se všemi povinnostmi pro poskytovatele, které z toho vyplývají.

Světlo do uvedené problematiky má vnést **Směrnice (EU) 2018/1972 o evropském kodexu pro elektronické komunikace**, podle které bude nově definice služby elektronické komunikace zahrnovat mimo jiné i „interpersonální komunikační službu“, tedy službu za úplatu umožňující přímou interaktivní výměnu informací mezi dvěma a více lidmi, kdy tyto osoby, které komunikaci zahajují nebo se jí účastní, určují jejího příjemce.

Až v rámci této kategorie má dále dojít k rozlišení na služby založené na číslech (klasické telefonické spojení a zasílání SMS zpráv prostřednictvím telefonních čísel přidělených operátory) a na služby nezávislé na číslech, kam se řadí i tzv. OTT

[4] Rozhodnutí Soudního dvora EU ve věci C-582/14 *Patrick Breyer v. Bundesrepublik Deutschland*
[5] Rozsudek Kasačního soudu (*Cour de Cassation*) ze dne 19. 2. 2019, sp. zn. P.17.1229.N.
[6] Rozsudek Soudního dvora EU ze dne 5. 6. 2019, sp. zn. C-142/18.

služby využívající ke zprostředkování komunikace internetový protokol. Uvedená směrnice má být implementována do prosince 2020.

K dlouhodobě diskutované problematice **relevance fyzického umístění dat** je nutno zmínit **rozhodnutí Nejvyššího soudu Norska**[7], ve kterém se soud zabýval zákonností nařízení domovní prohlídky v prostorách právnické osoby, v jejímž rámci bylo provedeno také „stažení" dat ze vzdálených úložišť, která se fyzicky nacházejí mimo norské území. Soud shledal postup orgánů činných v trestním řízení za zákonný a uvedl, že užití donucujícího procesního opatření (domovní prohlídky) započalo na norské půdě, relevantní data byla získána opatřením směřujícím proti norské společnosti se sídlem v Norsku. Rozhodnutí o opatření bylo vydáno norským soudem při zachování obecně platných zákonných záruk. Prohlídkou (vzdáleného úložiště) byl získán přístup pouze k datům, která zde uchovávala dotčená společnost, která tato data mohla volně stahovat z úložiště umístěného v zahraničí. Data na zahraničním serveru byla zachována a nebyla nijak pozměněna. Norský soud také uvedl, že nenašel žádné ustanovení v právním řádu Norska, ani v mezinárodních úmluvách, které by provedení takového úkonu zakazovalo a neshledává jeho provedením narušení jurisdikce a státní suverenity jiného státu.

Incidenty v oblasti kybernetické bezpečnosti pouze potvrzují to, co bylo uvedeno ve zprávách z předešlých let, tedy, že je pouze otázkou času, kdy také na území ČR dojde k úspěšným kybernetickým útokům na významné nebo citlivé cíle. Jako příklad lze uvést kybernetický útok ze dne 20. 12. 2019 na zařízení společnosti OKD, který vedl k přerušení těžby ve všech dolech uvedené společnosti na Karvinsku, nebo útok ransomwarového viru na zdravotnické zařízení v Benešově, jehož následkem nebylo možné spustit přístroje, včetně počítačové sítě, což vedlo například ke zrušení plánovaných operací. Předmětem trestního vyšetřování se stal také kybernetický útok na vnější síť ministerstva zahraničních věcí v červnu 2019. Podle Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) byl tento incident útokem cizí státní moci. Podle NÚKIB a podle společnosti Kaspersky Lab bylo za první tři měsíce roku 2019 v porovnání s předchozím čtvrtletím zachyceno o 84 % více DDoS útoků, než v předchozím období. Výrazně se také navýšila jejich délka. Průměrná doba trvání, která byla více než hodinu, se zdvojnásobila. Rostoucí čísla naznačují, že je o DDoS útoky v kyberzločinecké komunitě stálé větší zájem, a to i přes to, že mezinárodní policejní koalice na jaře 2018 zavřela největší tržiště webstresser.org, kde bylo možné DDoS koupit jako službu.

Globálním politickým i mediálním tématem se stala otázka tzv. *fake news*, tedy digitálního obsahu, který vytváří přesvědčivou iluzi věcí, které se nikdy nestaly nebo neexistují tak, jak je předkládáno. Stále větší úlohu přitom sehrává využití tzv. botů a chatbotů, tedy jednoduché umělé inteligence.

Právě **umělá inteligence** je tím nejvýznamnějším technologickým trendem a její využití a případně zneužití bezpochyby největší budoucí výzvou pro vyšetřování a právní hodnocení trestní odpovědnosti. Především tzv. prediktivní vyhledávání trestné činnosti, případně dovozování trestní odpovědnosti za „připravovanou trestnou činnost" za pomoci jednoduché umělé inteligence, je dnes v některých

[7] Rozsudek Nejvyššího soud Norska ze dne 28. března 2019, sp. zn. HR-2019-610-A, ve věci Tidal Music AS proti státnímu zastupitelství

zemích světa již realitou. Potenciálního využití umělé inteligence při rozhodování v justici je otázkou, která je již analyzována na úrovni Rady Evropy[8], Evropské unie[9], nebo jednotlivých členských států[10]. Bylo by proto vhodné, aby se i české orgány činné v trestním řízení a specialisté na použití informačních technologií v justici touto otázkou také v České republice včas zabývali, neboť jde o zcela novou a komplexní etickou, právní a technickou problematiku.

Lze tedy shrnout, že přetrvávají dříve popsané fenomény, jako je zneužívání kryptoměn k praní špinavých peněz, podvodům a daňovým únikům, zneužívání anonymity sítě (především sítě TOR) k obchodu s nelegálním obsahem všeho druhu, krádeže osobních a platebních údajů a jejich prodej či zneužití, v neposlední řadě v anonymním kriminálním prostředí na sítích přetrvává fenomén nabídky zločinu jako služby.

Síť specializovaných státních zástupců

Specialisté na kybernetickou kriminalitu se v září 2019 zúčastnili setkání se státními zástupci a policejními specialisty z Bavorska (*Generalstaatsanwaltschaft Bamberg*) a Saska (*Generalstaatsanwaltschaft Dresden a LKA Cyber Dresden*), setkání se účastnili také zástupci sekce kybernetické kriminality NCOZ. Setkání bylo zaměřeno především na výměnu zkušeností formou prezentace konkrétních případových studií a volně navazovalo na studijní návštěvu specializovaného státního zastupitelství v Bamberku v roce 2018.

Vzhledem k velkému zájmu z řad státních zástupců došlo k dohodě, že přístup k elektronickému portálu NCOZ, kde je k dispozici řada aktualizovaných informací, bude do budoucna umožněn všem státním zástupcům, kteří o něj požádají.

Velmi pozitivně lze hodnotit skutečnost, že se sítí státních zástupců byly diskutovány některé interní dokumenty, či návrhy právních předpisů. Aktivitu této sítě však do budoucna nebude možno nechávat na aktivitě jednotlivých členů, neboť vzhledem k množství otázek, které tato problematika s sebou aktuálně přináší, bude při hledání řešení potřeba rozdělení konkrétních úkolů mezi členy sítě. Existence a činnost sítě prokázaly, že se velmi dobrých výsledků dá dosáhnout i neformální dohodu vedoucích státních zástupců, nebo flexibilní spoluprací členů sítě například s NCOZ, Masarykovou univerzitou, nebo NÚKIB.

[8] Viz např. Evropská charta etiky pro užívání umělé inteligence v justičních systémech a v prostředí justice, dostupné pouze v anglické verzi z: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

[9] Viz např. Koordinovaný plán pro umělou inteligenci „Made in Europe“ a další politiky Komise EU, jejichž přehled je dostupný z: https://ec.europa.eu/digital-single-market/en/artificial-intelligence

[10] V tomto ohledu lze doporučit zejména analýzu Společnosti pro právo Anglie a Walesu z června 2019, *Algorithms in the Criminal Justice System*, dostupnou z https://www.lawsociety.org.uk/support-services/research-trends/algorithm-use-in-the-criminal-justice-system-report/